



Information Risk & Security Institute (IRSI)
Especialización en Security Operations Center

Instructor: Antonio Cabrera

Jornada matutina

Proyecto de graduación

SOC-TRAINING

(Plataforma de aprendizaje en línea para los aspirantes interesados en el área de
SOC-CTIS-DFIR)

Kevin Fabricio Alvarado Buezo

Héctor Josué Ponsoy Ayala

Franklin Benito Mayorga Baquedano

Jezer Abimael Jiménez López

Fecha: Noviembre 2023



ÍNDICE

INTRODUCCIÓN	10
CAPITULO I MARCO CONCEPTUAL.....	12
1.1 Objetivos de la Investigación	12
1.1.1 General	12
1.1.2 Específicos	12
1.2 Antecedentes.....	13
1.3 Justificación	13
1.4 Alcances y límites.....	14
1.4.1 Alcances	14
1.4.2 Límites.....	15
CAPITULO II MARCO METODOLÓGICO	16
2.1 Hipótesis	16
2.2 Tipo de Investigación	16
2.3 Diseño de la Investigación.....	16
2.4 Población	17
2.5 Muestra	18
2.6 Cálculo de la muestra	18
2.7 Técnicas e Instrumentos de Recolección de Datos.....	19
2.7.1 Técnicas de recolección de datos	19
2.7.2 Instrumento de recolección de datos	19
2.8 Procesamiento de los Datos	20
2.9 Análisis de los Resultados	20
2.9.1 Datos Generales.....	20

2.9.2	Datos de Preguntas	21
2.10	Prueba de Hipótesis.....	32
2.10.1	Frecuencias Observadas	32
2.10.2	Frecuencia esperada.....	32
2.10.3	Distribución Chi-Cuadrado Calculado	33
2.10.4	Distribución Chi-Cuadrado Crítico	35
2.10.5	Análisis de los Resultados	36
CAPITULO III MARCO TEÓRICO		38
3.1	Incidente de Seguridad	38
3.2	Inteligencia de Amenazas	38
3.3	APT (Advanced Persistent Threat).....	38
3.4	Firewall.....	38
3.5	IPS (Intrusion Prevention System)	39
3.6	Phishing	39
3.7	SOC Analyst.....	39
3.8	IOC (Indicators of Compromise).....	40
3.9	VPN (Virtual Private Network)	40
3.10	Ransomware.....	40
3.11	Ciberseguridad	40
3.12	EDR (Endpoint Detection and Response).....	41
3.13	Gestión de Eventos	41
3.14	Ciberdefensa	41
3.15	Relaciones B2B.....	41
3.16	Capturas de Paquetes	42
3.17	PowerShell	42

3.18	Hash	42
3.19	VirusTotal	43
3.20	Directiva de seguridad local.....	43
3.21	Administrador	43
3.22	Firewall	43
3.23	Windows Defender	44
3.24	Puerto USB	44
3.25	Regedit	44
3.26	Ransomware WannaCry	44
3.27	Ransomware Petya.....	45
3.28	Ransomware NotPetya.....	45
3.29	Gestión de parches	46
3.30	Actualizaciones de software	46
3.31	Copias de seguridad	46
3.32	Respuesta a incidentes	47
3.33	Prueba de penetración	47
3.34	Filtración de datos.....	47
3.35	Resiliencia cibernética	48
3.36	Indicador de compromiso	48
3.37	Stakeholders	48
3.38	Marco de ciberseguridad del NIST	49
CAPITULO IV DESARROLLO DEL PROYECTO		50
4.1	Plugins utilizados.....	50
4.1.1	Edubin Core.....	50
4.1.2	Tutor LMS Pro	50

4.1.3	All-in-One WP Migration	50
4.1.4	Dynamic Visibility for Elementor.....	51
4.1.5	Elementor	51
4.1.6	PRO Elements	51
4.1.7	The Events Calendar	52
4.1.8	Tutor LMS Elementor Addons.....	52
4.1.9	WPForms Lite	52
4.1.10	WP Super Cache.....	52
4.2	Herramientas.....	53
4.2.1	WordPress	53
4.2.2	Hostinger	53
4.3	Desarrollo de la plataforma	54
4.3.1	Dashboard.....	54
4.3.2	Footer	55
4.3.3	Cursos.....	56
4.3.4	Contacto sobre nosotros	57
4.3.5	Sección de Eventos.....	58
4.3.6	Registro para estudiante	58
4.3.7	Sección de Mi perfil	59
4.3.8	Sección de login	59
4.3.9	Login con OTP	60
4.3.10	Correo electrónico con la clave OTP.....	60
4.3.11	Formulario de Registro de confirmación de correo electrónico	61
4.3.12	Correo electrónico con el enlace de confirmación	61
4.4	Guía educativa	62

4.4.1	Curso 1 – Introducción al Centro de Operaciones de Seguridad (SOC)	62
4.4.2	Curso 2 – SOC: Fundamentos y Colaboración	64
4.4.3	Curso 3 – Modelos y tipos de despliegue de los SOC	65
4.4.4	Curso 4 – SOC360: Personal, Funciones e Interacción en Ciberseguridad	67
4.4.5	Curso 5 – Datos de eventos de seguridad y herramientas para analistas SOC....	68
4.4.6	Curso 6 – Relaciones clave del SOC con los stakeholders	70
4.4.7	Curso 7 – Estrategias de Protección Cibernética	71
4.4.8	Curso 8 – Comprender el flujo de trabajo y la automatización del SOC	72
4.4.9	Curso 9 – Vulnerabilidades, malware y respuesta a incidentes	74
4.4.10	Curso 10 – Laboratorios	76
4.4.11	Examen Final SOC: Travesía de Conocimiento en 10 Cursos	77
4.6	Diagrama de Gantt.....	79
CONCLUSIONES		81
RECOMENDACIONES		82
BIBLIOGRAFÍA.....		84
ANEXOS.....		90
Anexos 1. Manuales		90
Manual de Usuario Administrador.....		90
Manual de Usuario Docente.....		91
Manual de Usuario Estudiante		92
Anexos 2. Autoevaluaciones		93
Anexos 3. Coevaluaciones		97
Anexos 4. Constancia de participación en la elaboración del proyecto		101
Anexos 5. Enlace de la demostración real de la plataforma en video		105

ÍNDICE DE TABLAS

Tabla 1. <i>Datos generales de la encuesta</i>	20
Tabla 2. <i>Datos - Primera pregunta</i>	21
Tabla 3. <i>Datos - Segunda pregunta</i>	23
Tabla 4. <i>Datos - Tercera pregunta</i>	24
Tabla 5. <i>Datos - Cuarta pregunta</i>	25
Tabla 6. <i>Datos - Quinta pregunta</i>	26
Tabla 7. <i>Datos - Sexta pregunta</i>	27
Tabla 8. <i>Datos - Séptima pregunta</i>	28
Tabla 9. <i>Datos - Octava pregunta</i>	29
Tabla 10. <i>Datos - Novena pregunta</i>	30
Tabla 11. <i>Datos - Decima pregunta</i>	31
Tabla 12. <i>Frecuencias Observadas</i>	32
Tabla 13. <i>Frecuencias Esperadas</i>	33
Tabla 14. <i>Comprobación del Chi-Cuadrado</i>	34
Tabla 15. <i>Versión de Plugins utilizados</i>	54

INDICE DE FIGURAS

<i>Figura 1. Datos Generales</i>	21
Figura 2. Edad del Personal	22
Figura 3. Interacción con una plataforma de aprendizaje	23
Figura 4. Aceptación de la Implementación del Sistema	24
Figura 5. Disposición a utilizar el Sistema Web	25
Figura 6. Punto de vista sobre la plataforma.....	26
Figura 7. Aprobación de la comodidad del uso de la plataforma.....	27
Figura 8. Aprobación de centralizar el contenido	28
Figura 9. Aumento de estudio en los estudiantes	29
Figura 10. Inversión de horas al día	30
Figura 11. Prevenir información errónea	31
Figura 12. Tabla de Distribución Chi-Cuadrado.....	36
Figura 13. Dashboard	54
Figura 14. Dashboard 2	55
Figura 15. Footer	55
Figura 16. Cursos parte 1	56
Figura 17. Cursos parte 2	56
Figura 18. Sobre nosotros parte 1	57
Figura 19. Sobre nosotros parte 2	57
Figura 20. Sección de Eventos	58
Figura 21. Registro para estudiante.....	58
Figura 22. Sección de mi perfil	59
Figura 23. Sección de login.....	59
Figura 24. Login con OTP	60
Figura 25. Correo electrónico con la clave OTP	60
Figura 26. Formulario de Registro de confirmación de correo electrónico	61
Figura 27. Correo electrónico con el enlace de confirmación	61
Figura 28. Curso 1	62
Figura 29. Curso 2.....	64

Figura 30. Curso 3.....	65
Figura 31. Curso 4.....	67
Figura 32. Curso 5.....	68
Figura 33. Curso 6.....	70
Figura 34. Curso 7.....	71
Figura 35. Curso 8.....	72
Figura 36. Curso 9.....	74
Figura 37. Curso 10.....	76
Figura 38. Examen Final	77
Figura 39. Diagrama de Gantt 1	79
Figura 40. Diagrama de Gantt 2	80

INTRODUCCIÓN

La presente investigación se sitúa en el campo de entrenamiento de la ciberseguridad, un área de creciente importancia en el mundo digitalizado en el que vivimos. En particular, nos enfocamos en el área de las Operaciones de Seguridad (SOC), la Tecnología de la Información y la Seguridad (CTIS), y la Respuesta a Incidentes de Seguridad Digital (DFIR). Estos campos son fundamentales para proteger la integridad y confidencialidad de la información en las organizaciones y, por lo tanto, son de gran relevancia tanto para los profesionales del sector como para los estudiantes que aspiran a trabajar en este campo.

La pregunta central que guía esta investigación es: “¿Cómo la implementación de una plataforma de aprendizaje en línea mejora el acceso a información relevante y de calidad para los aspirantes en el área de SOC-CTIS-DFIR?” Esta pregunta surge del reconocimiento de una brecha en el curso actual de IRSI, donde los estudiantes están estudiando ciberseguridad. Mientras que otras áreas tienen su sección en la plataforma, el área de SOC carece de una, y toda la información que los estudiantes retienen es a través de las clases, lo cual no es suficiente. Por lo tanto, es de vital importancia la creación de una plataforma de enseñanza para SOC.

Para abordar esta pregunta, proponemos una metodología basada en el diseño y desarrollo de una plataforma educativa en línea. Esta plataforma servirá como un recurso integral para aquellos que buscan instruirse en la especialización de SOC. Al proporcionar un espacio centralizado y accesible, esperamos mejorar significativamente el acceso a información relevante y de calidad para los aspirantes en el área.

La importancia de esta investigación radica en su potencial para transformar la forma en que los estudiantes y profesionales acceden a la información sobre SOC-CTIS-DFIR. Al crear una plataforma virtual, no sólo estamos proporcionando un recurso educativo valioso, sino también contribuyendo al avance del campo de la ciberseguridad al facilitar la formación y educación continua de sus profesionales.

La tesis se organizará en varios módulos, cada uno centrado en un aspecto específico del área de SOC. Cada módulo incluirá una evaluación del contenido con un mínimo del 80% para aprobar. Los módulos cubrirán temas como la introducción al Centro de Operaciones de Seguridad, los servicios del Centro de Operaciones de Seguridad, los modelos y tipos de despliegue del SOC, la dotación del personal para un equipo SOC eficaz, los datos relevantes del SOC y las herramientas para analistas SOC, las relaciones clave del SOC con los stakeholders, los marcos de seguridad y respuesta a incidentes, conceptos básicos de redes, vulnerabilidades y amenazas, tipos de malware y respuesta según tipo de incidente. Además, habrá laboratorios prácticos realizados por los integrantes del equipo a forma de video tutorial.

CAPITULO I MARCO CONCEPTUAL

1.1 Objetivos de la Investigación

1.1.1 General

Avanzar como grupo en la investigación y comprensión de temas relacionados a Security Operation Center (SOC) y la importancia que este rol conlleva en el área de la seguridad cibernética.

1.1.2 Específicos

- a) Investigar y preparar el contenido relacionado a los módulos y temas asignados para posteriormente empezarlos a subir a la página web.
- b) Generar preguntas relevantes para cuestionarios con base a los temas que se han estado investigando de manera que le sirvan al estudiante para su posterior evaluación.
- c) Llevar a cabo un análisis en profundidad de las implicaciones prácticas de los conceptos estudiados, teniendo en consideración la relevancia en el entorno actual de la seguridad cibernética.

1.2 Antecedentes

En el proceso de desarrollo de este proyecto centrado en la implementación de una plataforma de aprendizaje en línea para aspirantes interesados en el área de SOC-CTIS-DFIR, es esencial contextualizar la problemática que busca abordar. La decisión de emprender este desafío se fundamenta en la identificación de una carencia significativa de recursos educativos especializados y exhaustivos para aquellos que se adentran en el fascinante campo de los Centros de Operaciones de Seguridad (SOC).

Los motivos que nos llevaron a seleccionar este desafío son evidentes al considerar las diversas problemáticas enfrentadas por los aspirantes y profesionales en la ciberseguridad. La falta de recursos educativos específicos, la brecha en la capacitación, los riesgos para la seguridad y los desafíos en la retención de talento han sido identificados como obstáculos clave en la formación efectiva en el ámbito del SOC. La ausencia de una fuente centralizada y confiable de información agrava estas problemáticas, creando un escenario propicio para el desarrollo de una solución que aborde estas deficiencias.

Por lo tanto, la selección de este desafío se basa en la necesidad de proporcionar a los aspirantes y profesionales en el campo de SOC-CTIS-DFIR un recurso educativo integral y accesible que supere las limitaciones actuales. Esta plataforma de aprendizaje en línea se concibe como una respuesta directa a la falta de recursos especializados, buscando llenar el vacío educativo y facilitar la formación continua de los individuos en la ciberseguridad, contribuyendo así al avance del sector y al fortalecimiento de la comunidad de profesionales en el mundo de la ciberseguridad.

1.3 Justificación

La ciberseguridad ha surgido como un elemento principal en la protección de sistemas de información y datos críticos. El aumento de amenazas cibernéticas requiere demasiada demanda de profesionales altamente capacitados en SOC, ya que son esenciales para salvaguardar y defender las infraestructuras digitales de organizaciones y empresas.

Existe poca información de recursos educativos especializados diseñados para satisfacer las necesidades específicas de los aspirantes a profesionales de SOC. El campo de la ciberseguridad

es muy amplio, especializado y diverso, lo que dificulta que los interesados en el SOC encuentren información precisa y capacitación para instruirlos al área.

Un sistema de aprendizaje enfocado en SOC ayudará a mejorar la seguridad cibernética en las organizaciones. Esto permitirá una mayor protección de los sistemas de información y ayudará a reducir el riesgo de incidentes cibernéticos, aspecto de vital importancia en un entorno donde las amenazas cibernéticas están en constante evolución.

El desarrollo de habilidades esenciales es un factor crucial que respalda la necesidad de este sistema de aprendizaje. Capacitar a los aspirantes en SOC les ayudará en adquirir y desarrollar las habilidades necesarias para identificar, mitigar y gestionar amenazas, también ayudará a poder garantizar la continuidad de las operaciones en caso de ataques, lo que resulta en una necesidad importante para la seguridad de las organizaciones.

En la actualidad las amenazas cibernéticas continúan evolucionando y volviéndose más sofisticadas con el tiempo, invertir en la formación en SOC es esencial para preparar a los profesionales y las organizaciones que puedan venir en el futuro en el ámbito de la ciberseguridad. Esto asegurará que las organizaciones puedan estar preparadas para afrontar cualquier tipo de amenaza que surja en un entorno digital en constante cambio.

1.4 Alcances y límites

1.4.1 Alcances

- a) Geográfico: La plataforma será implementada de manera web lo cual no habrá impedimento geográfico y podrá ser utilizado por diferentes personas de cualquier lugar sin ningún problema.
- b) Conceptual: La plataforma incluirá las siguientes funcionalidades: Registro de estudiante, registro de tutor, funcionalidad de login, creación de cursos, publicación

de cursos, creación de lecciones, creación de entregables, creación de exámenes, barra de herramientas tanto para estudiantes y de instrucciones.

- c) Temporal: El proyecto tiene un tiempo de desarrollo estimado de dos meses, que se está realizando desde octubre hasta finales de noviembre del año 2023.

1.4.2 Límites

- a) El sistema online será utilizado exclusivamente para estudiantes interesados en el área de especialización en el área de SOC.
- b) Por decisión del Ingeniero encargado es necesario que al momento de crear una cuenta recibir un correo para tener factor de autenticación
- c) Por decisión del Ingeniero encargado la plataforma debe tener manuales de estudiante, docente y administrador.

CAPITULO II MARCO METODOLÓGICO

2.1 Hipótesis

H₀: La implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR, no tiene un impacto significativo para los estudiantes o profesionales interesados en el área de SOC. (Hipótesis Nula)

H₁: La implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR, tiene un impacto significativo para los estudiantes o profesionales interesados en el área de SOC. (Hipótesis Alternativa)

2.2 Tipo de Investigación

En la presente investigación se utiliza el método mixto para examinar la efectividad de una plataforma de aprendizaje diseñada para individuos interesados en las áreas de Security Operations Center (SOC), Computer and Information Technology Security (CTIS), y Digital Forensics and Incident Response (DFIR). A través de encuestas en línea y entrevistas, se recopilarán datos cuantitativos y cualitativos con el propósito de evaluar la percepción, utilidad y relevancia de la plataforma. Los resultados obtenidos guiarán ajustes necesarios para asegurar que la plataforma satisfaga las expectativas y necesidades de los usuarios en estos campos específicos.

2.3 Diseño de la Investigación

Se tomaron en cuenta cuatro elementos fundamentales en el proceso de desarrollo de la investigación:

- a) Sujetos:** Investigadores, Jezer Jiménez, Héctor Ponsoy, Kevin Alvarado, Franklin Mayorga.

- b) **Objeto:** Encuestas destinadas a evaluar la relevancia y aceptación de implementar una plataforma de aprendizaje en línea para fortalecer las habilidades en el área de Security Operations Center (SOC), Computer and Information Technology Security (CTIS), y Digital Forensics and Incident Response (DFIR). El enfoque se centra en optimizar el aprendizaje y reducir posibles obstáculos al adquirir conocimientos en estos campos especializados.
- c) **Medio:** Las herramientas para el desarrollo del sistema web son las siguientes: WordPress y Plugins como: Edubin Core, Tutor LMS Pro, All-in-One WP Migration, Dynamic Visibility for Elementor, etc.
- d) **Fin:** La implementación exitosa y la adopción de una plataforma de aprendizaje en línea que mejore la eficacia y la satisfacción en la adquisición de conocimientos en áreas especializadas como Security Operations Center (SOC), Computer and Information Technology Security (CTIS), y Digital Forensics and Incident Response (DFIR). El objetivo final es optimizar el proceso de aprendizaje tanto para los interesados en estas disciplinas como para el personal encargado de la formación, permitiendo una adquisición de habilidades más efectiva y contribuyendo al fortalecimiento de la comunidad de profesionales en seguridad informática.

2.4 Población

La población para esta investigación comprenderá a la totalidad de la comunidad del Dojo interesada en ciberseguridad, y constará de 300 personas. Este grupo específico de individuos está compuesto por profesionales, estudiantes y entusiastas de la seguridad informática que participan activamente en las actividades y recursos proporcionados por el Dojo. La población es finita y representa el conjunto completo de miembros involucrados en el Dojo, contribuyendo al estudio y la práctica de la ciberseguridad en su comunidad.

2.5 Muestra

En el estudio en cuestión, se empleó una fórmula estadística precisa con el fin de obtener una muestra representativa y confiable. Debido a que la población bajo investigación es finita, se aplicó cuidadosamente la fórmula correspondiente para calcular el tamaño de la muestra y obtener resultados exactos.

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

Donde:

n=Tamaño de la muestra

z= Nivel de confianza

p= Probabilidad de éxito

q= Probabilidad de fracaso

N= Población Total

e=Error estándar

Datos

n=?

z= Nivel de confianza 95% (1.96)

p= Probabilidad de éxito 50% (0.5)

q= Probabilidad de fracaso 50% (0.5)

N= Población Total (300)

e= Error estándar 5% (0.05)

2.6 Cálculo de la muestra

$$n = \frac{(1.96)^2 * 0.5 * 0.5 * 300}{(0.05)^2 * (300 - 1) + (1.96)^2 * 0.5 * 0.5}$$

$$n = \frac{288.12}{1.7079}$$

$$n = 168.69$$

$$n \approx 170$$

Luego de realizar la fórmula se obtuvo una muestra de 170 personas que se tomará como muestra para hacer el análisis de los resultados.

2.7 Técnicas e Instrumentos de Recolección de Datos

2.7.1 Técnicas de recolección de datos

En este estudio sobre la implementación de una plataforma de aprendizaje en el área de SOC, se empleará la técnica de encuesta en línea para recolectar datos. A través de cuestionarios diseñados, se aplicarán encuestas a la comunidad de Dojo, compuesta por 300 personas interesadas en ciberseguridad de las cuales se tomará de muestra 170 personas. El objetivo es obtener información relevante sobre sus necesidades de aprendizaje, preferencias y expectativas con respecto a la plataforma propuesta. Esta técnica eficiente facilitará el análisis de los datos recopilados y orientará el desarrollo de la plataforma para satisfacer las demandas de la comunidad de Dojo.

2.7.2 Instrumento de recolección de datos

En el caso de la implementación de la plataforma de aprendizaje en el área de SOC, se utilizará Google Forms como herramienta principal para la recopilación de información. Los cuestionarios diseñados para la encuesta online contendrán preguntas cerradas y de escala, sumando un total de 10 preguntas para la comunidad de Dojo, compuesta por 300 personas interesadas en ciberseguridad. Estas preguntas se han estructurado de manera específica para obtener detalles sobre diversos aspectos cruciales para la investigación, como el nivel de conocimiento tecnológico

de los participantes, la receptividad hacia la implementación de una plataforma de aprendizaje y las expectativas con respecto al contenido y las funcionalidades propuestas en la plataforma.

2.8 Procesamiento de los Datos

La recolección de datos se llevará a cabo a través de encuestas en línea dirigidas a la comunidad de Dojo, compuesta por 300 personas interesadas en el área de SOC. La muestra para el estudio se determinará mediante cálculos estadísticos para garantizar representatividad y precisión en los resultados. Los datos recopilados se almacenarán en un formato digital, facilitando su análisis y tabulación para obtener información significativa. Se utilizarán gráficos y visualizaciones para presentar de manera clara y ordenada los resultados, permitiendo un análisis exhaustivo de las respuestas y la obtención de conclusiones valiosas para la investigación.

2.9 Análisis de los Resultados

A continuación, se muestra el análisis de los resultados recopilados de las encuestas realizadas. Este análisis está organizado con información extraída gracias a las preguntas obteniendo los resultados que se detallan a continuación.

2.9.1 Datos Generales

Tabla 1. *Datos generales de la encuesta*

Género	Frecuencia	Porcentaje
Masculino	113	34%
Femenino	57	66%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)

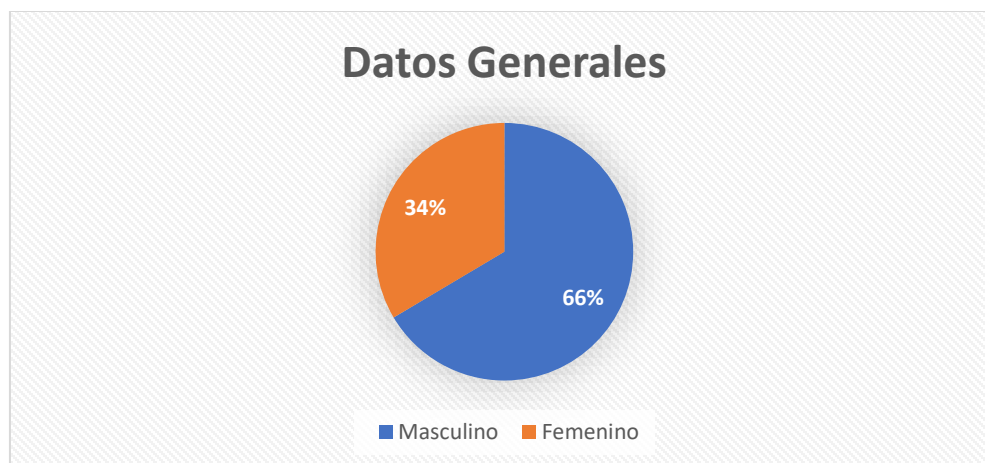


Figura 1. Datos Generales

Fuente: Elaboración Propia

Interpretación: En esta gráfica se observa que la mayoría de los encuestados, son de género masculino equivalente a un 66% de las personas tomadas para la muestra, mientras que el otro 34% es de género femenino, determinando que la mayoría de las personas que utilizarán el sistema web serán de género masculino.

2.9.2 Datos de Preguntas

Pregunta No. 1 ¿Cuál es su edad?

Tabla 2. Datos - Primera pregunta

Respuestas	Frecuencia	Porcentaje
Menor a 18 años	0	0%
Entre 18 y 20 años	0	0%
Entre 20 y 22 años	85	50%
Entre 24 y 28 años	48	28%
Mayor a 28 años	37	22%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)

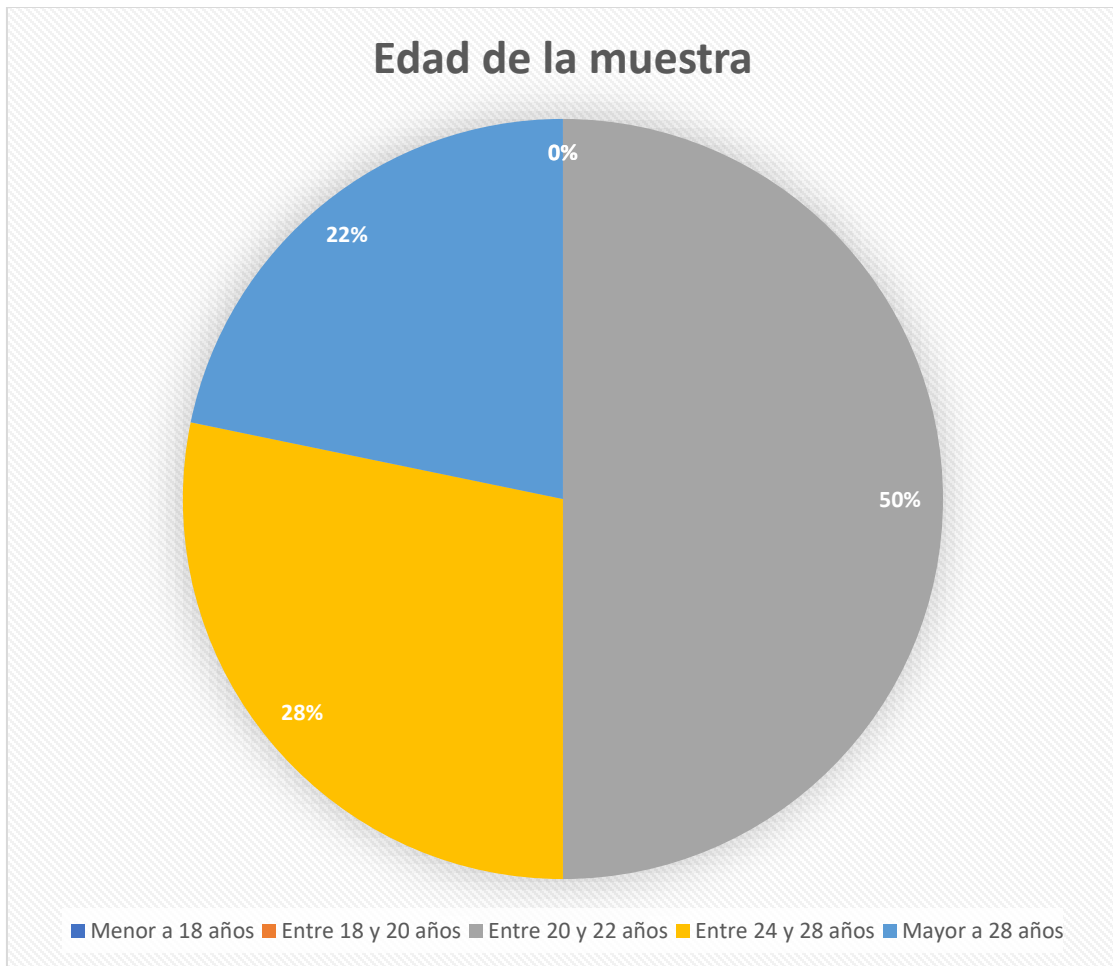


Figura 2. Edad del Personal

Fuente: Elaboración Propia

Interpretación: En esta gráfica podemos analizar que el rango de edad de los encuestado del total y es conformado por personas jóvenes, teniendo un total de 50% del total de la muestra entre 20 y 22 años lo que equivale a la mayoría de la edad, esto demuestra lo que facilita significativamente la interacción que las personas tienen con la tecnología y sea fácil que se adapten a la plataforma de aprendizaje online.

Pregunta No. 2 ¿Haz utilizado alguna vez una plataforma de aprendizaje en línea?

Tabla 3. *Datos - Segunda pregunta*

Respuestas	Frecuencia	Porcentaje
Si	170	100%
No	0	0%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)

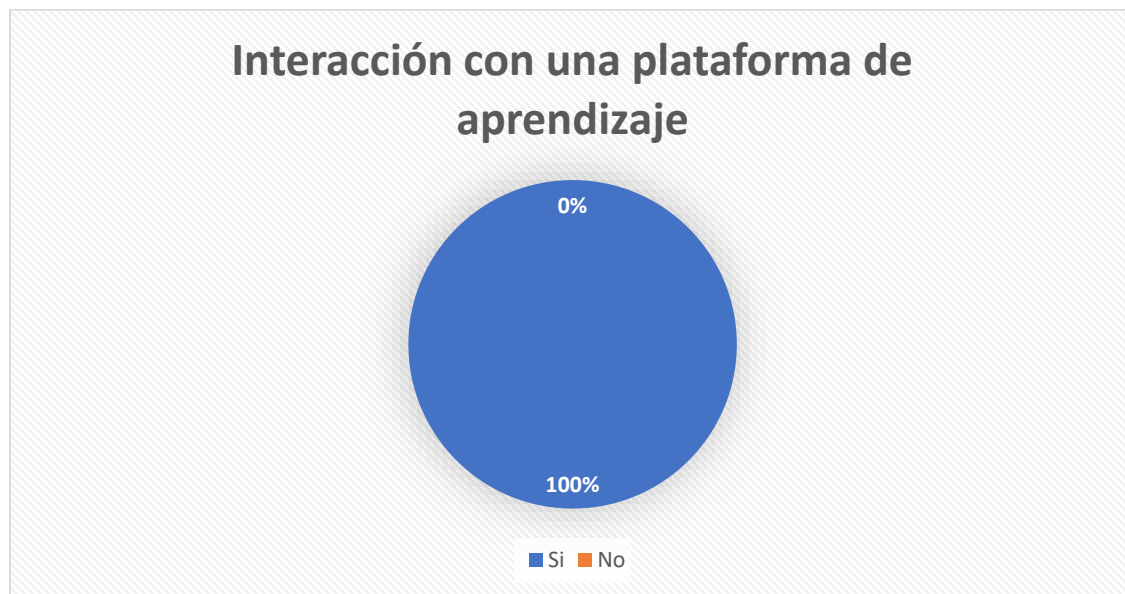


Figura 3. Interacción con una plataforma de aprendizaje

Fuente: Elaboración Propia

Interpretación: En esta gráfica se observa que el 100% de los encuestados han interactuado alguna vez con una plataforma de aprendizaje, lo que favorece de manera significativa la implementación del proyecto.

Pregunta No. 3 ¿Cuál ha sido tu experiencia utilizando plataformas de aprendizaje en línea?

Tabla 4. *Datos - Tercera pregunta*

Respuestas	Frecuencia	Porcentaje
Muy buena	95	56%
Aceptable	67	39%
No tan agradable	8	5%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)

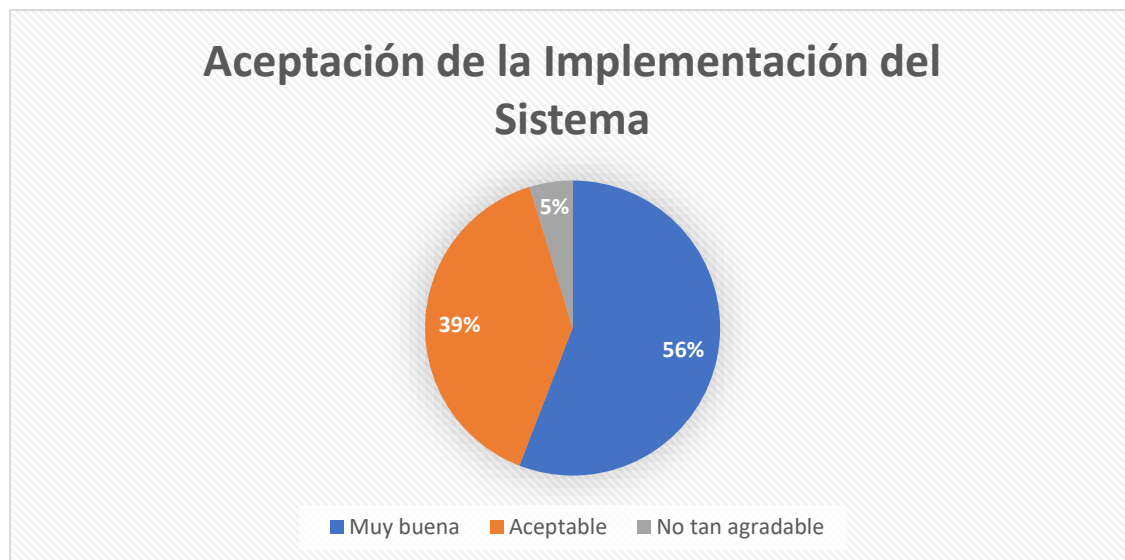


Figura 4. Aceptación de la Implementación del Sistema

Fuente: Elaboración Propia

Interpretación: De acuerdo con esta gráfica se observa que el 56% de la población investigada ha tenido una muy buena experiencia del uso de una plataforma o sistema Web la mayoría ha tenido interacción con un sistema web comentan que no será difícil implementar dicho sistema.

Pregunta No. 4 ¿Estás de acuerdo en que en la actualidad es de gran importancia el aprendizaje autodidacta a través de una plataforma de aprendizaje en línea?

Tabla 5. Datos - Cuarta pregunta

Respuestas	Frecuencia	Porcentaje
Si	170	100%
No	0	0%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)



Figura 5. Disposición a utilizar el Sistema Web

Fuente: Elaboración Propia

Interpretación: Los resultados de los datos representan que el 100% de la población investigada, está de acuerdo en la importancia de una plataforma de aprendizaje por lo tanto también influye en que quieran utilizar y adaptarse a usar un sistema web.

Pregunta No. 5 ¿Estarías dispuesto a utilizar la nueva plataforma de aprendizaje en línea, SOC-Training, ¿para formarte en la especialidad de ciberseguridad en el SOC?

Tabla 6. Datos - Quinta pregunta

Respuestas	Frecuencia	Porcentaje
Si	164	96%
No	6	4%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)



Figura 6. Punto de vista sobre la plataforma

Fuente: Elaboración Propia

Interpretación: De acuerdo con los datos obtenidos de esta gráfica se observa que el 96% de las personas encuestadas están de acuerdo en utilizar la nueva plataforma de aprendizaje en línea SOC-Training, mientras que el 4% de la población no considera seguro utilizarla.

Pregunta No. 6 ¿Cree que el uso de una plataforma de aprendizaje en línea podría mejorar su comodidad y eficacia al estudiar?

Tabla 7. Datos - Sexta pregunta

Respuestas	Frecuencia	Porcentaje
Si	158	93%
No	12	7%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)



Figura 7. Aprobación de la comodidad del uso de la plataforma

Fuente: Elaboración Propia

Interpretación: En los resultados de la encuesta se obtienen los resultados dónde se observa que el 93% de las personas encuestadas está de acuerdo en el uso de una plataforma de aprendizaje en línea podría mejorar su comodidad y eficacia al estudiar, mientras el 7% respondió que, no siendo una frecuencia de 12, por lo que sí es favorable su implementación.

Pregunta No. 7 ¿Considera importante contar con una fuente centralizada de información accesible en todo momento a través de una plataforma de aprendizaje en línea?

Tabla 8. Datos - Séptima pregunta

Respuestas	Frecuencia	Porcentaje
Si	170	100%
No	0	0%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)

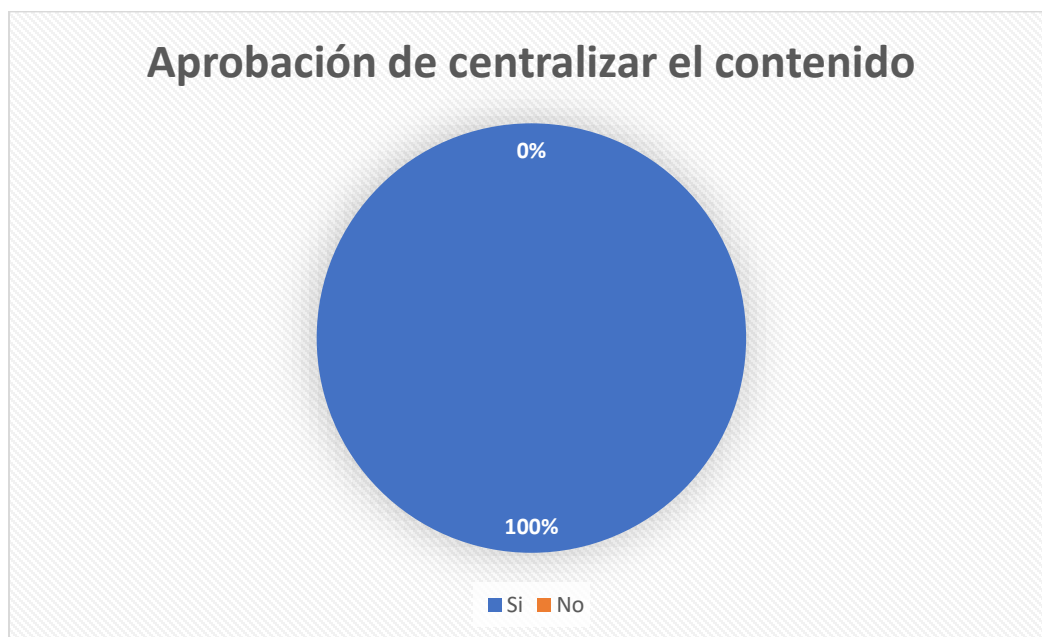


Figura 8. Aprobación de centralizar el contenido

Fuente: Elaboración Propia

Interpretación: De acuerdo con los datos, el 100% de las personas encuestadas, aprueban la importancia contar con una fuente centralizada de información accesible en todo momento a través de una plataforma de aprendizaje en línea

Pregunta No. 8 ¿Cree que el uso de una plataforma de aprendizaje en línea didáctica podría aumentar sus horas de estudio continuo al día?

Tabla 9. *Datos - Octava pregunta*

Respuestas	Frecuencia	Porcentaje
Si	152	89%
No	18	11%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)



Figura 9. Aumento de estudio en los estudiantes

Fuente: Elaboración Propia

Interpretación: Los resultados en esta gráfica indican que el 89% de la población encuestada aprueban que el uso de las plataformas de aprendizaje en línea podría aumentar sus horas de estudio continuo al día, mientras el 11% considera que no podría aumentar sus horas de estudio.

Pregunta No. 9 ¿Cuántas horas estaría dispuesto a invertir en el estudio autodidáctico a través de esta plataforma?

Tabla 10. *Datos - Novena pregunta*

Respuestas	Frecuencia	Porcentaje
2 horas al día	102	60%
3 horas al día	44	26%
4 horas al día	24	14%
Mas de 4 horas al día	0	0%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)

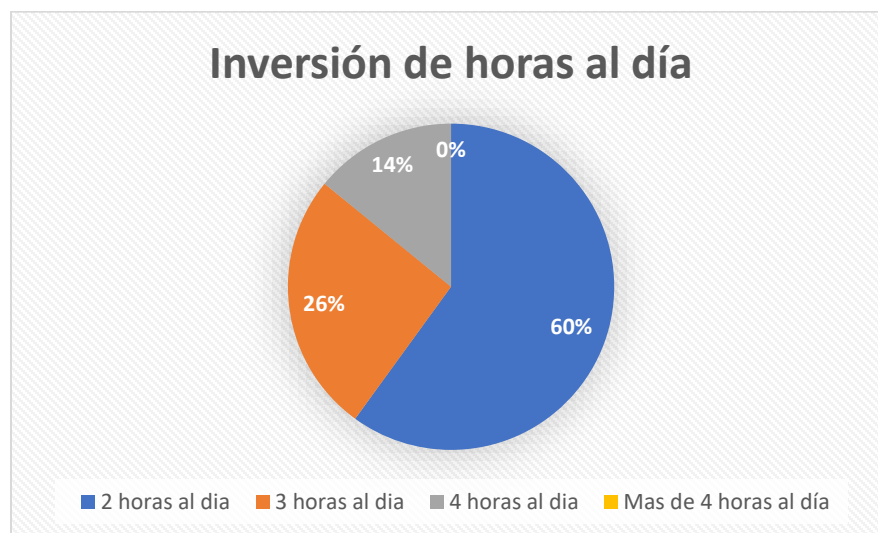


Figura 10. Inversión de horas al día

Fuente: Elaboración Propia

Interpretación: Según los datos obtenidos en la pregunta de selección múltiple, se observa que de las 170 personas que equivalen al 100% de la población tienen diferentes puntos de vista al estar dispuesto a invertir en el estudio autodidáctico a través de esta plataforma, se obtiene que el 60% que equivale a la mayoría de la población, piensan invertir 2 horas al día, el 26% piensa invertir 3 horas al día, mientras que el 14% piensa invertir 4 horas al día considerando que es el segundo horario más extenso y donde si hubo parte de la población que es el tiempo que invertiría.

Pregunta No. 10 ¿Considera que el uso de una plataforma de aprendizaje en línea podría ayudar a prevenir la búsqueda de recursos e información en fuentes no fidedignas, contribuyendo así a evitar la desinformación?

Tabla 11. *Datos - Decima pregunta*

Respuestas	Frecuencia	Porcentaje
Si	156	92%
No	14	8%
TOTAL	170	100%

Fuente: Datos obtenidos en el campo (Elaboración propia)

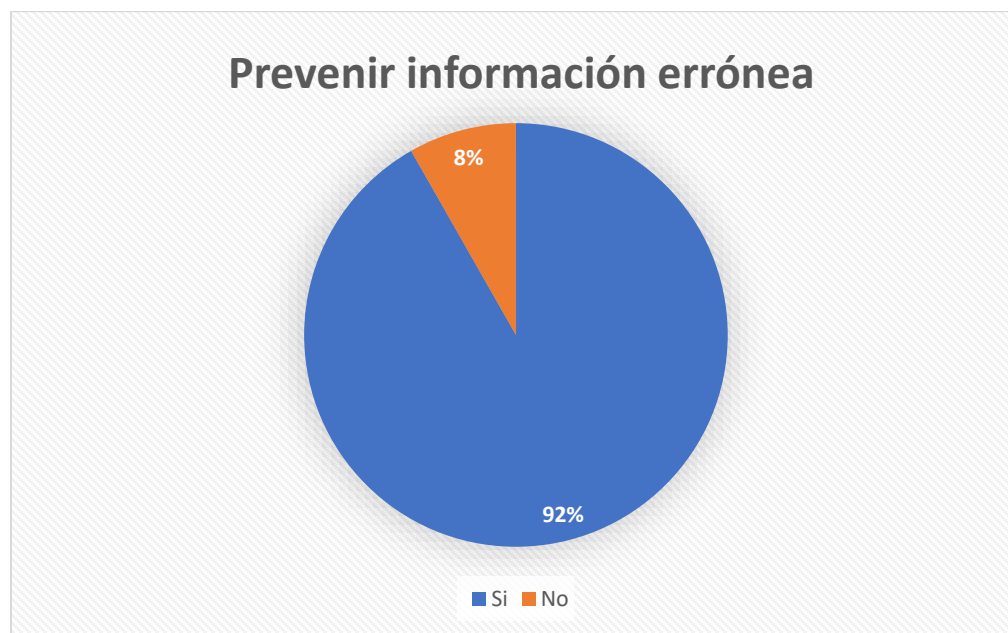


Figura 11. Prevenir información errónea

Fuente: Elaboración Propia

Interpretación: En los resultados de la siguiente gráfica se demuestra que las personas encuestadas consideran el uso de una plataforma de aprendizaje en línea podría ayudar a prevenir la búsqueda de recursos e información en fuentes no fidedignas, contribuyendo así a evitar la desinformación por lo tanto se observa que el 92% indica que, si es beneficioso, y el otro 8% indica que no sería beneficioso o no contribuye.

2.10 Prueba de Hipótesis

Se llevó a cabo una evaluación de hipótesis mediante la prueba de "Independencia Chi Cuadrada", utilizando tanto las Frecuencias Observadas (f_o) como las Frecuencias Esperadas (f_e) con respecto a la hipótesis nula, y con un nivel de significancia $\alpha = 0.05$, lo que representa una confianza del 95%. Esta evaluación permitió determinar si las hipótesis formuladas previamente como H_0 (Hipótesis Nula) y H_1 (Hipótesis Alternativa).

2.10.1 Frecuencias Observadas

Con el objetivo de evaluar la hipótesis, se seleccionaron únicamente cinco preguntas fundamentales de las diez que comprende el cuestionario utilizado para la encuesta y así obtener los datos necesarios de las frecuencias observadas. Cabe destacar que, en la tabla siguiente, se espera que la suma total de las columnas sea equivalente a la suma total de las filas.

Tabla 12. *Frecuencias Observadas*

Respuestas	Preguntas					Total de Filas
	P2	P4	P7	P8	P3	
Si	170	170	170	152	0	662
No	0	0	0	18	0	18
Muy buena	0	0	0	0	95	95
Aceptable	0	0	0	0	67	67
No tan agradable	0	0	0	0	8	8
Total de Columnas	170	170	170	170	170	850

Fuente: Elaboración propia

2.10.2 Frecuencia esperada

Esta frecuencia fue calculada con la fórmula siguiente:

$$f_e = \frac{TotalFilas(f_o) * TotalColumnas(f_o)}{TotalSuma(f_o)}$$

Se debe realizar una operación matemática para obtener el resultado deseado, la cual consiste en multiplicar el número total de filas en las frecuencias observadas por el número total de columnas, y luego dividir entre la suma total de ambos valores.

Tabla 13. *Frecuencias Esperadas*

Respuestas	Preguntas					Total de Filas
	P2	P4	P7	P8	P3	
Si	132.4	132.4	132.4	132.4	132.4	662
No	3.6	3.6	3.6	3.6	3.6	18
Muy buena	19	19	19	19	19	95
Aceptable	13.4	13.4	13.4	13.4	13.4	67
No tan agradable	1.6	1.6	1.6	1.6	1.6	8
Total de Columnas	170	170	170	170	170	850

Fuente: Elaboración propia

2.10.3 Distribución Chi-Cuadrado Calculado

Para el cálculo de la distribución Chi-Cuadrado Calculado se usa la siguiente fórmula.

$$x^2 = \sum \left[\frac{(f_o - f_e)^2}{f_e} \right]$$

Tabla 14. *Comprobación del Chi-Cuadrado*

f_0	f_e	$(f_0 - f_e)^2$	$(f_0 - f_e)^2 / f_e$
170	132.4	1413.76	10.67794562
0	3.6	12.96	3.6
0	19	361	19
0	13.4	179.56	13.4
0	1.6	2.56	1.6
170	132.4	1413.76	10.67794562
0	3.6	12.96	3.6
0	19	361	19
0	13.4	179.56	13.4
0	1.6	2.56	1.6
170	132.4	1413.76	10.67794562
0	3.6	12.96	3.6
0	19	361	19
0	13.4	179.56	13.4
0	1.6	2.56	1.6
152	132.4	384.16	2.901510574
18	3.6	207.36	57.6
0	19	361	19
0	13.4	179.56	13.4
0	1.6	2.56	1.6
0	132.4	17529.76	132.4
0	3.6	12.96	3.6
95	19	5776	304
67	13.4	2872.96	214.4
8	1.6	40.96	25.6
850	850	33276.8	$\Sigma = 919.335$

Fuente: Elaboración propia

Después de aplicar la fórmula a la mayoría de los datos, se obtiene la sumatoria total determinando el valor de Chi-Cuadrado Calculado, dicho valor es el siguiente:

$$\chi^2_{calc} = 919.335$$

2.10.4 Distribución Chi-Cuadrado Crítico

Para llevar a cabo una prueba de hipótesis, es esencial contar con el valor crítico del estadístico Chi-Cuadrado. Por lo tanto, el primer paso es calcular los grados de libertad (v) mediante la siguiente fórmula:

$$v = (\text{Cantidad de Filas} - 1) * (\text{Cantidad de Columnas} - 1)$$

Dónde los grados de libertad (v) son:

$$v = (5-1) * (5-1)$$

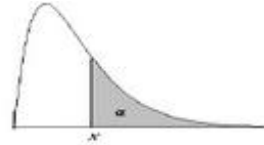
$$v = 4 * 4$$

$$v = 16$$

Después de calcular los grados de libertad, que en este caso es $v = 16$, y de establecer el nivel de significancia $\alpha = 0.05$, es posible determinar el valor crítico del estadístico Chi-Cuadrado (χ^2). Para hacerlo, se empleó una tabla de Distribución Chi-Cuadrado Crítico, que se presenta a continuación:

Tabla de la distribución chi-cuadrado.

La tabla contiene los valores x tales que $P[\chi^2 \geq x] = \alpha$ en función de los grados de libertad (n).



n	0.99	0.98	0.975	0.95	0.90	0.80	0.50	0.20	0.10	0.05	0.025	0.02	0.01	0.001
1	0.0002	0.0006	0.0010	0.0039	0.0158	0.0642	0.4549	1.6424	2.7055	3.8415	5.0239	5.4119	6.6349	10.8274
2	0.0201	0.0404	0.0506	0.1026	0.2107	0.4463	1.3863	3.2189	4.6052	5.9915	7.3778	7.8241	9.2104	13.8150
3	0.1148	0.1848	0.2158	0.3518	0.5844	1.0052	2.3660	4.6416	6.2514	7.8147	9.3484	9.8374	11.3449	16.2660
4	0.2971	0.4294	0.4844	0.7107	1.0636	1.6488	3.3567	5.9886	7.7794	9.4877	11.1433	11.6678	13.2767	18.4662
5	0.5543	0.7519	0.8312	1.1455	1.6103	2.3425	4.3515	7.2893	9.2363	11.0705	12.8325	13.3882	15.0863	20.5147
6	0.8721	1.1344	1.2373	1.6354	2.2041	3.0701	5.3481	8.5581	10.6446	12.5916	14.4494	15.0332	16.8119	22.4575
7	1.2390	1.5643	1.6899	2.1673	2.8331	3.8223	6.3458	9.8032	12.0170	14.0671	16.0128	16.6224	18.4753	24.3213
8	1.6465	2.0325	2.1797	2.7326	3.4895	4.5936	7.3441	11.0301	13.3616	15.5073	17.5345	18.1682	20.0902	26.1239
9	2.0879	2.5324	2.7004	3.3251	4.1682	5.3801	8.3428	12.2421	14.6837	16.9190	19.0228	19.6790	21.6660	27.8767
10	2.5582	3.0591	3.2470	3.9403	4.8652	6.1791	9.3418	13.4420	15.9872	18.3070	20.4832	21.1608	23.2093	29.5879
11	3.0535	3.6087	3.8157	4.5748	5.5778	6.9887	10.3410	14.6314	17.2750	19.6752	21.9200	22.6179	24.7250	31.2635
12	3.5706	4.1783	4.4038	5.2260	6.3038	7.8073	11.3403	15.8120	18.5493	21.0261	23.3367	24.0539	26.2170	32.9092
13	4.1069	4.7654	5.0087	5.8919	7.0415	8.6339	12.3398	16.9848	19.8119	22.3620	24.7356	25.4715	27.6882	34.5274
14	4.6604	5.3682	5.6287	6.5706	7.7895	9.4673	13.3393	18.1508	21.0641	23.6848	26.1189	26.8727	29.1412	36.1239
15	5.2294	5.9849	6.2621	7.2609	8.5468	10.3070	14.3389	19.3107	22.3071	24.9958	27.4884	28.2595	30.5780	37.6978
16	5.8122	6.6142	6.9077	7.9616	9.3122	11.1521	15.3385	20.4651	23.5418	26.2962	28.8453	29.6332	31.9999	39.2518
17	6.4077	7.2550	7.5642	8.6718	10.0852	12.0023	16.3382	21.6146	24.7690	27.5871	30.1910	30.9950	33.4087	40.7911
18	7.0149	7.9062	8.2307	9.3904	10.8649	12.8570	17.3379	22.7595	25.9894	28.8693	31.5264	32.3462	34.8052	42.3119
19	7.6327	8.5670	8.9065	10.1170	11.6509	13.7158	18.3376	23.9004	27.2036	30.1435	32.8523	33.6874	36.1908	43.8194
20	8.2604	9.2367	9.5908	10.8508	12.4426	14.5784	19.3374	25.0375	28.4120	31.4104	34.1696	35.0196	37.5663	45.3142
21	8.8972	9.9145	10.2829	11.5913	13.2396	15.4446	20.3372	26.1711	29.6151	32.6706	35.4789	36.3434	38.9322	46.7963
22	9.5425	10.6000	10.9823	12.3380	14.0415	16.3140	21.3370	27.3015	30.8133	33.9245	36.7807	37.6595	40.2894	48.2676
23	10.1957	11.2926	11.6885	13.0905	14.8480	17.1865	22.3369	28.4288	32.0069	35.1725	38.0756	38.9683	41.6383	49.7276
24	10.8563	11.9918	12.4011	13.8484	15.6587	18.0618	23.3367	29.5533	33.1962	36.4150	39.3641	40.2703	42.9798	51.1790
25	11.5240	12.6973	13.1197	14.6114	16.4734	18.9397	24.3366	30.6752	34.3816	37.6525	40.6465	41.5660	44.3140	52.6187
26	12.1982	13.4086	13.8439	15.3792	17.2919	19.8202	25.3365	31.7946	35.5632	38.8851	41.9231	42.8558	45.6416	54.0511
27	12.8785	14.1254	14.5734	16.1514	18.1139	20.7030	26.3363	32.9117	36.7412	40.1133	43.1945	44.1399	46.9628	55.4751
28	13.5647	14.8475	15.3079	16.9279	18.9392	21.5880	27.3362	34.0266	37.9159	41.3372	44.4608	45.4188	48.2782	56.8918
29	14.2564	15.5745	16.0471	17.7084	19.7677	22.4751	28.3361	35.1394	39.0875	42.5569	45.7223	46.6926	49.5878	58.3006
30	14.9535	16.3062	16.7908	18.4927	20.5992	23.3641	29.3360	36.2502	40.2560	43.7730	46.9792	47.9618	50.8922	59.7022

Figura 12. Tabla de Distribución Chi-Cuadrado

Fuente: <https://imgv2-2-f.scribdassets.com/img/document/59314560/original/28637af3fe/1678102567?v=1>

En este diagrama se observa que para la significancia de $\alpha = 0.05$ y 16 grados de libertad, se obtiene un valor crítico según la tabla de Distribución Chi-Cuadrado (X^2), dicho valor es:

$$X^2_{(0.05,20)} = 26.2962$$

2.10.5 Análisis de los Resultados

El cálculo de la prueba de Chi-Cuadrado nos ayuda a determinar si hay una relación significativa entre dos conjuntos de datos, en este caso nos proporciona los siguientes datos: el valor calculado de $X^2_{Calc} = 919.335$ y el valor crítico $X^2_{(0.05,16)} = 26.2962$. Con base a estos

resultados, se puede determinar que el valor calculado $>$ al valor crítico por lo que se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1).

$$919.335 > 26.2962$$

Los datos obtenidos muestran que el valor de la estadística de chi cuadrado obtenida es significativamente mayor que el valor crítico de chi cuadrado. En consecuencia, se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1), que sugiere que hay una relación significativa entre las variables categóricas analizadas. Estableciendo textualmente lo siguiente: *“La implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR, tiene un impacto significativo para los estudiantes o profesionales interesados en el área de SOC.”*

A partir de estos resultados, se considera que existe una base sólida para proceder con el desarrollo de la plataforma de aprendizaje SOC-CTIS-DFIR y se esperan resultados positivos en la siguiente fase del proyecto que será el Desarrollo del Proyecto.

CAPITULO III MARCO TEÓRICO

3.1 Incidente de Seguridad

Un incidente de seguridad, o suceso de seguridad, es cualquier infracción digital o física que amenace la confidencialidad, la integridad o la disponibilidad de los sistemas de información o datos confidenciales de una organización. Los incidentes de seguridad engloban desde ciberataques intencionales realizados por hackers o usuarios no autorizados, hasta violaciones no intencionadas de la política de seguridad por parte de usuarios legítimos autorizados. (IBM, 2022).

3.2 Inteligencia de Amenazas

La inteligencia de amenazas, también llamada "inteligencia de ciberamenazas" (CTI, por sus siglas en inglés) son datos con conocimientos detallados sobre las amenazas de ciberseguridad dirigidas a una organización. La inteligencia de amenazas ayuda a los equipos de seguridad a ser más proactivos, lo que les permite tomar medidas efectivas basadas en datos para impedir ciberataques antes de que ocurran. También puede ayudar a una organización a detectar y responder mejor a los ataques en curso. (IBM,2023).

3.3 APT (Advanced Persistent Threat)

Una amenaza persistente avanzada (APT) es un término amplio utilizado para describir una campaña de ataque en la que un intruso, o equipo de intrusos, establece un, presencia a largo plazo en una red para minar altamente datos sensibles.

Los objetivos de estos ataques, que se eligen e investigan con mucho cuidado, generalmente incluyen grandes empresas o redes gubernamentales. (Hasson, E. ,2023).

3.4 Firewall

Un firewall es un sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada.

Este software o esta unidad de hardware y software dedicados funciona bloqueando o permitiendo los paquetes de datos de forma selectiva. Normalmente, su finalidad es ayudar a prevenir la actividad maliciosa y evitar que cualquier persona (dentro o fuera de la red privada) pueda realizar actividades no autorizadas en la web. (Kaspersky, 2023).

3.5 IPS (Intrusion Prevention System)

Un sistema de prevención de intrusiones (IPS) es a seguridad de red herramienta (que puede ser un dispositivo de hardware o software) que monitorea continuamente una red en busca de actividad maliciosa y toma medidas para evitarla, incluidos los informes, el bloqueo o la caída, cuando ocurre. (VMware, 2023).

3.6 Phishing

Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o “suplanta su identidad”) a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. (Malwarebytes, 2019).

3.7 SOC Analyst

Un/a analista SOC, también conocido/a como analista del centro de operaciones de seguridad, es un/a especialista en ciberseguridad a cargo de rastrear y abordar las amenazas informáticas dentro de una organización. Su deber principal es proteger la confidencialidad e integridad de la información corporativa. Para garantizar la defensa contra posibles amenazas, un/a SOC Analyst colabora estrechamente con otros/as profesionales de ciberseguridad. (Page, M., 2023).

3.8 IOC (Indicators of Compromise)

Los indicadores de riesgo (IoC) son información sobre un fallo de seguridad concreto que puede ayudar a los equipos de seguridad a determinar si se ha producido un ataque. Estos datos pueden incluir detalles sobre el ataque, como el tipo de malware utilizado, las direcciones IP implicadas y otros detalles técnicos. (Cloudflare, 2023).

3.9 VPN (Virtual Private Network)

Una VPN (Virtual Private Network) o red privada virtual es una conexión segura y privada a través de una red no confiable como Internet para acceder de manera remota a los sistemas o red de una organización. Se trata de una conexión privada porque se utilizan protocolos de cifrado y encapsulamiento para asegurar la confidencialidad e integridad de los datos transmitidos. Es importante remarcar que la tecnología VPN necesita un túnel cifrado para funcionar de manera segura y que los datos no puedan ser accedidos por personas no autorizadas o terceros (ataques Man in the Middle). (Unir, V. ,2022)

3.10 Ransomware

El ransomware es un tipo de malware que bloquea los datos o dispositivos de una víctima y amenaza con mantenerlos bloqueados, a menos que la víctima pague un rescate al atacante. Según el IBM Security X-Force Threat Intelligence Index 2023, los ataques de ransomware representaron el 17 por ciento de todos los ciberataques en 2022. (IBM, s.f)

3.11 Ciberseguridad

La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir la normativa. Utilizan medidas y herramientas de ciberseguridad para proteger los datos confidenciales del acceso no autorizado, así como para evitar interrupciones en las operaciones empresariales debido a una actividad de red

no deseada. Las organizaciones implementan la ciberseguridad al optimizar la defensa digital entre las personas, los procesos y las tecnologías. (AWS, s.f)

3.12 EDR (Endpoint Detection and Response)

Detección y Respuesta de Punto Final (EDR), también conocida como detección de punto final y respuesta a amenazas (EDTR), es una solución de seguridad de punto final que monitorea continuamente los dispositivos del usuario final para detectar y responder a amenazas cibernéticas como ransomware y malware. (CrowdStrike, 2023)

3.13 Gestión de Eventos

La gestión de eventos es la actividad profesional de planificación, organización y dirección de eventos a pequeña y gran escala -ya sea en persona, de manera virtual o con una combinación de ambas- que recurre a un conjunto de expertos capacitados para llevarse a cabo. (Esdai, s.f).

3.14 Ciberdefensa

Ciberdefensa el conjunto de operaciones activas o pasivas utilizadas por el Estado para garantizar la seguridad y el uso adecuado del ámbito digital de un país, a la vez que lo protege de amenazas como las descritas previamente. Sin embargo, la ciberdefensa se puede confundir con la ciberseguridad, puesto que a priori ambas parecen aludir a la protección de un espacio virtual o cibernético. (Herrero, E. ,2023)

3.15 Relaciones B2B

El B2B es el acrónimo de Business-To-Business que se puede traducir al español como empresa a empresa. Se trata de un modelo de negocio en el que una compañía ofrecerá sus servicios a otra, con el propósito de mejorar los beneficios de sus ventas y bienes. (Vega, M,2023)

3.16 Capturas de Paquetes

La captura de paquetes implica capturar los paquetes de datos sin procesar que se envían y reciben a través de una red. Estos paquetes contienen información como las direcciones IP de origen y destino, los protocolos utilizados y los datos de carga útil. Al capturar estos paquetes, los profesionales de TI pueden analizar el tráfico de la red y comprender cómo se transmiten los datos. (TS2 Space, 2023)

3.17 PowerShell

En la tecnología de la información, este término hace referencia a una interfaz entre un ordenador y su usuario. El término inglés "shell" significa, literalmente, "concha" pero en sentido figurado se utiliza para describir una "carcasa exterior". En informática, este término se refiere a la interfaz de usuario visible a través de la cual se puede interactuar con las funciones internas del sistema en un ordenador.

Las shells suelen estar orientadas a comandos y, por lo tanto, se controlan exclusivamente con el teclado y la entrada de texto. Son una alternativa a las interfaces gráficas de usuario (GUI) en las que se navega principalmente con el ratón, como el Explorador de Windows. Dado que las shells también proporcionan acceso a un número mayor y más profundo de funciones y componentes del PC, son los preferidos por muchos profesionales de TI y administradores de sistemas. (Equipo editorial de IONOS, 2023)

3.18 Hash

Una función criptográfica hash- usualmente conocida como "hash"- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud. (Donohue, 2021)

3.19 VirusTotal

Virus Total es un sitio web que proporciona de forma gratuita el análisis de archivos y páginas web a través de un antivirus. Creada por la empresa de seguridad española Hispasec Sistemas incluye 55 antivirus y 61 motores de detección en línea para su análisis. (colaboradores de Wikipedia, 2023)

3.20 Directiva de seguridad local

La directiva de seguridad local de un sistema es un conjunto de información sobre la seguridad de un equipo local. La información de la directiva de seguridad local incluye, dominios de confianza para autenticar intentos de inicio de sesión, qué cuentas de usuario pueden acceder al sistema y cómo (forma interactiva, a través de una red o como servicio), derechos y privilegios asignados a las cuentas. Directiva de auditoría de seguridad. (Alvinashcraft, 2023).

3.21 Administrador

Un administrador es la persona que se ocupa de realizar la tarea administrativa por medio de la planificación, organización, dirección y control de todas las tareas dentro de un grupo social o de una organización para lograr los objetivos mediante el uso eficiente de los recursos. (Quiroa, 2022)

3.22 Firewall

Un firewall es un sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada.

Este software o esta unidad de hardware y software dedicados funciona bloqueando o permitiendo los paquetes de datos de forma selectiva. Normalmente, su finalidad es ayudar a prevenir la actividad maliciosa y evitar que cualquier persona (dentro o fuera de la red privada) pueda realizar actividades no autorizadas en la web. (¿Qué Es Un Firewall? Definición Y Explicación, 2023).

3.23 Windows Defender

Windows Defender es un antivirus fundamental para los usuarios del sistema operativo de Microsoft. Viene integrado, es gratuito y además cuenta con muchas funciones interesantes. Una de ellas es la de protección en tiempo real. Esto es algo que, como hemos comentado, es muy útil para evitar problemas que puedan poner en riesgo nuestros equipos. (Jiménez, 2023)

3.24 Puerto USB

Puerto es una noción con varios usos. En la informática, el término se emplea para nombrar a una clase de conexión que posibilita el envío y la recepción de información. USB, por su parte, es la sigla correspondiente a Universal Serial Bus, una interfaz que permite la conexión de periféricos a diversos dispositivos, entre los cuales se encuentran los ordenadores y los teléfonos móviles. (Porto & Gardey, 2021)

3.25 Regedit

Regedit es el editor del registro de Windows, una herramienta gráfica que le permite ver y supervisar el registro del sistema operativo de Windows y editarlo si es necesario. Regedit le permite hacer cambios a nivel raíz y administrativo en su ordenador y en los ajustes de configuración de las aplicaciones conectadas al registro, por lo que debería tener mucho cuidado al utilizarlo. (Freda, 2023)

3.26 Ransomware WannaCry

WannaCry es un ejemplo de ransomware de cifrado, un tipo de software malicioso (malware) que los cibercriminales utilizan a fin de extorsionar a un usuario para que pague. El ransomware ataca cifrando archivos valiosos para que no puedas acceder a ellos, o bien bloqueando tu acceso al ordenador para que no puedas utilizarlo. (¿Qué Es El Ransomware WannaCry?, 2023)

3.27 Ransomware Petya

Petya es una variedad de ransomware que se identificó por primera vez en 2016. Al igual que otros tipos de ransomware, Petya encripta los archivos y datos en el ordenador de la víctima. Los operadores de Petya exigen un pago en Bitcoin antes de desencriptar los archivos y hacer que se puedan usar de nuevo.

A diferencia de las variedades de ransomware más antiguas, que solo encriptan determinados archivos importantes para extorsionar a la víctima, Petya bloquea todo el disco duro de un ordenador. En concreto, encripta la Tabla de archivos maestros (MFT) de un ordenador, lo cual hace imposible el acceso a cualquier archivo del disco duro. (Cloudflare, n.d.)

3.28 Ransomware NotPetya

En junio de 2017, un nuevo tipo de ransomware que era similar a Petya en muchos aspectos infectó a organizaciones de todo el mundo. Debido a sus similitudes con Petya, aunque tenía algunas diferencias importantes, el proveedor de seguridad Kaspersky lo denominó "NotPetya." NotPetya había afectado al menos a 2000 organizaciones hasta el 28 de junio de 2017. La gran mayoría de las organizaciones afectadas estaban en Ucrania.

Al igual que Petya, el ransomware NotPetya afectaba a todo el disco duro de la víctima. Sin embargo, NotPetya encriptaba todo el disco duro en lugar de la MFT. Se extendió de forma rápida y repentina, e infectó rápidamente redes enteras aprovechándose de vulnerabilidades y haciendo uso de métodos de robo de credenciales. (Cloudflare, n.d.)

3.29 Gestión de parches

La gestión de parches es el proceso de aplicar actualizaciones emitidas por proveedores para resolver vulnerabilidades de seguridad y optimizar el rendimiento de software y dispositivos. La gestión de parches a veces se considera parte de la gestión de vulnerabilidades. En la práctica, la gestión de parches consiste en ajustar la ciberseguridad a las necesidades operativas del negocio.

Los hackers pueden explotar vulnerabilidades en el entorno de TI de una empresa para iniciar ciberataques y dispersar malware. Los proveedores publican actualizaciones, llamadas "parches", para corregir estas vulnerabilidades. Sin embargo, el proceso de aplicación de parches puede interrumpir los flujos de trabajo y provocar tiempo de inactividad para el negocio. La gestión de parches tiene como objetivo minimizar ese tiempo de inactividad mediante la optimización del despliegue de parches. (IBM, 2023)

3.30 Actualizaciones de software

Las actualizaciones de software (también conocidas como parches) son fragmentos adicionales de software publicados por quienes producen los sistemas operativos y programas que usan nuestros equipos con el fin de mejorarlos. Estas actualizaciones se instalan sobre el software actual del dispositivo y no suelen requerir que se instalen los programas desde cero. (idearius, 2022)

3.31 Copias de seguridad

En el sentido más académico, una copia de seguridad es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos. Sin embargo, en el ámbito empresarial podríamos definir la copia de seguridad como la salvaguarda de nuestro negocio, una medida indispensable para garantizar su continuidad y conservar la confianza que nuestros clientes han depositado en nuestra organización. De lo contrario, podríamos proyectar una imagen negativa y generar desconfianza. (INCIBE, 2018)

3.32 Respuesta a incidentes

Se refiere a los procesos y tecnologías de una organización para detectar y responder a ciberamenazas, brechas de seguridad o ciberataques. El objetivo de la respuesta a incidentes es evitar ciberataques antes de que se produzcan y minimizar el coste y la interrupción del negocio asociados a los ciberataques que lleguen a producirse. Idealmente, una organización define los procesos y las tecnologías de respuesta a incidentes en un plan de respuesta a incidentes (IRP) formal que especifica exactamente cómo se deben identificar, contener y resolver los diferentes tipos de ciberataques. (IBM, 2021)

3.33 Prueba de penetración

Una prueba de penetración, o "pen test", es una prueba de seguridad que lanza un ciberataque simulado para encontrar vulnerabilidades en un sistema informático. Los evaluadores de penetración son profesionales de seguridad expertos en el arte del hackeo ético, que es el uso de herramientas y técnicas de hackeo para corregir las debilidades de seguridad en lugar de causar daños. Las empresas contratan evaluadores de penetración para lanzar ataques simulados contra sus aplicaciones, redes y otros activos. Al organizar ataques falsos, los evaluadores de penetración ayudan equipos de seguridad a descubrir vulnerabilidades de seguridad críticas y mejorar la posición general de seguridad. (IBM, 2021)

3.34 Filtración de datos

Una filtración de datos es un incidente de seguridad en que usuarios internos malintencionados o atacantes externos obtienen acceso no autorizado a datos confidenciales o información sensible como historias clínicas, información financiera o información de identificación personal (PII). Las filtraciones de datos son uno de los tipos de incidentes de ciberseguridad más comunes y costosos. Afectan a empresas de todos los tamaños, industrias y geografías, etc. y se producen con una regularidad alarmante. (CYBERARK, 2019)

3.35 Resiliencia cibernética

La resiliencia cibernética es un concepto que aúna la continuidad del negocio, la seguridad de los sistemas de información y la resiliencia organizacional. Es decir, el concepto describe la capacidad de seguir ofreciendo resultados previstos a pesar de experimentar eventos cibernéticos desafiantes, como ciberataques, desastres naturales o ataques económicos. Un nivel medido de competencia y resiliencia en la seguridad de la información afecta al grado en que una organización puede continuar las operaciones empresariales con poco o ningún tiempo de inactividad, en otras palabras. (IBM, 2021)

3.36 Indicador de compromiso

Un Indicador de compromiso (IOC) es un conjunto de datos sobre un objeto o una actividad que indica acceso no autorizado al equipo (compromiso de datos). Por ejemplo, muchos intentos fallidos de iniciar sesión en el sistema pueden constituir un indicador de compromiso. La tarea Análisis de IOC permite encontrar indicadores de compromiso en el equipo y tomar medidas de respuesta ante amenazas. (Kaspersky, 2023)

3.37 Stakeholders

Un stakeholder es el público de interés para una empresa que permite su completo funcionamiento. Con público, me refiero a todas las personas u organizaciones que se relacionan con las actividades y decisiones de una empresa como: empleados, proveedores, clientes, gobierno, entre otros. (Rockcontent, 2019)

3.38 Marco de ciberseguridad del NIST

El Instituto Nacional de Estándares y Tecnología (NIST) es una agencia no reguladora que promueve la innovación mediante el fomento de la ciencia, los estándares y la tecnología de la medición. El marco de ciberseguridad del NIST (CSF del NIST) consta de estándares, pautas y mejores prácticas que ayudan a las organizaciones a mejorar su gestión de riesgos de ciberseguridad. El diseño del CSF del NIST tiene una flexibilidad que le permite integrarse con los procesos de seguridad existentes dentro de cualquier organización, en cualquier industria. Proporciona un excelente punto de partida para implementar la seguridad de la información y la gestión de riesgos de ciberseguridad en prácticamente cualquier organización del sector privado en los Estados Unidos. (IBM, 2021)

CAPITULO IV DESARROLLO DEL PROYECTO

4.1 Plugins utilizados

4.1.1 Edubin Core

Edubin para WordPress. Perfecto para cursos en línea, universidad, colegio, escuela, centro de formación y otros institutos.

Este plugin, que prácticamente es un tema es todo lo visual dentro de nuestra plataforma, este tema nos permite integrar muchas plantillas la cual se escogió una de ellas y se armó de acuerdo con las páginas prediseñadas.

4.1.2 Tutor LMS Pro

Tutor LMS es un plugin WordPress LMS completo, repleto de funciones y robusto para crear y vender fácilmente cursos en línea. Todas las características de este sistema de gestión de aprendizaje golpean todos los puntos de control para un mercado de cursos en línea de pleno derecho.

Este es el plugin central, el que utilizamos para montar la plataforma de cursos, en este plugin creamos los perfiles de estudiantes, tutores, cursos, lecciones, exámenes y asignaciones, este plugin es lo que hace funcionar nuestra plataforma de aprendizaje online.

4.1.3 All-in-One WP Migration

All-in-One WP Migration viene cargado con funciones fáciles de usar que le permiten migrar su sitio web de WordPress con poco o ningún conocimiento técnico o experiencia.

Este plugin fue utilizado para hacer copias de seguridad de todo el sitio web, incluyendo funcionalidades plugin y toda interfaz de WordPress.

4.1.4 Dynamic Visibility for Elementor

La extensión Dynamic Visibility le permite ocultar widgets, columnas, contenedores, secciones o páginas.

Es particularmente útil cuando estás construyendo algo que no quieres mostrar a todo el mundo.

Este plugin fue utilizado en su mayoría para ocultar elementos, como botones, y algunas opciones del menú principal, para roles de usuarios logueados y no logueados.

4.1.5 Elementor

Elementor es un popular plugin para WordPress que permite la creación y personalización visual de páginas web mediante un editor de arrastrar y soltar. Con Elementor, los usuarios pueden diseñar páginas sin necesidad de conocimientos de código, lo que facilita la creación de sitios web de manera intuitiva y eficiente.

Este plugin fue de los principales para maquetar el sitio web, se utilizó para editar todas las páginas predefinidas y opciones como creación de formularios y ajustes de inicio.

4.1.6 PRO Elements

PRO Elements es una obra derivada del plugin para WordPress Elementor Pro de Elementor Ltd. Al igual que el original, está licenciado bajo la Licencia Pública General GNU, versión 3 (GPLv3).

Pero a diferencia del original, es 100% gratuito y no requiere activación para su uso.

Este al igual que elementor fue utilizado para maquetar el sitio, pero a diferencia del anterior mencionado solo fue requerido para utilizar algunas funcionalidades que están de paga en elementor.

4.1.7 The Events Calendar

Crea y gestiona fácilmente un calendario de eventos en tu sitio WordPress con el plugin gratuito The Events Calendar. Tanto si tus eventos son presenciales como virtuales, este plugin de calendario para WordPress cuenta con funciones profesionales respaldadas por nuestro equipo de desarrolladores y diseñadores de primer nivel.

Este plugin fue utilizado para darle una parte más atractiva a una sección de Tutor LMS que se llama integración por calendario, el cual al integrar este plugin muestra todos los eventos pendientes, desde tareas y exámenes asignados.

4.1.8 Tutor LMS Elementor Addons

Tutor LMS Elementor Addons es un plugin para WordPress que sincroniza Tutor LMS con el constructor de páginas Elementor. Le ayuda a diseñar sitios de cursos eLearning de la forma que desee. Cree su propio diseño y estilo personalizados para los cursos de Tutor LMS, añada diferentes diseños a cursos específicos, cree carruseles y listados de cursos y mucho más.

Al igual que Elementor se utilizó para diseñar el header y parte del sitio web, también para editar cosas premium que Elementor no nos ofrece.

4.1.9 WPForms Lite

WPForms, un constructor de formularios de WordPress de arrastrar y soltar que es fácil y ponente.

Este plugin fue utilizado para diseñar el formulario de contacto, y fue implementado en la plataforma en la sección de “contáctanos”

4.1.10 WP Super Cache

Este plugin crea archivos html estáticos de tu sitio WordPress dinámico. Una vez se haya creado el archivo html tu servidor servirá ese archivo en vez de procesar los scripts PHP de WordPress, en comparación mucho más pesados y consumidores de recursos.

Este plugin es encargado de optimizar la carga del sitio web al crear html estáticos y optimizar el sitio para aquellos visitantes casuales que no se registren.

4.2 Herramientas

4.2.1 WordPress

WordPress es un sistema de gestión de contenidos web (CMS o content management system), que en pocas palabras es un sistema para publicar contenido en la web de forma sencilla.

Utilizamos wordpress para montar todo el contenido dentro de nuestra plataforma de aprendizaje así para la instalación de plugins y temas y permitirnos administrarlo de forma rápida y didáctica

4.2.2 Hostinger

Hostinger es una alternativa para quienes desean contratar un servicio de hosting compartido. Sus servidores funcionan tanto para pequeñas como grandes empresas. Permite que desarrolles tu propio sitio sin amplia experiencia y con menos recursos que la competencia.

Utilizamos Hostinger para subir WordPress y luego instalarlo, así podremos tener el sitio tener una plataforma adaptable para todo público y con el objetivo que la experiencia y rendimiento sea buena.

Tabla 15. *Versión de Plugins utilizados*

Plugins	Versiones
Wordpress	6.4.1
Edubin Core	8.14.24
Tutor LMS Pro	2.4.0
All-in-One WP Migration	7.79
Dynamic Visibility	5.0.10
Elementor	3.16.6
PRO Elements	3.16.2
The Events Calendar	6.2.4
Tutor LMS Elementor	2.1.3
WPForms Lite	1.8.4.1
WP Super Cache	1.11.0

Fuente: (Elaboración propia)

4.3 Desarrollo de la plataforma

4.3.1 Dashboard

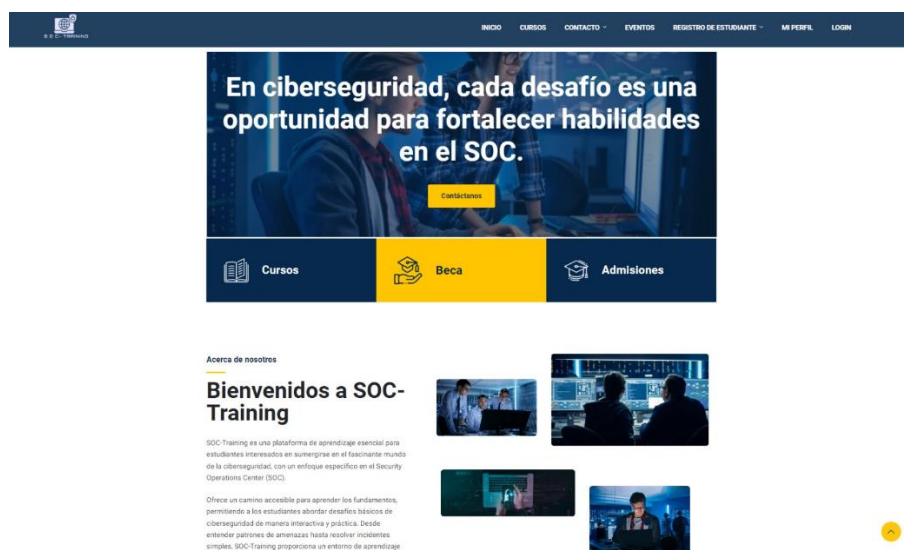


Figura 13. Dashboard

Fuente: Elaboración Propia

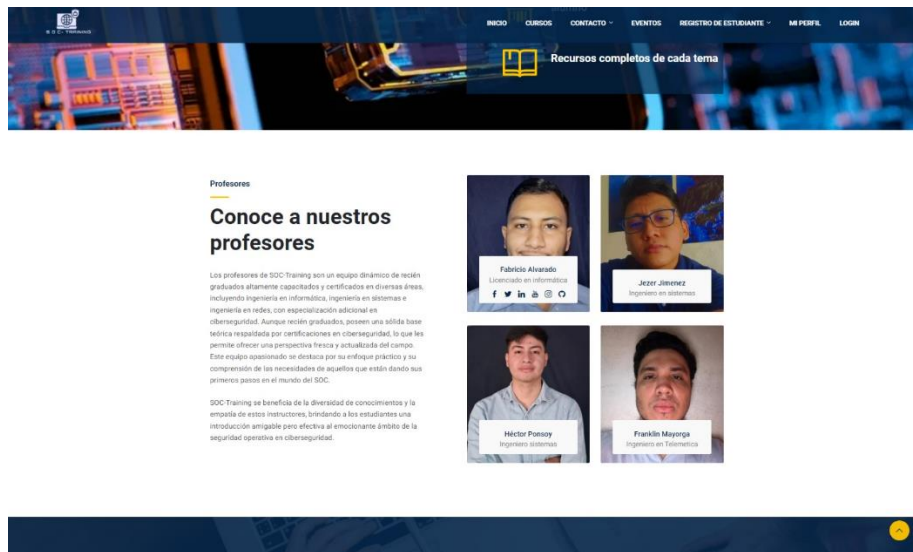


Figura 14. Dashboard 2

Fuente: Elaboración Propia

4.3.2 Footer



Figura 15. Footer

Fuente: Elaboración Propia

4.3.3 Cursos

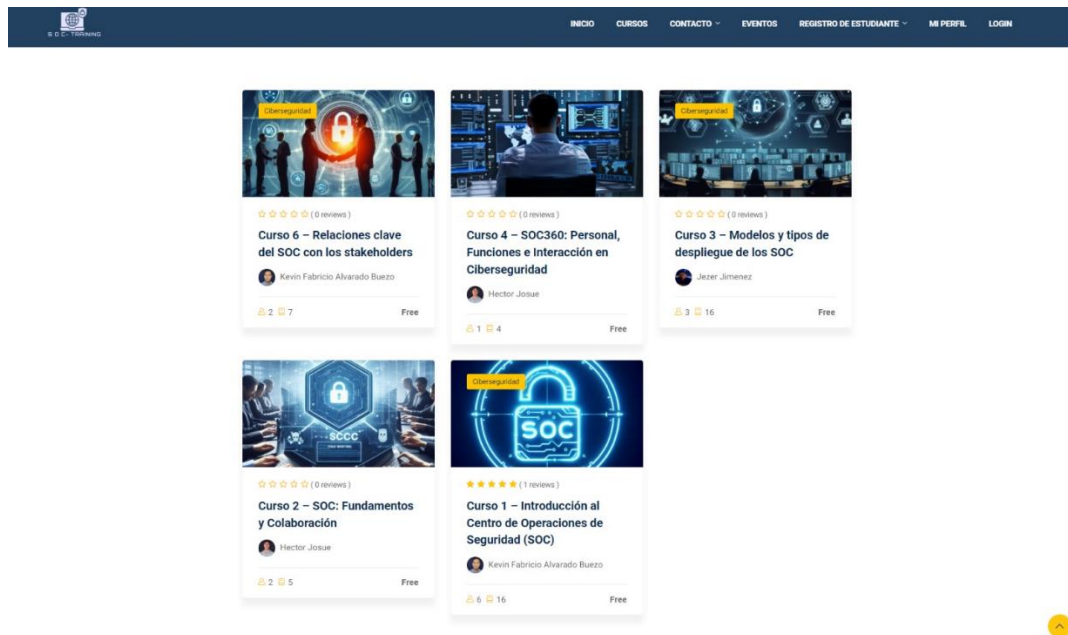


Figura 16. Cursos parte 1

Fuente: Elaboración Propia

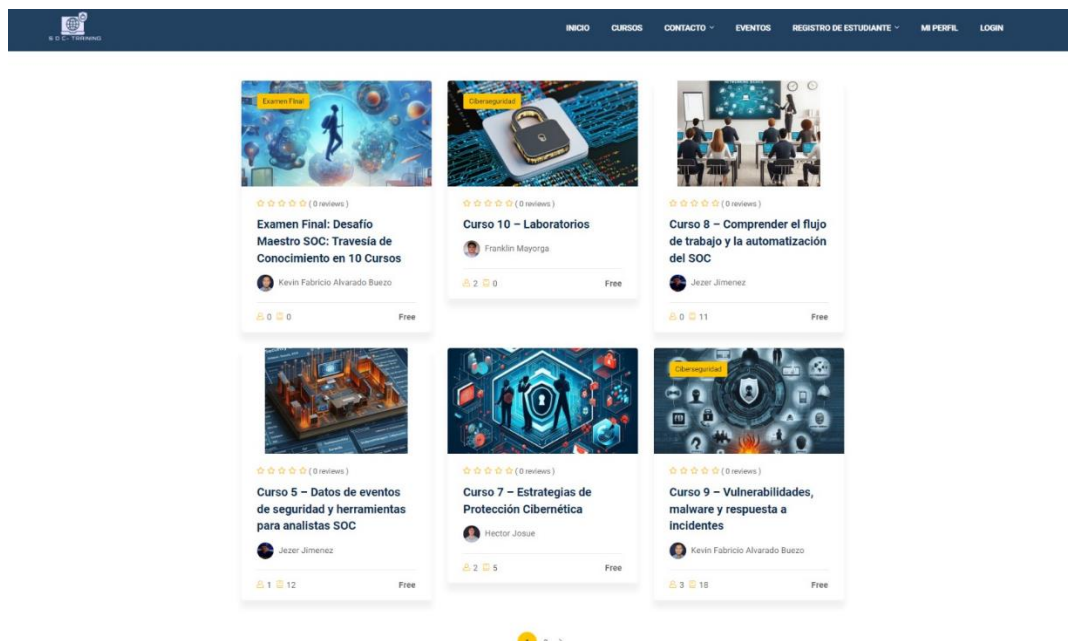


Figura 17. Cursos parte 2

Fuente: Elaboración Propia

4.3.4 Contacto sobre nosotros



Figura 18. Sobre nosotros parte 1

Fuente: Elaboración Propia



Figura 19. Sobre nosotros parte 2

Fuente: Elaboración Propia

4.3.5 Sección de Eventos

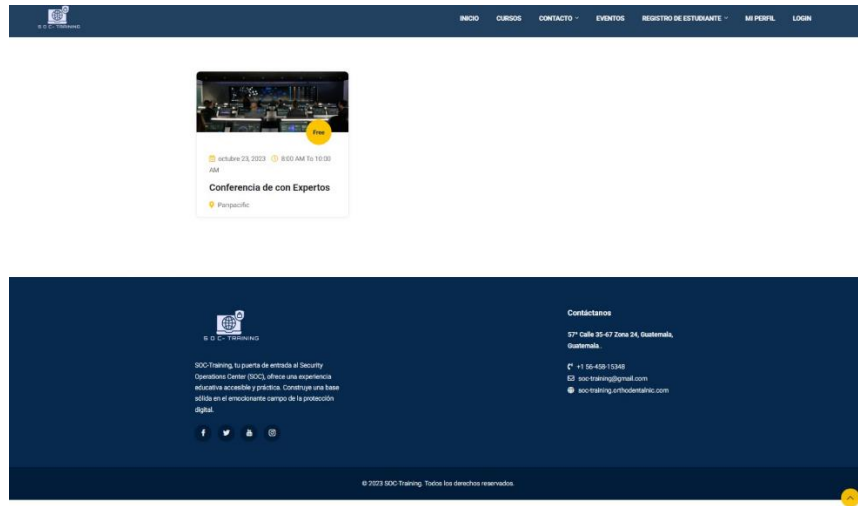


Figura 20. Sección de Eventos

Fuente: Elaboración Propia

4.3.6 Registro para estudiante

Figura 21. Registro para estudiante

Fuente: Elaboración Propia

4.3.7 Sección de Mi perfil

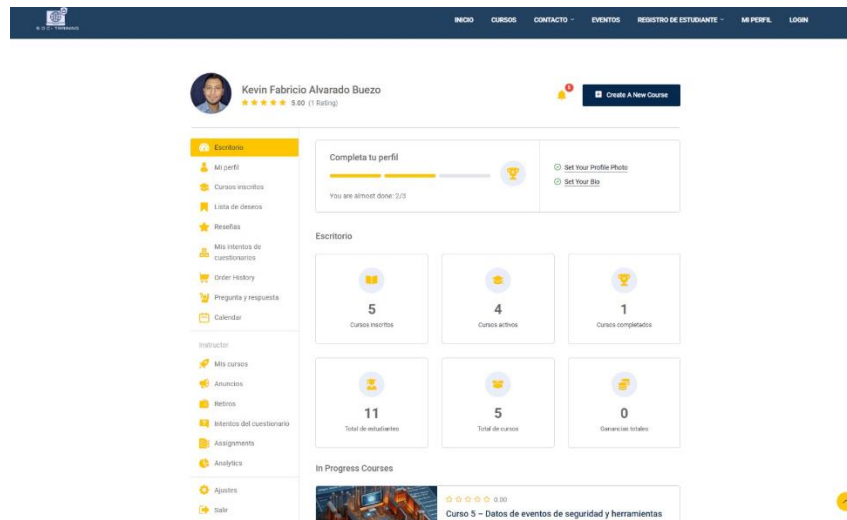


Figura 22. Sección de mi perfil

Fuente: Elaboración Propia

4.3.8 Sección de login

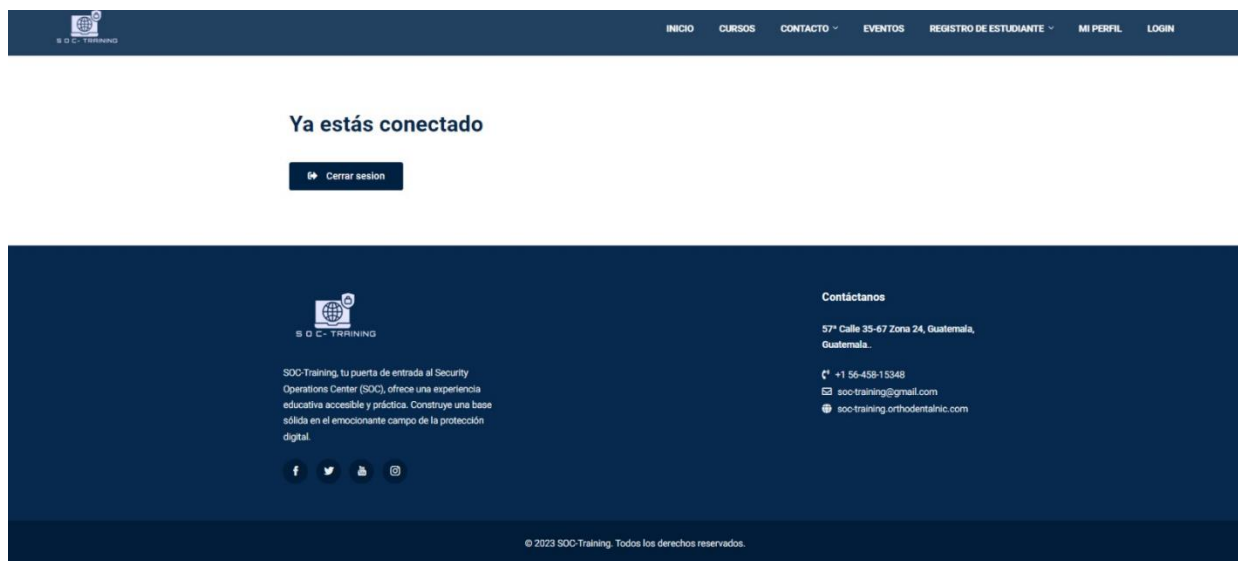
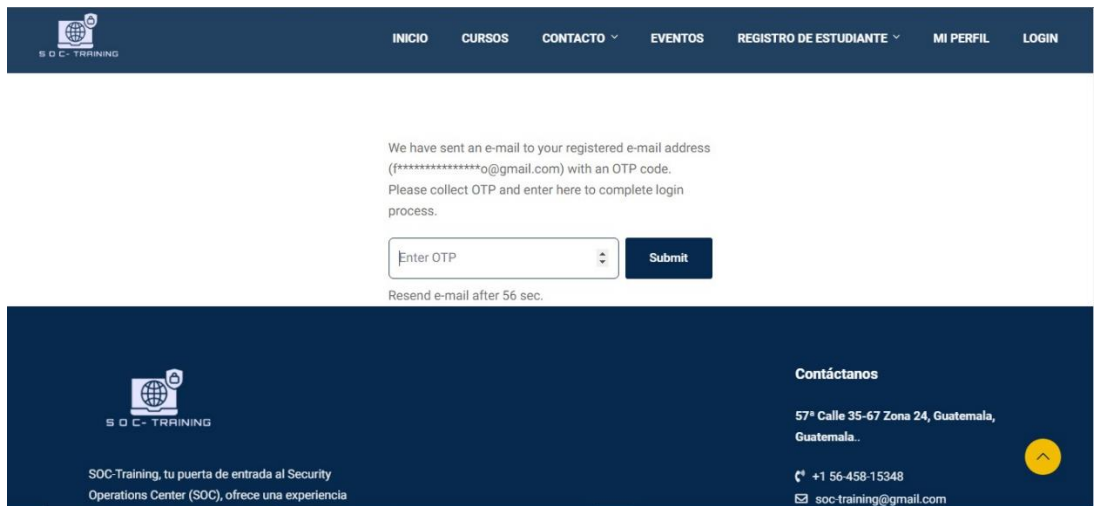


Figura 23. Sección de login

Fuente: Elaboración Propia

4.3.9 Login con OTP



The screenshot shows the SOC-TRAINING website's login interface. At the top is a dark blue navigation bar with the logo and menu items: INICIO, CURSOS, CONTACTO, EVENTOS, REGISTRO DE ESTUDIANTE, MI PERFIL, and LOGIN. The main content area has a white background with the following text: "We have sent an e-mail to your registered e-mail address (*****o@gmail.com) with an OTP code. Please collect OTP and enter here to complete login process." Below this is a text input field labeled "Enter OTP" and a dark blue "Submit" button. A link "Resend e-mail after 56 sec." is positioned below the input field. The footer is a dark blue bar containing the SOC-TRAINING logo, a description of the service, and contact information: "Contáctanos", "57ª Calle 35-67 Zona 24, Guatemala, Guatemala.", "+1 56-458-15348", and "soc-training@gmail.com". A yellow circular button with an upward arrow is also present in the footer.

Figura 24. Login con OTP

Fuente: Elaboración Propia

4.3.10 Correo electrónico con la clave OTP

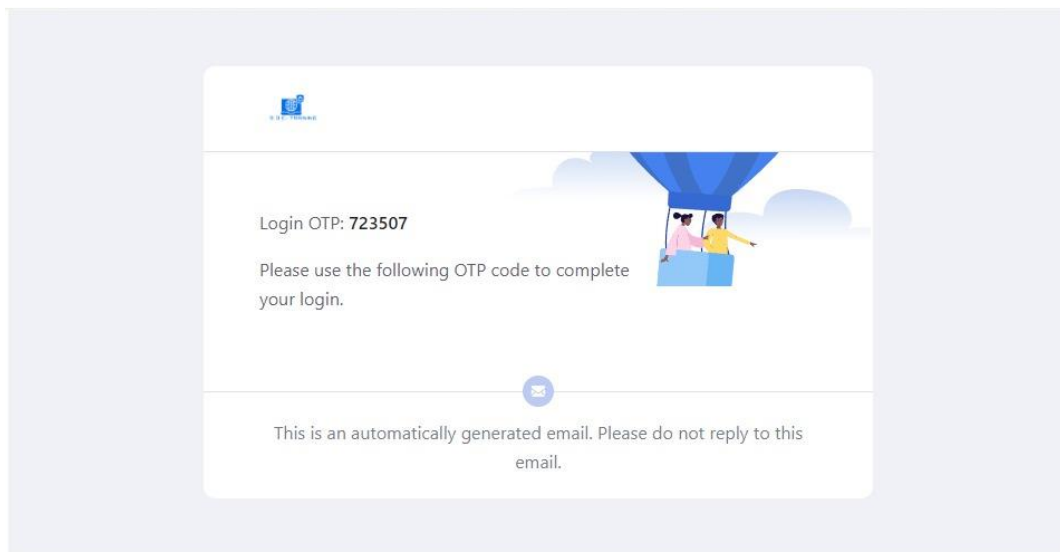
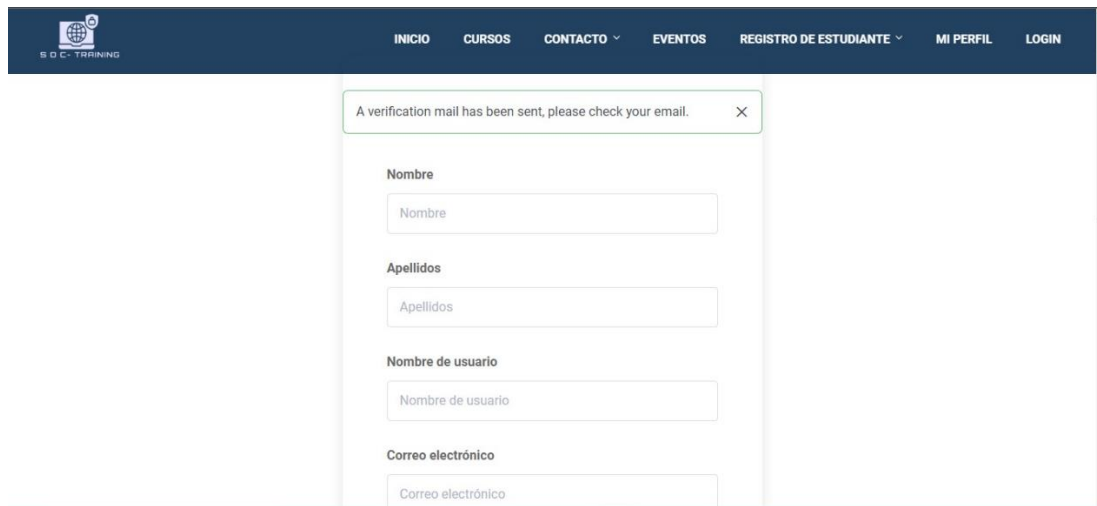


Figura 25. Correo electrónico con la clave OTP

Fuente: Elaboración Propia

4.3.11 Formulario de Registro de confirmación de correo electrónico



A verification mail has been sent, please check your email. X

Nombre

Apellidos

Nombre de usuario

Correo electrónico

Figura 26. Formulario de Registro de confirmación de correo electrónico

Fuente: Elaboración Propia

4.3.12 Correo electrónico con el enlace de confirmación

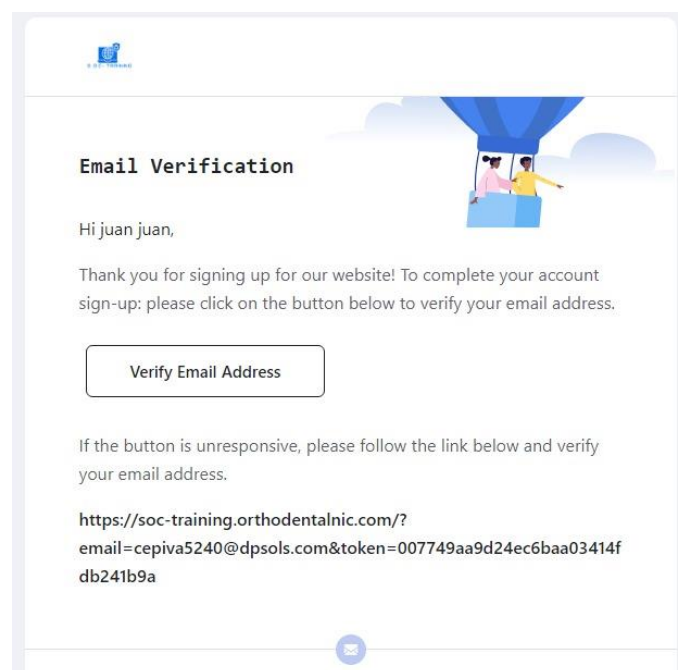


Figura 27. Correo electrónico con el enlace de confirmación

Fuente: Elaboración Propia

4.4 Guía educativa

4.4.1 Curso 1 – Introducción al Centro de Operaciones de Seguridad (SOC)



Figura 28. Curso 1

Fuente: Elaboración Propia

4.4.1.1 Descripción del curso

El curso Fundamentos del Centro de operaciones de seguridad (SOC) es ideal para profesionales que desean una comprensión más profunda de las capacidades y procesos de SOC, así como para aquellos interesados en una carrera en ciberseguridad. No se requieren conocimientos previos de seguridad cibernética ya que el curso proporcionará una base sólida para comprender los aspectos fundamentales del SOC y su importancia en la protección de una organización contra las amenazas cibernéticas.

4.4.1.2 Modulo #1 Introducción al Centro de Operaciones de Seguridad

Lección #1 Introducción al Centro de Operaciones de Seguridad

Lección #2 ¿Qué es un centro de operaciones (SOC)?

Lección #3 Centro de Operaciones de Seguridad (SOC) en una empresa
Cuestionario

4.4.1.3 Modulo #2 Fundamentos de SOC

Lección #1 Fundamentos de SOC
Lección #2 Gestión de eventos
Lección #3 ¿Qué es la gestión de eventos en SOC?
Lección #4 Respuesta a incidentes
Lección #5 Ciberdefensa
Cuestionario

4.4.1.4 Modulo #3 ¿Qué es el SOC?

Lección #1 ¿Qué es el SOC?
Lección #2 Que actividades realiza un Centro de Operaciones de Seguridad (SOC)
Lección #3 Funciones del centro de operaciones de seguridad (SOC)
Lección #4 ¿Cómo funciona un SOC?
Lección #5 Beneficios de contar con un SOC
Lección #6 Organización del SOC
Lección #7 Miembros clave del equipo del Centro de operaciones de seguridad (SOC)
Cuestionario

4.4.1.5 Modulo #4 SOC Medio ambiente hoy

Lección #1 SOC Medio ambiente hoy
Examen final del curso

4.4.2 Curso 2 – SOC: Fundamentos y Colaboración



☆☆☆☆☆ (0 reviews)

Curso 2 – SOC: Fundamentos y Colaboración

Figura 29. Curso 2

Fuente: Elaboración Propia

4.4.2.1 Descripción del curso

Bienvenidos al curso de “SOC: Fundamentos y colaboración”. Este curso se ha diseñado para poder brindar conocimiento amplio de los principios y practicas esenciales en la ciberseguridad, y también en la gestión de incidentes. Este curso tiene como meta brindar un amplio conocimiento del papel que tiene un analista SOC en la protección y respuesta efectiva contra amenazas.

4.4.2.2 Modulo #1 Servicios del Centro de Operaciones de Seguridad

Lección #1 Preparación, planificación y prevención

Lección #2 Monitoreo, detección y respuesta

Lección #3 Recuperación, refinamiento y cumplimiento

Cuestionario

4.4.2.3 Modulo #2 SOC Interacción con otros departamentos

Lección #1 SOC Interacción con otros departamentos

Cuestionario

4.4.2.4 Modulo #3 Servicios comunes del SOC

Lección #1 El moderno Centro de Operaciones de Seguridad

Cuestionario

4.4.3 Curso 3 – Modelos y tipos de despliegue de los SOC



☆☆☆☆☆ (0 reviews)

Curso 3 – Modelos y tipos de despliegue de los SOC

Figura 30. Curso 3

Fuente: Elaboración Propia

4.4.3.1 Descripción del curso

En este emocionante curso, exploraremos el mundo de los Centros de Operaciones de Seguridad (SOC) y sus diversas formas de implementación. nos sumergiremos en los fundamentos clave que todo profesional de la ciberseguridad necesita dominar. Con un enfoque en normativas, respuesta a incidentes y gestión de activos corporativos, abordaremos una gama completa de conocimientos vitales. Desde la clasificación de los SOC hasta los diferentes modelos de despliegue, descubriremos las fortalezas y debilidades de cada enfoque según las necesidades específicas de los clientes. Al final de este viaje de aprendizaje, tendrás una perspectiva clara sobre cómo elegir

el camino adecuado en tu papel como experto en seguridad cibernética. ¡Prepárate para sumergirte en el fascinante mundo de los SOC!

4.4.3.2 Modulo #1 Modelos y tipos de despliegue de los SOC

Lección #1 Tipos de SOC

Cuestionario: Modelos y tipos de despliegue de los SOC

4.4.3.3 Modulo #2 Tipos de SOC y consideraciones sobre el personal

Lección #1 SOC de primera generación

Lección #2 SOC de segunda generación

Lección #3 SOC de tercera generación

Lección #4 SOC de cuarta generación

Cuestionario: Tipos de SOC y consideraciones sobre el personal

4.4.3.4 Modulo #3 Características de un SOC eficaz

Lección #1 Patrocinio ejecutivo

Lección #2 Gobernanza

Lección #3 Operar el SOC como un programa

Lección #4 Colaboración

Lección #5 Acceso a datos y sistemas

Lección #6 Procesos y procedimientos aplicables

Lección #7 Conjunto de habilidades y experiencia

Lección #8 Presupuesto

Lección #9 Gente

Lección #10 Estructura

Lección #11 Capacitación y certificación

Cuestionario: Características de un SOC eficaz

Cuestionario

4.4.4 Curso 4 – SOC360: Personal, Funciones e Interacción en Ciberseguridad



☆☆☆☆☆ (0 reviews)

Curso 4 – SOC360: Personal, Funciones e Interacción en Ciberseguridad

Figura 31. Curso 4

Fuente: Elaboración Propia

4.4.4.1 Descripción del curso

En un entorno digital cada vez más complejo, la seguridad cibernética se erige como un pilar fundamental para proteger los activos críticos de una organización. Este curso se sumerge en los fundamentos esenciales para construir y operar un Equipo de Operaciones de Seguridad (SOC) eficaz. Desde la dotación estratégica de personal hasta el desglose detallado de funciones específicas del SOC, exploraremos cómo este equipo central juega un papel crucial en la identificación y respuesta a amenazas cibernéticas. Además, analizaremos la interacción dinámica entre las distintas funciones dentro del SOC, revelando la sinergia necesaria para mantener la seguridad digital en un mundo en constante evolución. Únete a nosotros en este viaje de aprendizaje integral, diseñado para dotarte de los conocimientos y habilidades necesarios para enfrentar los desafíos actuales y futuros en ciberseguridad.

4.4.4.2 Modulo #1 Dotación de personal para un equipo SOC eficaz

Lección #1 ¿Qué tipo de profesionales trabajan en el Security Operations Center (SOC)?

Cuestionario

4.4.4.3 Modulo #2 Funciones del SOC

Lección #1 ¿Qué hace un SOC?

Lección #2 Desafíos SOC

Cuestionario

4.4.4.4 Modulo #3 Interacción de las distintas funciones dentro del SOC

Lección #1 Trabajando como un equipo

Cuestionario

4.4.5 Curso 5 – Datos de eventos de seguridad y herramientas para analistas SOC



☆☆☆☆☆ (0 reviews)

Curso 5 – Datos de eventos de seguridad y herramientas para analistas SOC

Figura 32. Curso 5

Fuente: Elaboración Propia

4.4.5.1 Descripción del curso

Bienvenidos al curso “Datos de Eventos de Seguridad y Herramientas para Analistas SOC”. En este módulo, exploraremos a fondo cómo los profesionales de seguridad manejan y analizan los datos generados por eventos de seguridad. Desde la comprensión de las tecnologías que los generan hasta la identificación de datos cruciales para el SOC y el análisis de herramientas especializadas, este curso ofrece una inmersión práctica en las habilidades esenciales para detectar, analizar y responder a amenazas digitales. ¡Prepárense para fortalecer sus capacidades en el dinámico campo de la ciberseguridad!

4.4.5.2 Modulo #1 Datos de eventos de seguridad y tecnologías para analistas SOC

Lección #1 Fuentes de datos

Lección #2 Recopilación de datos

Lección #3 Tecnologías

4.4.5.3 Modulo #2 Datos relevantes del SOC y datos de eventos de seguridad

Lección #1 Gestión de Riesgos

Lección #2 Mapa de color de riesgo

Lección #3 Enriquecimiento de datos

Lección #4 Plataformas de Big Data para la seguridad

4.4.5.4 Modulo #3 Herramientas SOC y sus características

Lección #1 Herramienta de gestión y recopilación de logs

Lección #2 Seguridad de la información y gestión de eventos (SIEM)

Lección #3 Gestión de vulnerabilidades

Lección #4 Detección y respuesta de endpoint (EDR)

Lección #5 Herramientas de vulnerabilidad

Cuestionario

4.4.6 Curso 6 – Relaciones clave del SOC con los stakeholders



☆☆☆☆☆ (0 reviews)

Curso 6 – Relaciones clave del SOC con los stakeholders

Figura 33. Curso 6

Fuente: Elaboración Propia

4.4.6.1 Descripción del curso

Bienvenido al emocionante mundo de la ciberseguridad y el Centro de Operaciones de Seguridad (SOC). Este curso proporcionará a los estudiantes una comprensión integral de las relaciones clave del SOC con los stakeholders, tanto internos como externos, para fortalecer la ciberresiliencia de las organizaciones. Aquí, exploraremos la importancia vital de estos centros en la protección contra amenazas cibernéticas emergentes y sofisticadas.

4.4.6.2 Modulo #1 Relaciones clave del SOC con los stakeholders

Lección #1 Relaciones clave del SOC con los stakeholders

4.4.6.3 Modulo #2 Stakeholders internos

Lección #1 stakeholders Internos

Lección #2 ¿Cómo se involucran los stakeholders internos?

Lección #3 ¿Cuáles son los stakeholders internos?

4.4.6.4 Modulo #3 Stakeholders Externos

Lección #1 stakeholders externos

Lección #2 ¿Cómo se involucran los stakeholders externos?

Lección #3 ¿Cuáles son los stakeholders Externos?

Cuestionario

4.4.7 Curso 7 – Estrategias de Protección Cibernética



☆☆☆☆☆ (0 reviews)

Curso 7 – Estrategias de Protección Cibernética

Figura 34. Curso 7

Fuente: Elaboración Propia

4.4.7.1 Descripción del curso

¡Bienvenidos al curso “Estrategias de Protección Cibernética”!

Hoy en día la seguridad es fundamental, es por esto que se debe de tener una protección de datos y una respuesta correcta antes las amenazas cibernéticas que surgen cada día.

Aventúrate a descubrir los marcos de seguridad para establecer defensas sólidas y poder poner en práctica las estrategias efectivas ante una respuesta a incidentes.

4.4.7.2 Modulo #1 Marcos de seguridad

Lección #1 ISO/IEC 27001:2022

Lección #2 COBIT

Lección #3 NIST

4.4.7.3 Modulo #2 Respuesta a incidentes

Lección #1 Respuesta a incidentes de seguridad de la información

4.4.7.4 Modulo #3 Actividades Extra

Actividades

4.4.8 Curso 8 – Comprender el flujo de trabajo y la automatización del SOC



☆☆☆☆☆ (0 reviews)

Curso 8 – Comprender el flujo de trabajo y la automatización del SOC

Figura 35. Curso 8

Fuente: Elaboración Propia

4.4.8.1 Descripción del curso

¡Bienvenidos al curso “Comprender el Flujo de Trabajo y la Automatización del SOC”! Este módulo es una inmersión rápida en los conceptos esenciales que impulsan la eficiencia en un

Security Operations Center (SOC). Desde los fundamentos de redes hasta la comprensión de protocolos y puertos, este curso proporcionará las habilidades clave para optimizar el flujo de trabajo y aprovechar la automatización en la respuesta a amenazas digitales. ¡Prepárense para potenciar su experiencia en seguridad y operaciones!

4.4.8.2 Modulo #1 Conceptos básicos de redes

Lección #1 Tipos de Redes

Lección #2 Tipos de Topologías

Lección #3 Componentes de una Red

Lección #4 Medio guiado

Lección #5 Medio no guiado

Lección #6 Equipos de Red

Lección #7 Servicios de la Red

4.4.8.3 Modulo #2 Protocolos y puertos

Lección #1 Principales puertos TCP

Lección #2 Principales puertos UDP

Lección #3 Puertos más utilizados

Lección #4 Estados de los Puertos

Cuestionario

4.4.9 Curso 9 – Vulnerabilidades, malware y respuesta a incidentes



☆☆☆☆☆ (0 reviews)

Curso 9 – Vulnerabilidades, malware y respuesta a incidentes

Figura 36. Curso 9

Fuente: Elaboración Propia

4.4.9.1 Descripción del curso

El Curso 9 – Vulnerabilidades, malware y Respuesta a incidentes proporciona una comprensión integral de los desafíos de ciberseguridad, el paisaje de amenazas y los desafíos empresariales que enfrentan las organizaciones. El enfoque se centra en la gestión de vulnerabilidades, los anuncios de vulnerabilidades y una exploración detallada de los tipos de malware más relevantes en la actualidad, como ransomware, troyanos, gusanos, spyware, adware y botnets. Además, el curso aborda la respuesta a incidentes de seguridad de la información, desde la detección hasta la resolución y el análisis post-incidente.

4.4.9.2 Modulo #1 Vulnerabilidades y amenazas

Lección #1 Desafíos de ciberseguridad

Lección #2 Paisaje de amenazas

Lección #3 Desafíos empresariales

Lección #4 Gestión de vulnerabilidades
Lección #5 Anuncios de vulnerabilidades
Cuestionario

4.4.9.3 Modulo #2 Tipos de malware

Lección #1 Ransomware
Lección #2 Troyanos
Lección #3 Gusanos
Lección #4 Spyware y Adware
Lección #5 Botnets
Cuestionario

4.4.9.4 Modulo #3 Respuesta a incidentes

Lección #1 Respuesta a incidentes de seguridad de la información
Lección #2 Detección de incidentes
Lección #3 Triage de incidentes
Lección #4 Categorías de incidentes
Lección #5 Severidad de incidentes
Lección #6 Resolución de incidentes
Lección #7 Cierre de incidentes
Lección #8 Post incidente
Cuestionario

Cuestionario

4.4.10 Curso 10 – Laboratorios



☆☆☆☆☆ (0 reviews)

Curso 10 – Laboratorios

Figura 37. Curso 10

Fuente: Elaboración Propia

4.4.10.1 Descripción del curso

Bienvenidos al Curso de Laboratorios en Ciberseguridad e Ingeniería en SOC

¡Estudiantes, les damos la bienvenida a este curso de laboratorios, una experiencia práctica diseñada para fortalecer sus habilidades en el campo de la ciberseguridad y la ingeniería en Centro de Operaciones de Seguridad (SOC)! Este curso no solo evaluará sus conocimientos teóricos, sino que pondrá a prueba su capacidad para aplicar esos conocimientos en entornos prácticos.

4.4.10.2 Características del Curso:

Duración y Puntualidad: Cada laboratorio tiene un tiempo asignado. La puntualidad es esencial para aprovechar al máximo el tiempo de práctica y garantizar la entrega en tiempo y forma.

Requisitos de Entrega: Cada laboratorio tiene requisitos específicos que deben cumplirse para la entrega. La habilidad para seguir instrucciones detalladas y cumplir con los requisitos es crucial para el éxito.

80% para Aprobar: La aprobación del curso requiere un rendimiento mínimo del 80%. Este estándar refleja la excelencia que esperamos en la instalación y configuración de Splunk, análisis de hash, y la implementación de reglas de seguridad de firewall en entornos Windows.

4.4.10.3 Laboratorio #1 Comprobación de hash con Powershell y virus total

Practica de comprobación de HASH alterado y bloqueo de ejecución del ejecutable comprometido.

4.4.10.4 Laboratorio #2 Creación de reglas de entrada y salida de firewall de windows defender

Creación de reglas de entrada y salida de firewall de Windows defender

4.4.10.5 Laboratorio #2 Splunk instalación y configuración de entorno

laboratorio instalación de Splunk

4.4.11 Examen Final SOC: Travesía de Conocimiento en 10 Cursos



☆☆☆☆☆ (0 reviews)

**Examen Final: Desafío
Maestro SOC: Travesía de
Conocimiento en 10 Cursos**

Figura 38. Examen Final

Fuente: Elaboración Propia

4.4.11.1 Descripción del curso

¡Bienvenidos, estudiantes, al Examen Final “Desafío Maestro SOC”! Este desafío representa la culminación de una travesía a través de 10 cursos que han explorado a fondo el fascinante mundo del Centro de Operaciones de Seguridad (SOC).

Este examen no es solo una evaluación, es la prueba de fuego que demuestra la maestría adquirida a lo largo de estos cursos. Habiendo recorrido desde los fundamentos iniciales hasta las complejidades de la respuesta a incidentes y la interacción con los stakeholders, este es el momento de poner a prueba su conocimiento integral.

¡Ustedes han llegado lejos y están listos para este desafío! Recuerden los momentos de aprendizaje, las lecciones valiosas y las habilidades adquiridas. Este examen es su oportunidad de demostrar lo que han logrado. Mantengan la calma, lean cuidadosamente y confíen en su preparación.

4.4.11.2 Características del Examen:

1- Duración Limitada: Se les brindará un tiempo específico para completar el examen. Este es un recordatorio de que la concentración y el enfoque son clave para el éxito.

2- 80% para Pasar: La aprobación requiere un mínimo del 80%. Este estándar elevado refleja la calidad y profundidad del conocimiento que se espera de ustedes después de esta intensiva travesía educativa.

3- 50 Preguntas Desafiantes: Prepárense para una serie de 50 preguntas cuidadosamente diseñadas, que abarcan desde los conceptos fundamentales hasta las aplicaciones prácticas.

Examen Final Desafío Maestro SOC: Travesía de Conocimiento en 10 Cursos

4.6 Diagrama de Gantt

Equipo SOC	PRESENTACION DE PROPUESTA		PRIMERA ENTREGA	
ACTIVIDAD	Semana 1 Octubre	Semana 2 Octubre	Semana 3 Octubre	Semana 4 Octubre Entregable
<ul style="list-style-type: none"> - Ideas para el proyecto - Debate sobre idea mas ideonea - Detalles especificos sobre la idea - Eleccion de la idea del proyecto -busqueda de hosting y busqueda de plugins, temas, recursos y tutoriales para la creacion de la plataforma 				
<ul style="list-style-type: none"> - Investigacion sobre mejoras para el proyecto - Realizar entregable formato de resolucion de dudas - Entregable completado y enviado -Carga e instalacion de Wordpress al hosting -Creacion del dominio soc-training -Primeras pruebas de maquetacion del sitio 				
<ul style="list-style-type: none"> -Discusión e investigacion de los temas (SOC) -Detalles especificos sobre los modulos, contenido -Alojamiento de la plataforma -Creacion de modelo base de plataforma -Implementacion de Tutor MLS 				
<ul style="list-style-type: none"> -Distribucion de asignaciones -Confirmacion y verificacion de temas de contenido -Preparacion de informe de primer avance parcial -Trabajar en el contenido especifico de los modulos -Trabajar en el entregable parcial -Creacion de los primeros cursos de la plataforma -coreccion de errores del header -Creacion de formularios para registro de estudiante y tutor Creacion de inicio de sesion -creacion de pagina de acerca de nosotros -Creacion de pagina de admisiones Creacion de pagina de inicio 				

Figura 39. Diagrama de Gantt 1

Fuente: Elaboración Propia

Equipo SOC	SEGUNDA ENTREGA		ENTREGA FINAL	
ACTIVIDAD	Semana 5 Noviembre	Semana 6 Noviembre Entregable	Semana 7 Noviembre	Semana 8 Noviembre Entregable
<ul style="list-style-type: none"> -Ideas y mejoras para la plataforma en general -Desarrollar la estructura general de los cursos -Integracion de contenido e imágenes en los cursos -Ideas de como hacer mas didactica la pagina -Correccion de errores de la plataforma -Creacion de pagina de "mi perfil" -Creacion y pruebas cuentas de estudiantes y tutores 				
<ul style="list-style-type: none"> -Se agregaron fotos y redes sociales de los profesores -Se terminaron detalles de documentación -Realizacion de 6 cursos la mayormente con contenido estructurado -Creacion de pagina login y implementacion de cierre de sesion. -creacion de pagina contactos -Creacion de pagina preguntas y respuestas 				
<ul style="list-style-type: none"> -Se elaboraron nuevas asignaciones -Entrega de avances finales entre equipo en reuniones -Mejoras en la plataforma -Finalizacion de los modulos, lecciones y juegos en los cursos -Edicion de formulario de contacto para la pagina -Edicion de la pagina inicio -Edicion del footer -Retoques finales 				
<ul style="list-style-type: none"> -Elaboracion del informe final -Detalles de los diferentes manuales de la plataforma -Elaboracion de videos descriptivos de la plataforma -Realizacion del examen final para los 10 cursos -Correccion de errores del header -Correccion del responsive de telefonos -Retoques finales de la plataforma -Edicion final de perfiles de tutores 				

Figura 40. Diagrama de Gantt 2

Fuente: Elaboración Propia

CONCLUSIONES

La implementación en línea de una plataforma de aprendizaje ha demostrado ser una forma excelente para el acceso a información relevante y de calidad para los interesados en el área de SOC-CTIS-DFIR. Las personas que aprendan con la plataforma podrán ser parte de la disminución de la brecha que hay en cuanto al conocimiento limitado en tal área. Esto logró que se pudiera fortalecer la base de conocimiento en estudiantes y profesionales en ciberseguridad.

El desarrollo de la plataforma es un recurso positivo y especializado que aborda temas con detalles específicos en el área de SOC. Los cursos junto con sus distintos módulos abarcan desde conceptos básicos hasta temas incluso avanzados, lo cual genera una formación muy completa en tal área

Las distintas evaluaciones que hay en cada curso garantizan que el contenido que adquieren los estudiantes es un contenido fuerte y de calidad, dichas evaluaciones cuentan con un criterio del 80% para aprobarlas. Con esto se puede asegurar que los estudiantes hayan aprendido de una forma limpia sin que haya fraude en cuanto al conocimiento adquirido. Y también ayuda a que los profesionales emergentes del área de SOC-CTIS-DFIR posean las habilidades o conocimiento necesario para enfrentarse a los distintos desafíos del campo laboral en ciberseguridad.

El desarrollo de la plataforma ha sido una contribución en la formación de la ciberseguridad, también ha establecido un precedente para futuros desarrollos en la educación en línea enfocada en SOC-CTIS-DFIR. Esto cierra la carencia en la falta de información verídica y confiable que no estaba disponible en internet más que solo en fuentes de dudosa procedencia.

RECOMENDACIONES

Como conclusión de la investigación y el trabajo realizado en la creación de una plataforma de aprendizaje en línea para el área de ciberseguridad e Ingeniería en Security Operations Center (SOC), se derivan las siguientes recomendaciones fundamentales:

- a) **Implementación de una Plataforma Centralizada:** Se recomienda establecer una plataforma centralizada que sirva como recurso principal para los interesados en ciberseguridad e ingeniería en SOC. Esta plataforma debe ser fácilmente accesible y proporcionar un espacio unificado para el acceso a recursos, cursos, materiales de estudio y herramientas esenciales.
- b) **Desarrollo de Contenido Especializado:** Se sugiere la creación de contenido educativo altamente especializado y actualizado regularmente. Este contenido debe abarcar tanto los fundamentos teóricos como las aplicaciones prácticas de la ciberseguridad y la ingeniería en SOC, garantizando así la relevancia y la utilidad para los estudiantes.
- c) **Integración de Recursos Prácticos:** La inclusión de laboratorios virtuales, simulaciones y casos de estudio prácticos es esencial. La plataforma debe ofrecer a los estudiantes la oportunidad de aplicar sus conocimientos en entornos simulados que reflejen situaciones del mundo real en ciberseguridad y operaciones de SOC.
- d) **Colaboración con Profesionales del Sector:** Se recomienda establecer asociaciones con expertos y profesionales de la industria de la ciberseguridad. Estas colaboraciones pueden incluir conferencias, seminarios web y participación directa de profesionales en la creación de contenido, brindando a los estudiantes una perspectiva práctica y actualizada de la industria.
- e) **Programas de Certificación Reconocidos:** La plataforma debe ofrecer programas de certificación reconocidos en el campo de la ciberseguridad e ingeniería en SOC. Estas certificaciones son clave para validar las habilidades adquiridas y proporcionar a los estudiantes una ventaja competitiva en el mercado laboral.

- f) Acceso a Recursos Financieros: Dada la falta de recursos propios para estudiar en el área, se recomienda explorar opciones de becas, descuentos o programas de apoyo financiero para garantizar que la educación en ciberseguridad sea accesible para un amplio espectro de estudiantes, independientemente de sus recursos económicos.
- g) Monitoreo Continuo y Retroalimentación: Implementar un sistema de monitoreo continuo para evaluar la efectividad de la plataforma y recopilar retroalimentación de los usuarios. Este ciclo de retroalimentación constante permitirá realizar mejoras iterativas, asegurando que la plataforma evolucione de acuerdo con las necesidades cambiantes de la comunidad de ciberseguridad.
- h) Desarrollo de Comunidad: Fomentar la creación de una comunidad activa en línea donde los estudiantes puedan intercambiar conocimientos, experiencias y colaborar en proyectos. La interacción entre pares y la creación de redes son aspectos fundamentales para el crecimiento y el éxito a largo plazo de los estudiantes en el campo de la ciberseguridad.

BIBLIOGRAFÍA

- Aarness, A. (2019, mayo 24). *What is EDR? Endpoint Detection & Response Defined*. CrowdStrike.com; CrowdStrike. <https://www.crowdstrike.com/cybersecurity-101/endpoint-security/endpoint-detection-and-response-edr/>
- Alfonso. (2019, abril 5). *Actualizaciones de software: qué son, para qué sirven, cuándo instalarlas*. idearius. <https://www.idearius.com/es/blog/actualizaciones-de-software-que-son-para-que-sirven-cuando-instalarlas/>
- Analizar en busca de indicadores de compromiso (IOC)*. (s/f). Kaspersky.com. Recuperado el 28 de noviembre de 2023, de <https://support.kaspersky.com/KESWin/11.7.0/es-MX/213408.htm>
- ¿Cómo funciona un centro de operaciones de seguridad (SOC)? (2023, febrero 22). Auditech. <https://auditech.es/blog/como-funciona-un-centro-de-operaciones-de-seguridad-soc/>
- de Actividades Profesionales, I. (s/f). *Actividades de monitoreo y análisis en un Security Operation Center*. Unam.mx:8080. Recuperado el 28 de noviembre de 2023, de <http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/15960/Actividades%20de%20monitoreo%20y%20an%C3%A1lisis%20en%20un%20Security%20Operation%20Center.pdf?sequence=1&isAllowed=y>
- Directiva de seguridad local*. (s/f). Microsoft.com. Recuperado el 28 de noviembre de 2023, de <https://learn.microsoft.com/es-es/windows/win32/secmgmt/local-security-policy>
- Donohue, B. (2014, abril 10). *¿Qué Es Un Hash Y Cómo Funciona?* Kaspersky. <https://latam.kaspersky.com/blog/que-es-un-hash-y-como-funciona/2806/>

El empresario, U. G. de A. P. (s/f). *Copias de seguridad*. Incibe.es. Recuperado el 28 de noviembre de 2023, de <https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf>

ElevenPaths. (2020, abril 2). ¿Qué tipo de profesionales trabajan en el Security Operations Center (SOC)? *Telefónica Tech*. <https://telefonicatech.com/blog/que-tipo-profesionales-trabajan-soc>

ESDAI. (s/f). *¿Qué es la gestión de eventos y cuál es su importancia?* Edu.mx. Recuperado el 28 de noviembre de 2023, de <https://blog.up.edu.mx/gdl/posgrados-esdai/que-es-la-gestion-de-eventos-y-cual-es-su-importancia>

Filtración de Datos. (2020, abril 27). CyberArk; CyberArk Software. <https://www.cyberark.com/es/what-is/data-breach/>

Freda, A. (2021, noviembre 26). *¿Qué es el registro de Windows y cómo funciona?* ¿Qué es el registro de Windows y cómo funciona?; Avast. <https://www.avast.com/es-es/c-windows-registry>

Gusanos informáticos. (s/f). Hornetsecurity – Servicios de seguridad en nube para empresas. Recuperado el 28 de noviembre de 2023, de <https://www.hornetsecurity.com/es/knowledge-base/gusanos-informaticos/>

Habte, F. (2020, mayo 5). *Qu'est-ce que le SOC (Security Operation Center) ? - Logiciel Check Point*. Check Point Software. <https://www.checkpoint.com/fr/es/cyber-hub/what-is-soc/>

Herrero, E. G. (2023, febrero 3). *¿Qué es la ciberdefensa?* Seguritecnia. https://www.seguritecnia.es/actualidad/que-es-la-ciberdefensa_20230203.html

Introducción a Windows PowerShell. (2023, septiembre 14). IONOS Digital Guide; IONOS. <https://www.ionos.es/digitalguide/servidores/know-how/windows-powershell/>

Jiménez, J. (2022, abril 21). *Conoce si Windows Defender es suficiente o necesitas otro antivirus.*

RedesZone. <https://www.redeszone.net/tutoriales/seguridad/windows-defender-suficiente-seguridad/>

Myers, L. (s/f). *Top 5 de botnets zombi más aterradoras.* Welivesecurity.com. Recuperado el 28 de noviembre de 2023, de <https://www.welivesecurity.com/la-es/2014/10/29/top-5-botnets-zombi/>

No title. (s/f-a). Imperva.com. Recuperado el 28 de noviembre de 2023, de <https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/>

No title. (s/f-b). Scribbr.es. Recuperado el 28 de noviembre de 2023, de <https://www.scribbr.es/citar/generador/folders/2EJ3eRELVRaD9ssoqwd2hU/lists/2i7xSEs8jyUACzTUb8AKF9/>

Pachón, C. (2021, febrero 25). *Qué es un SOC: Funciones y objetivos principales.* Nsit; NSIT SAS. <https://www.nsit.com.co/que-es-un-soc-funciones-y-objetivos-principales/>

Page, M. (2023, junio 2). *Perfil de SOC Analyst.* Michael Page. <https://www.michaelpage.es/advice/profesi%C3%B3n/tecnolog%C3%ADa/perfil-de-soc-analyst>

Porto, J. P., & Gardey, A. (2013, septiembre 16). *Puerto USB.* Definición.de; Definicion.de. <https://definicion.de/puerto-usb/>

¿Qué es botnet? - Definición y cómo funciona. (2021, noviembre 15). Proofpoint. <https://www.proofpoint.com/es/threat-reference/botnet>

¿Qué es el marco de ciberseguridad del NIST? (s/f-a). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/mx-es/topics/nist>

¿Qué es el marco de ciberseguridad del NIST? (s/f-b). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/mx-es/topics/nist>

¿Qué es el phishing? (2018, diciembre 20). Malwarebytes. <https://es.malwarebytes.com/phishing/>

¿Qué es el ransomware? (s/f-a). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/mx-es/topics/ransomware>

¿Qué es el ransomware? (s/f-b). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/es-es/topics/ransomware>

¿Qué es el ransomware WannaCry? (2023, agosto 18). www.kaspersky.es. <https://www.kaspersky.es/resource-center/threats/ransomware-wannacry>

¿Qué es la Captura de Paquetes? Introducción al Glosario de TI. (2023, septiembre 4). TS2 SPACE. <https://ts2.space/es/que-es-la-captura-de-paquetes-introduccion-al-glosario-de-ti/>

¿Qué es la gestión de parches? (s/f). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/es-es/topics/patch-management>

¿Qué es la inteligencia de amenazas? (s/f). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/es-es/topics/threat-intelligence>

¿Qué es la resiliencia cibernética? (s/f). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/es-es/topics/cyber-resilience>

¿Qué es la respuesta a incidentes? (s/f-a). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/es-es/topics/incident-response>

¿Qué es la respuesta a incidentes? (s/f-b). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/es-es/topics/incident-response>

¿Qué es un Centro de Operaciones de Seguridad (SOC)? (s/f). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/es-es/topics/security-operations-center>

¿Qué es un firewall? Definición y explicación. (2023, agosto 15). latam.kaspersky.com. <https://latam.kaspersky.com/resource-center/definitions/firewall>

¿Qué es un SOC? (s/f). Oracle.com. Recuperado el 28 de noviembre de 2023, de <https://www.oracle.com/es/database/security/que-es-un-soc.html>

¿Qué es un troyano? - Definición y explicación. (2023, octubre 6). www.kaspersky.es. <https://www.kaspersky.es/resource-center/threats/trojans>

¿Qué son las pruebas de penetración? (s/f). Ibm.com. Recuperado el 28 de noviembre de 2023, de <https://www.ibm.com/mx-es/topics/penetration-testing>

Qué son los stakeholders, qué tipos existen y de qué manera impactan a una empresa. (2019a, agosto 21). Rock Content - ES; Rock Content. <https://rockcontent.com/es/blog/que-es-un-stakeholder/>

Qué son los stakeholders, qué tipos existen y de qué manera impactan a una empresa. (2019b, agosto 21). Rock Content - ES; Rock Content. <https://rockcontent.com/es/blog/que-es-un-stakeholder/>

Quiroa, M. (2020, enero 29). *Administrador*. Economipedia. <https://economipedia.com/definiciones/administrador.html>

Spyware. (2018, diciembre 20). Malwarebytes. <https://es.malwarebytes.com/spyware/>

Toledo, R. (2022, agosto 23). Centro de Operaciones de Seguridad para empresas: Tipos y funciones. *Grupocibernos.com*. <https://www.grupocibernos.com/blog/que-es-un-centro-de-operaciones-de-seguridad-para-empresas-tipos-y-funciones>

Vive. (2021, julio 1). *¿Qué es una VPN?: funciones, tipos e importancia*. UNIR.
<https://www.unir.net/ingenieria/revista/que-es-vpn/>

What is Intrusion Prevention System? (2023, agosto 9). VMware.
<https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html>

Wikipedia contributors. (s/f). *VirusTotal*. Wikipedia, The Free Encyclopedia.
<https://es.wikipedia.org/w/index.php?title=VirusTotal&oldid=154649080>

(S/f-a). Cloudflare.com. Recuperado el 28 de noviembre de 2023, de
<https://www.cloudflare.com/es-es/learning/security/what-are-indicators-of-compromise/>

(S/f-b). Amazon.com. Recuperado el 28 de noviembre de 2023, de
<https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La%20ciberseguridad%20es%20la%20pr%C3%A1ctica,datos%20de%20posibles%20amenazas%20digitales.>

(S/f-c). Cloudflare.com. Recuperado el 28 de noviembre de 2023, de
<https://www.cloudflare.com/es-es/learning/security/ransomware/petya-notpetya-ransomware/>

(S/f-d). Protecciondatos-lopd.com. Recuperado el 28 de noviembre de 2023, de
<https://protecciondatos-lopd.com/empresas/centro-operaciones-seguridad-soc/>

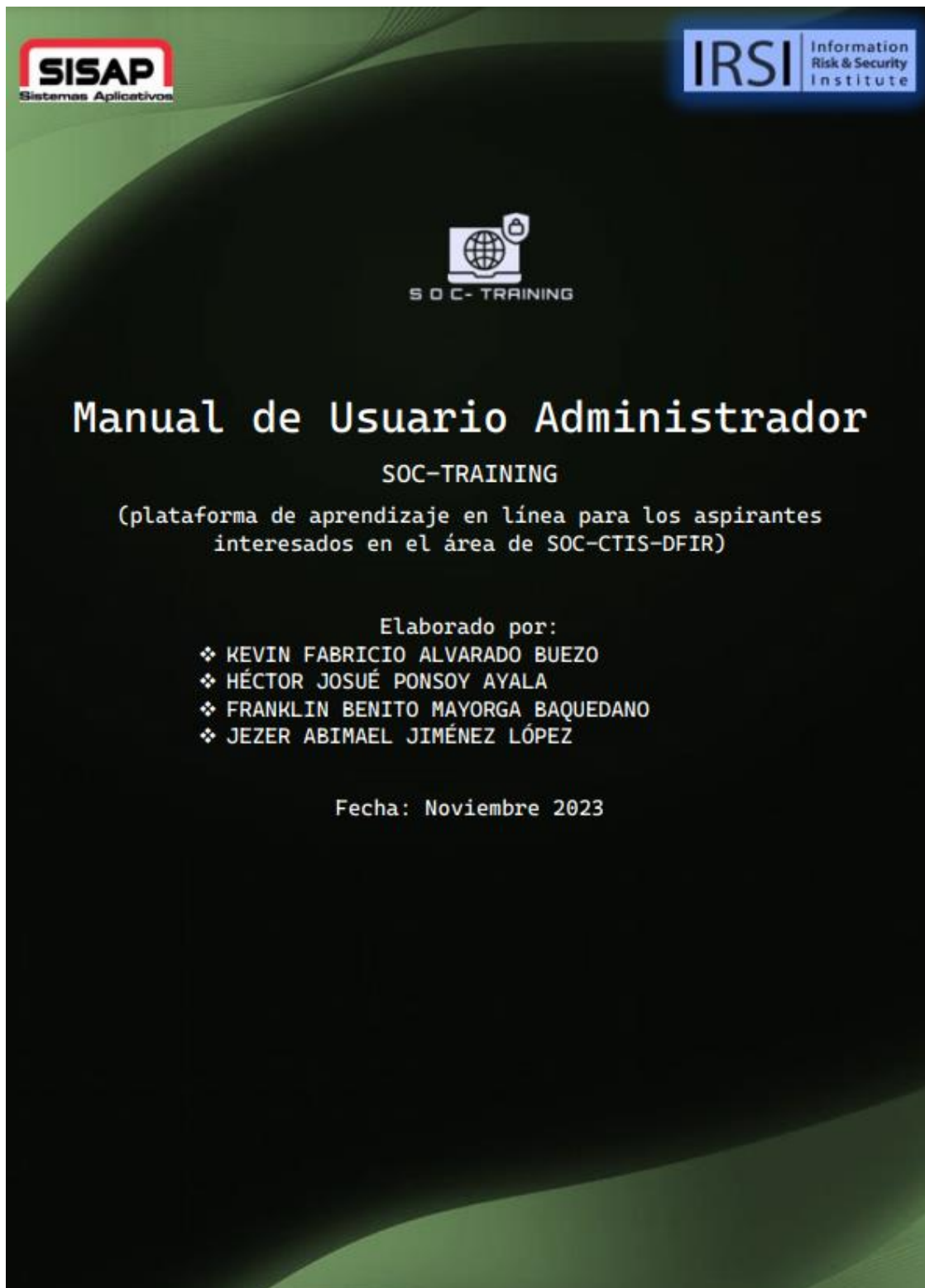
(S/f-e). Servicenow.com. Recuperado el 28 de noviembre de 2023, de
<https://www.servicenow.com/es/products/security-operations/what-is-soc.html>

(S/f-f). Pearsoncmg.com. Recuperado el 28 de noviembre de 2023, de
<https://ptgmedia.pearsoncmg.com/images/9780134052014/samplepages/9780134052014.pdf>

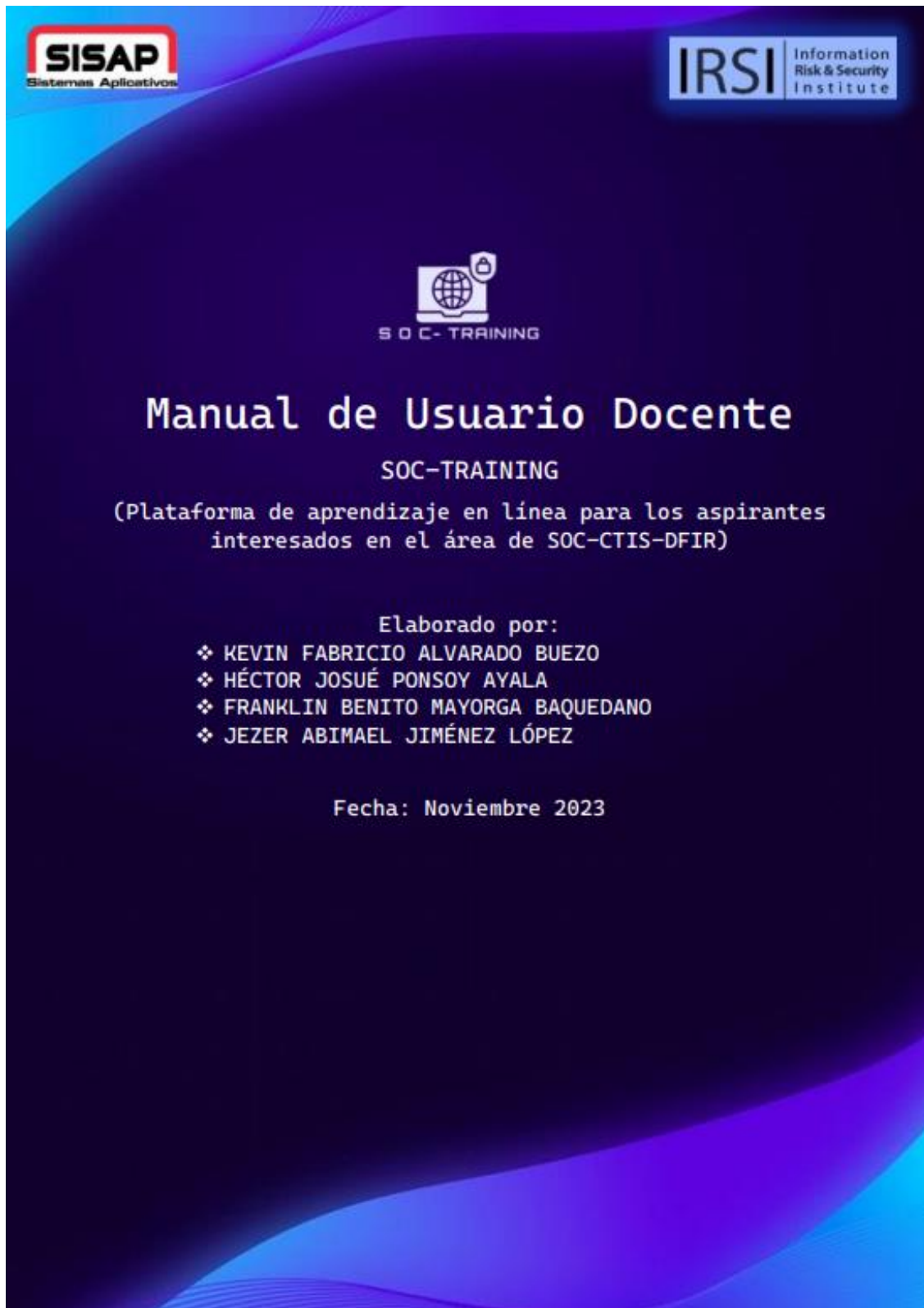
ANEXOS

Anexos 1. Manuales

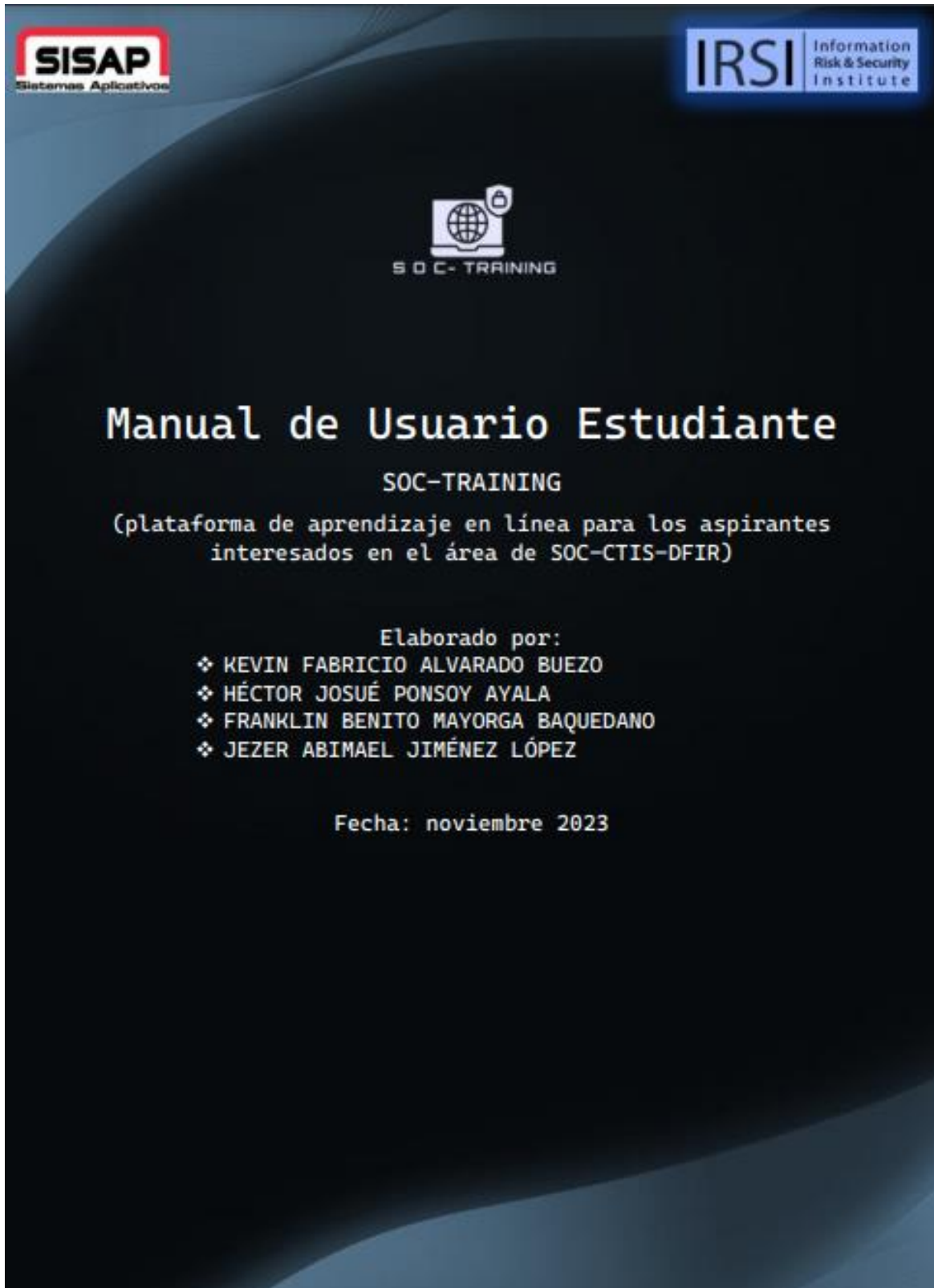
Manual de Usuario Administrador



Manual de Usuario Docente



Manual de Usuario Estudiante



Anexos 2. Autoevaluaciones



Programa Certificación en Ciberseguridad

Proyecto de graduación

Autoevaluación

Nombre del alumno: Kevin Fabricio Alvarado Buezo

Grupo No.: Área de especialización: SOC-CTIS-DFIR

Nombre del proyecto: Implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR

Fecha: Domingo 26 noviembre 2023

No.	ACTIVIDAD	NUNCA	A VECES	SIEMPRE
1	Asisto regularmente a las reuniones de grupo de trabajo.			X
2	Cumplo con las instrucciones recibidas de la coordinación de grupo en relación a la elaboración del proyecto de graduación.			X
3	Participo activamente en las reuniones contribuyendo a resolver problemas encontrados por mis compañeros en la investigación y el diseño del proyecto.			X
4	Cumplo con los pasos y requisitos del plan de trabajo y diseño del proyecto.			X
5	Respeto el orden de las fases del diseño del proyecto.			X
6	Atiendo las orientaciones de mis compañeros para resolver dificultades en el proceso de la elaboración del proyecto.			X
7	Cumplo con las tareas asignadas por la coordinación del grupo y las entrego en el tiempo estipulado.			X
8	Tengo una actitud positiva hacia la elaboración del proyecto de graduación.			X

Nunca:

A veces:

Siempre:

Proyecto de graduación

Autoevaluación

Nombre del alumno: Héctor Josué Ponsoy Ayala

Grupo No.: Área de especialización: SOC-CTIS-DFIR

Nombre del proyecto: Implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR

Fecha: Domingo 26 noviembre 2023

No.	ACTIVIDAD	NUNCA	A VECES	SIEMPRE
1	Asisto regularmente a las reuniones de grupo de trabajo.			X
2	Cumplo con las instrucciones recibidas de la coordinación de grupo en relación a la elaboración del proyecto de graduación.			X
3	Participo activamente en las reuniones contribuyendo a resolver problemas encontrados por mis compañeros en la investigación y el diseño del proyecto.			X
4	Cumplo con los pasos y requisitos del plan de trabajo y diseño del proyecto.			X
5	Respeto el orden de las fases del diseño del proyecto.			X
6	Atiendo las orientaciones de mis compañeros para resolver dificultades en el proceso de la elaboración del proyecto.			X
7	Cumplo con las tareas asignadas por la coordinación del grupo y las entrego en el tiempo estipulado.			X
8	Tengo una actitud positiva hacia la elaboración del proyecto de graduación.			X

Nunca:

0

A veces:

5

Siempre:

10

Proyecto de graduación
Autoevaluación
Nombre del alumno: Franklin Benito Mayorga Baquedano
Grupo No.: **Área de especialización:** SOC-CTIS-DFIR
Nombre del proyecto: Implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR
Fecha: Domingo 26 noviembre 2023

No.	ACTIVIDAD	NUNCA	A VECES	SIEMPRE
1	Asisto regularmente a las reuniones de grupo de trabajo.			X
2	Cumplo con las instrucciones recibidas de la coordinación de grupo en relación a la elaboración del proyecto de graduación.			X
3	Participo activamente en las reuniones contribuyendo a resolver problemas encontrados por mis compañeros en la investigación y el diseño del proyecto.			X
4	Cumplo con los pasos y requisitos del plan de trabajo y diseño del proyecto.			X
5	Respeto el orden de las fases del diseño del proyecto.			X
6	Atiendo las orientaciones de mis compañeros para resolver dificultades en el proceso de la elaboración del proyecto.			X
7	Cumplo con las tareas asignadas por la coordinación del grupo y las entrego en el tiempo estipulado.			X
8	Tengo una actitud positiva hacia la elaboración del proyecto de graduación.			X

Nunca:

A veces:

Siempre:

Proyecto de graduación

Autoevaluación

Nombre del alumno: Jezzer Abimael Jiménez López

Grupo No.: **Área de especialización:** SOC-CTIS-DFIR

Nombre del proyecto: Implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR

Fecha: Domingo 26 noviembre 2023

No.	ACTIVIDAD	NUNCA	A VECES	SIEMPRE
1	Asisto regularmente a las reuniones de grupo de trabajo.			X
2	Cumplo con las instrucciones recibidas de la coordinación de grupo en relación a la elaboración del proyecto de graduación.			X
3	Participo activamente en las reuniones contribuyendo a resolver problemas encontrados por mis compañeros en la investigación y el diseño del proyecto.			X
4	Cumplo con los pasos y requisitos del plan de trabajo y diseño del proyecto.			X
5	Respeto el orden de las fases del diseño del proyecto.			X
6	Atiendo las orientaciones de mis compañeros para resolver dificultades en el proceso de la elaboración del proyecto.			X
7	Cumplo con las tareas asignadas por la coordinación del grupo y las entrego en el tiempo estipulado.			X
8	Tengo una actitud positiva hacia la elaboración del proyecto de graduación.			X

Nunca:

A veces:

Siempre:

Anexos 3. Coevaluaciones



Programa Certificación en Ciberseguridad

Proyecto de graduación

Coevaluación

Nombre del alumno: Kevin Fabricio Alvarado Buezo
Grupo No.: Área de especialización: SOC-CTIS-DFIR
Nombre del proyecto: Implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR
Fecha: Domingo 26 noviembre 2023

No.	ACTIVIDAD	NUNCA	A VECES	SIEMPRE
1	Asiste regularmente a las reuniones de grupo de trabajo.			X
2	Cumple con las instrucciones recibidas de la coordinación de grupo en relación a la elaboración del proyecto de graduación.			X
3	Participa activamente en las reuniones contribuyendo a resolver problemas encontrados por mis compañeros en la investigación y el diseño del proyecto.			X
4	Cumple con los pasos y requisitos del plan de trabajo y diseño del proyecto.			X
5	Respeta el orden de las fases del diseño del proyecto.			X
6	Atiende las orientaciones de sus compañeros para resolver dificultades en el proceso de la elaboración del proyecto.			X
7	Cumple con las tareas asignadas por la coordinación del grupo y las entrega en el tiempo estipulado.			X
8	Tiene una actitud positiva hacia la elaboración del proyecto de graduación.			X

Nunca:

A veces:

Siempre:

Proyecto de graduación

Coevaluación

Nombre del alumno: Héctor Josué Ponsoy Ayala
Grupo No.: Área de especialización: SOC-CTIS-DFIR
Nombre del proyecto: Implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR
Fecha: Domingo 26 noviembre 2023

No.	ACTIVIDAD	NUNCA	A VECES	SIEMPRE
1	Asiste regularmente a las reuniones de grupo de trabajo.			X
2	Cumple con las instrucciones recibidas de la coordinación de grupo en relación a la elaboración del proyecto de graduación.			X
3	Participa activamente en las reuniones contribuyendo a resolver problemas encontrados por mis compañeros en la investigación y el diseño del proyecto.			X
4	Cumple con los pasos y requisitos del plan de trabajo y diseño del proyecto.			X
5	Respeto el orden de las fases del diseño del proyecto.			X
6	Atiende las orientaciones de sus compañeros para resolver dificultades en el proceso de la elaboración del proyecto.			X
7	Cumple con las tareas asignadas por la coordinación del grupo y las entrego en el tiempo estipulado.			X
8	Tiene una actitud positiva hacia la elaboración del proyecto de graduación.			X

Nunca:

A veces:

Siempre:

Proyecto de graduación

Coevaluación

Nombre del alumno: Franklin Benito Mayorga Baquedano
 Grupo No.: Área de especialización: SOC-CTIS-DFIR
 Nombre del proyecto: Implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR
 Fecha: Domingo 26 de noviembre 2023

No.	ACTIVIDAD	NUNCA	A VECES	SIEMPRE
1	Asiste regularmente a las reuniones de grupo de trabajo.			X
2	Cumple con las instrucciones recibidas de la coordinación de grupo en relación a la elaboración del proyecto de graduación.			X
3	Participa activamente en las reuniones contribuyendo a resolver problemas encontrados por mis compañeros en la investigación y el diseño del proyecto.			X
4	Cumple con los pasos y requisitos del plan de trabajo y diseño del proyecto.			X
5	Respeto el orden de las fases del diseño del proyecto.			X
6	Atiende las orientaciones de sus compañeros para resolver dificultades en el proceso de la elaboración del proyecto.			X
7	Cumple con las tareas asignadas por la coordinación del grupo y las entrego en el tiempo estipulado.			X
8	Tiene una actitud positiva hacia la elaboración del proyecto de graduación.			X

Nunca:

0

A veces:

5

Siempre:

10

Proyecto de graduación

Coevaluación

Nombre del alumno: Jezzer Abimael Jiménez López
Grupo No.: **Área de especialización:** SOC-CTIS-DFIR
Nombre del proyecto: Implementación de plataforma de aprendizaje para los aspirantes SOC-CTIS-DFIR
Fecha: Domingo 26 de noviembre 2023



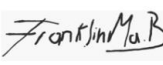




No.	ACTIVIDAD	NUNCA	A VECES	SIEMPRE
1	Asiste regularmente a las reuniones de grupo de trabajo.			X
2	Cumple con las instrucciones recibidas de la coordinación de grupo en relación a la elaboración del proyecto de graduación.			X
3	Participa activamente en las reuniones contribuyendo a resolver problemas encontrados por mis compañeros en la investigación y el diseño del proyecto.			X
4	Cumple con los pasos y requisitos del plan de trabajo y diseño del proyecto.			X
5	Respeto el orden de las fases del diseño del proyecto.			X
6	Atiende las orientaciones de sus compañeros para resolver dificultades en el proceso de la elaboración del proyecto.			X
7	Cumple con las tareas asignadas por la coordinación del grupo y las entrego en el tiempo estipulado.			X
8	Tiene una actitud positiva hacia la elaboración del proyecto de graduación.			X

Nunca:

A veces:

Siempre:

Anexos 4. Constancia de participación en la elaboración del proyecto

 Information Risk & Security Institute		Programa Certificación en Ciberseguridad				
CONSTANCIA DE PARTICIPACIÓN EN LA ELABORACIÓN DEL PROYECTO DE GRADUACIÓN						
Especialidad:		SOC-CTIS-DFIR				
Integrantes del grupo:		Franklin Benito Mayorga Baquedano Hector Josue Ponsoy Ayala Jezer Abimael Jimenez Lopez				
Coordinador del grupo:		Kevin Fabricio Alvarado Buezo				
Nombre del proyecto:		Entrenamiento para analista SOC				
	No.	FECHA	TIEMPO INVERTIDO		FIRMA	FIRMA PARTICIPANTE
			Hr. INICIO	Hr. finalización	COORDINADOR DE GRUPO	
Primer Entrega	1	Miercoles 27/09/2023	8:37 p. m.	10:58 a. m.		
	2	Domingo 01/10/2023	8:56 p. m.	10:51 p. m.		
	3	Miercoles 04/10/2023	8:16 p. m.	10:00 p. m.		
	4	Martes 10/10/2023	8:17 a. m.	10:10 p. m.		
	5	Jueves 12/10/2023	8:45 p. m.	10:00 p. m.		
	6	Domingo 15/10/2023	8:40 p. m.	10:30 p. m.		
	7	Viernes 20/10/2023	9:02 p. m.	10:32 p. m.		
Segunda Entrega	8	Domingo 22/10/2023	8:19 p. m.	10:40 p. m.		
	9	Miercoles 25/10/2023	8:00 p.m	11:00 p. m.		
	10	Lunes 30/10/2023	8:00 p.m	9:00 p. m.		
	11	Miercoles 08/11/2023	8:08 p.m.	10:13 pm		
Entrega Final	11	Junes 13/11/2023	8:18 p.m.	11:25 p.m.		
	12	Martes 14/11/2023	9:07 a. m.	10:25 a. m.		
	13	Lunes 20/11/2023	8:51 a.m	10:20 a. m.		
	14	Miercoles 22/11/2023	8:47 a.m	10:45 a.m		
	15	Viernes 24/11/2023	9:24 a.m	10:57 a.m		
	16	Domingo 26/11/2023	6:31 p.m	11:00 p.m		

Primer Entrega

FECHA		Descripcion
1	Miercoles 27/09/2023	Ideas para proyecto Debate sobre la idea mas idonea para nuestro proyecto Detalles mas especificos sobre la idea del proyecto Eleccion de la idea del proyecto (Plataforma web para curso SOC)
2	Domingo 01/10/2023	Investigacion sobre mejoras para proyecto Eleccion del alcance, finalidades, objetivos, justificacion. Elaboracion de la propuesta completa del proyeco
3	Miercoles 04/10/2023	Realizar el entregable Formato para resolución de casos planteamiento, solucion, alternativas, temas Trabajar en la plataforma wordpress Entregable completado y enviado según formato entregago
4	Martes 10/10/2023	Discusión e investigacion de los temas (SOC) detalles especificos sobre los modulos, contenido Alojamiento de la plataforma Trabajar en la plataforma wordpress Herramientas a utilizar en plataforma (wordpress)
5	Jueves 12/10/2023	Realizar propuesta de acuerdo al formato Eleccion de pluins para trabajo de la plataforma Detalles sobre contenidos y cuestionarios del curso Realizar el entregable nuevo de correccion de temas
6	Domingo 15/10/2023	Distribucion de asignaciones Confirmacion y verificacion de temas de contenido Preparacion de informe de primer avance parcial Busqueda del contenido asignado por cada integrante
7	Viernes 20/10/2023	Trabajar en el contenido especifico de los modulos Trabajar en el Alojamiento de la plataforma Metricas para aprobacion del curso Trabajar en la plataforma wordpress
8	Domingo 22/10/2023	Trabajar en el entregable parcial Realizar autoevaluacion y coevaluacion Realizar marco teorico, objetivos ,justificacion entre otras.

Segunda Entrega

9	Miercoles 25/10/2023	Se elaboro una distribucion de actividades en general Trabajar en el contenido de los cursos en especifico Ideas y mejoras para la plataforma en general Ideas y mejoras pruebas para los cursos
10	Lunes 30/10/2023	Implementar contenidos en los cursos Desarrollar la estructura general de los cursos Implementar las ideas mas idoneas según el cursos Integracion de contenido e imágenes en los cursos
8	Miercoles 08/11/2023	Retoques de la plataforma en general Ideas de como hacer mas didactica la pagina Mejorar en cuanto a navegacion de la plataforma Se realizo un curso modelo para tomarlo como guia Ideas sobre actividades interactivas en las lecciones
4	lunes 13/11/2023	Se agregaron fotos y redes sociales de los profesores Se terminaron detalles de documentación Realizacion de 6 cursos la mayormente con contenido estructurado Elaboracion y union del informe y detalles generales para entrega

NOTA:

Cabe mencionar que muchas asignaciones no hemos dependido exclusivamente de reuniones virtuales, hemos usado la red social WhatsApp a través de nuestro grupo para facilitar una comunicación más rápida y eficiente entre los miembros del grupo. Esta nos ha servido para la rápida división de tareas y la coordinación instantánea de asignaciones, división y comunicación en pro del proyecto.

Entrega Final

12	Martes 14/11/2023	Se elaboraron nuevas asignaciones
		Revision de asignaciones
		Entrega Division de trabajo
		Entrega de avances finales entre equipo en reuniones
		Asignaciones de los modulos finales
		Fechas de pruebas en la plataforma
		Fechas aproximadas de elaboracion de informe final
		Asignaciones de manuales del sistema
13	Lunes 20/11/2023	Finalizacion de asignaciones de detalles de los cursos
		Revision de avances asignados
		Mejoras en la plataforma (Login, Dashboard, Navegacion...)
		Elaboracion de preguntas para los cursos
14	Miercoles 22/11/2023	Revision de avances asignados
		Finalizacion de los modulos, lecciones y juegos en los cursos
		Asignaciones para elaboracion del informe final
		Elaboracion de manuales para uso del sistema
		Asignaciones para elaboracion de video introductorio para cada curso
		Elaboracion de encuesta para analisis de probabilidades
15	Viernes 24/11/2023	Asignaciones finales y puntos finales para entregas
		Detalles sobre el informe final
		Realizacion del analisis de probabilidades (Calculo de muestra según encuesta)
		Realizacion del examen final para los 10 cursos
		Detalles para la redaccion del informe final
16	Domingo 26/11/2023	Elaboracion del informe final
		Detalles de los diferentes manuales de la plataforma
		Elaboracion de videos descriptivos de la plataforma
		Revision General de la plataforma
		Verificacion del Examen final y examen diagnostico inicial en la plataforma

Anexos 5. Enlace de la demostración real de la plataforma en video

<https://youtu.be/sKZ6TWT9q2c>

