



Dirección de Proyectos II

DIVISIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN
INGENIERÍA EN REDES INTELIGENTES Y
CIBERSEGURIDAD

Producto 3. Formalización del cierre del proyecto.

INTEGRANTES DEL EQUIPO:

GARCÍA MARTÍNEZ LUIS DANIEL
CORTÉS ALCALÁ JESSICA BANELLY
DE LA ROSA VÁZQUEZ MARCO ANTONIO
RODRÍGUEZ LÓPEZ RICARDO

NOMBRE DE/LA PROFESOR (A):

NOLASCO HERNANDEZ JAVIER

Contenido

Introducción	3
Documento que acredita la aceptación del producto	4
Carta de aceptación del proyecto.....	5
Reporte final de desempeño del proyecto.....	6
Análisis Presupuestal	6
Análisis Global	7
Evaluación	8
Cumplimiento de Alcance del Proyecto	9
Lecciones aprendidas durante el desarrollo del proyecto	11
Final de Cierre y Reflexión del Proyecto	13
Repositorio del proyecto	15
Conclusión	16

Introducción

El presente informe representa la conclusión formal del proyecto titulado “Sistema de Detección de Intrusos (IDS)”, el cual fue diseñado, planeado y desarrollado a lo largo del primer cuatrimestre como parte integral de las actividades académicas de la asignatura Dirección de Proyectos I. Este documento tiene como finalidad registrar oficialmente la finalización del proyecto, a través de la presentación de los elementos clave que demuestran el cumplimiento de los objetivos establecidos, así como la correcta ejecución de cada una de sus fases.

El desarrollo del proyecto IDS fue concebido como una solución tecnológica orientada a reforzar la seguridad informática mediante la identificación de amenazas potenciales dentro de un entorno de red. Su implementación incluyó la integración de diversos módulos, como el monitoreo de tráfico, escaneo de puertos, verificación de dispositivos USB y análisis de archivos, todos unificados mediante una interfaz web funcional. A lo largo del proyecto se emplearon herramientas como Python, Flask, Scapy y Nmap, entre otras, que permitieron construir un sistema modular, intuitivo y práctico. Este informe incluye información detallada sobre varios aspectos esenciales: el documento que valida la aceptación del sistema por parte de los interesados, un análisis final del desempeño del proyecto considerando variables como cronograma, presupuesto y alcance, así como una reflexión profunda sobre las lecciones aprendidas durante el proceso. También se presenta un enlace o referencia al repositorio donde se encuentra alojada la totalidad del código, documentación técnica, presentaciones y entregables generados durante el ciclo de vida del proyecto. Cabe destacar que el cierre de un proyecto no se limita únicamente al cese de actividades operativas, sino que implica un proceso estructurado de revisión, documentación y análisis de resultados. Este proceso permite identificar aciertos y áreas de oportunidad, fortaleciendo así la experiencia profesional y académica de los participantes. En este contexto, el presente documento no sólo cumple una función informativa, sino también formativa, permitiendo establecer bases sólidas para la continuidad o mejora del sistema en futuras fases.

Con esta formalización del cierre, se concluye de manera exitosa la primera etapa de vida del sistema IDS, quedando disponible para futuras optimizaciones, adaptaciones o implementaciones en ambientes reales donde la detección temprana de amenazas digitales resulte crítica.

Documento que acredita la aceptación del producto

Una vez culminada la fase de pruebas funcionales del Sistema de Detección de Intrusos (IDS), se procedió a su presentación formal ante los principales interesados del proyecto, en este caso el docente responsable y el equipo de trabajo.

La revisión incluyó la demostración de todos los módulos desarrollados, así como su integración efectiva dentro de una interfaz web operativa.

Durante la sesión de validación se comprobó que el sistema cumplía con los requisitos funcionales y técnicos definidos desde la etapa de planificación, incluyendo:

- Monitoreo de tráfico de red mediante la captura y análisis de paquetes (TCP, UDP e ICMP).
- Escaneo de puertos sobre dispositivos objetivo, con validación previa de direcciones IP.
- Verificación de dispositivos USB conectados al sistema, con listas blancas configurables.
- Análisis de archivos cargados, con clasificación del estado del archivo y retroalimentación al usuario.
- Interfaz gráfica basada en Flask, permitiendo navegación fluida y acceso a cada módulo.

Con base en la revisión de resultados, evidencias prácticas y documentación técnica presentada, el producto fue formalmente aceptado, al demostrar que cumplía satisfactoriamente con los criterios de funcionalidad, estabilidad, usabilidad y documentación. Este hecho fue registrado en un acta de aceptación, firmada por el docente evaluador, que se integra como parte del cierre formal del proyecto.

Carta de aceptación del proyecto

DIRECCIÓN GENERAL DE INNOVACIÓN
Y DESARROLLO TECNOLÓGICO

ACTA DE ACEPTACIÓN DEL PROYECTO

Dirección de Proyectos Especiales

NOMBRE DEL PROYECTO
Desarrollo e Implementación de un Sistema IDS con Interfaz Web
NOMBRE DEL CLIENTE

DESCRIPCIÓN		
Proyecto académico desarrollado por el equipo liderado por Marco de la Rosa Vázquez, consistente en la creación de un prototipo funcional de un sistema de detección de intrusos (IDS), con el objetivo de identificar, registrar y alertar sobre posibles accesos no autorizados dentro de una red local. El sistema cuenta con una interfaz web para el monitoreo de eventos en tiempo real.		
Partes funcionales del proyecto	Descripción	Observaciones
Monitoreo de red	Registro de tráfico en tiempo real y visualización de posibles anomalías.	Funcionando correctamente
Escaneo de puertos	Identificación de puertos abiertos en dispositivos conectados.	Cumple con lo especificado
Análisis de archivos	Revisión de archivos con posible contenido malicioso.	Funcionamiento confirmado
Verificación de dispositivos USB	Detección automática y registro de dispositivos conectados.	Funcionalidad operativa
Interfaz web	Plataforma gráfica accesible para controlar y visualizar el IDS.	Interfaz estable y funcional
OBSERVACIONES ADICIONALES		
El producto cumple con todos los requisitos funcionales establecidos en la planeación del proyecto. Las pruebas de validación fueron satisfactorias. Se sugiere continuar con su perfeccionamiento para su integración en entornos más amplios. Proyecto adecuado para fines académicos y como base para aplicaciones de seguridad reales.		
FUNCIONALIDADES DEL PROYECTO		
ENTREGABLE	DESCRIPCIÓN	
Sistema IDS	Ejecutable funcional con detección de intrusos locales.	
Interfaz Web	Acceso a funciones de monitoreo, escaneo y análisis de eventos.	
Informe de pruebas funcionales	Documento detallado que respalda el funcionamiento del sistema.	
Evidencia operativa	Capturas y logs.	
ACEPTADO		
NOMBRE	FIRMA	
Nolasco Hernandez Javier		

Elaborado:

Aprobado:

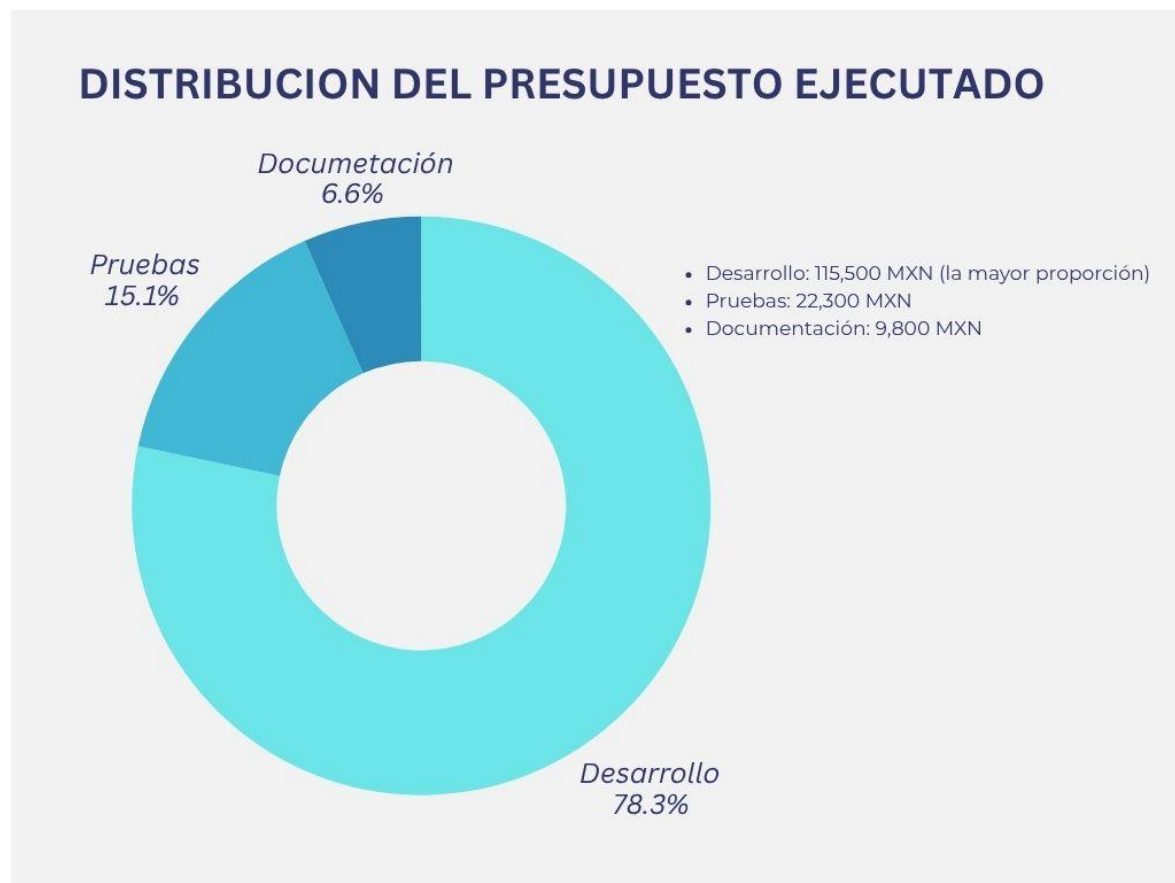
Reporte final de desempeño del proyecto

Durante el desarrollo del proyecto Sistema de Detección de Intrusos (IDS) se realizó un seguimiento continuo a los tres pilares fundamentales: **presupuesto, cronograma y alcance**, con el fin de asegurar que los entregables se ajustarán a las metas pactadas. A continuación, se presenta el análisis completo:

Análisis Presupuestal

Durante la planeación del Sistema de Detección de Intrusos (IDS), se asignó un presupuesto total de \$150,000 MXN, el cual se distribuyó en rubros estratégicos relacionados con el ciclo de vida del proyecto: desarrollo, pruebas y documentación. Esta asignación respondió a un análisis inicial de necesidades técnicas, tiempos estimados de implementación y herramientas a utilizar.

A lo largo del proyecto, el control presupuestal fue uno de los pilares fundamentales para asegurar la viabilidad del desarrollo, evaluando constantemente los gastos reales frente a lo planificado. A continuación, se presenta una tabla con el desglose financiero, seguido de un análisis detallado por cada rubro:



Concepto	Presupuestado (\$)	Ejecutado (\$)	Desviación (\$)	% Desviación	Justificación Técnica
Desarrollo	\$120,000	\$115,500	-\$4,500	-3.75%	Se reaprovecharon fragmentos de código de proyectos anteriores, reduciendo tiempo de desarrollo. -Se optó por librerías y herramientas de código abierto (open source), como Flask, Nmap, Scapy y PyUSB, evitando costos por licencias. -El equipo realizó trabajo paralelo en módulos, maximizando el uso de horas hombre.
Pruebas	\$20,000	\$22,300	+\$2,300	+11.5%	- Se amplió el alcance de pruebas para incluir escenarios más complejos, como ataques simulados y pruebas de estrés. - Se realizaron validaciones cruzadas en múltiples entornos operativos: Ubuntu, Windows. - Hubo inversión en herramientas de escaneo y análisis adicionales no contempladas inicialmente.
Documentación	\$10,000	\$9,800	-\$200	-2.00%	- Se utilizaron plantillas estandarizadas y herramientas gratuitas como Google Docs - Parte de la documentación fue realizada durante el desarrollo, lo cual redujo tiempo y costos en la etapa final.

| Totales | \$150,000 | \$147,600 | -\$2,400 | -1.6% | El proyecto finalizó por debajo del presupuesto general sin comprometer funcionalidad, calidad o alcance.

Análisis Global

El desempeño financiero del proyecto fue eficiente, mostrando un ahorro del 1.6% sobre el total proyectado. Esta eficiencia no fue producto de recortes o limitaciones, sino de decisiones estratégicas bien fundamentadas durante la ejecución. La reutilización de recursos, el uso de tecnologías libres y la planificación adecuada de tareas permitieron reducir costos sin impactar en la calidad del entregable. En el caso del incremento en pruebas, aunque representó una desviación positiva, esta se justifica plenamente: se mejoró la confiabilidad del sistema al probarlo en múltiples escenarios reales, lo que refuerza su estabilidad y valor funcional. Esta inversión fue clave para garantizar un IDS robusto y con menor probabilidad de fallos en operación.

Por otro lado, los ahorros en el desarrollo y documentación fueron resultado de la experiencia del equipo y la madurez de sus procesos, lo que permitió trabajar con eficiencia sin requerir horas extra o contratar servicios externos.

Evaluación del Cronograma

Se estableció un cronograma del 05 de febrero al 16 de mayo de 2025, distribuido en siete fases. A continuación, se presenta una tabla comparativa con las desviaciones encontradas, seguida de un desglose detallado:

<i>Fase</i>	<i>Actividades Clave</i>	<i>Fechas de Ejecución</i>
1. Análisis y Recolección de Requisitos	<ul style="list-style-type: none"> Definición del problema- Investigación preliminar. Revisión de tecnologías y herramientas 	05 – 16 de febrero 2025
2. Diseño de Arquitectura	<ul style="list-style-type: none"> Diseño de módulos (red, USB, escaneo, archivos). Diseño de la interfaz web Planeación de la integración 	17 – 28 de febrero 2025
3. Desarrollo de Módulos	<ul style="list-style-type: none"> Programación del módulo de red Módulo de escaneo de puertos. Verificación de USB. Análisis de archivos 	01 – 28 de marzo 2025
4. Desarrollo de Interfaz Web e Integración con Flask	<ul style="list-style-type: none"> Diseño visual (UI). Integración de todos los módulos al sistema web. Validaciones de entrada y navegación 	01 – 14 de abril 2025
5. Pruebas Funcionales y Correcciones	<ul style="list-style-type: none"> Pruebas individuales por módulo. Pruebas del sistema integrado. Corrección de errores (bugs) 	15 – 25 de abril 2025
6. Documentación y Manual de Usuario	<ul style="list-style-type: none"> Documentación técnica. Manual de instalación y uso. Preparación de presentaciones 	26 de abril – 2 de mayo 2025
7. Evaluación Final y Presentación del Proyecto	<ul style="list-style-type: none"> Entrega de entregables finales Presentación ante el docente Retroalimentación y cierre 	05 – 16 de mayo 2025

Diagrama de Gantt del proyecto






Cumplimiento de Alcance del Proyecto

Durante la fase de planificación del Sistema de Detección de Intrusos (IDS), se definió un alcance técnico claro y delimitado para asegurar el cumplimiento de los objetivos dentro del cronograma y presupuesto establecidos. El alcance se centró en el desarrollo de seis módulos funcionales clave, orientados a cubrir distintos vectores de ataque comunes en entornos de red locales y estaciones de trabajo.

A lo largo de la ejecución del proyecto, el equipo mantuvo un riguroso control sobre el cumplimiento de este alcance mediante revisiones periódicas, reuniones técnicas y sesiones de pruebas funcionales

Módulos Desarrollados:

MÓDULO	TECNOLOGÍA BASE	ESTADO ACTUAL	OBSERVACIONES TÉCNICAS
MONITOREO DE RED	Scapy	 Completado	Permite la captura y análisis de tráfico en tiempo real; compatible con protocolos TCP, UDP e ICMP. Se incorporó la detección automática de interfaz de red.
ESCANEO DE PUERTOS	Nmap + Python	 Completado	Ejecuta escaneos rápidos y precisos sobre direcciones IP configuradas. Se validan las IPs antes de escanear para evitar errores.
VERIFICACIÓN DE USB	PyUSB	 Completado	Detecta y compara dispositivos conectados

ANÁLISIS DE ARCHIVOS	Python (I/O, os)	✓ Completado	contra una lista blanca configurable. Alertas en caso de USB desconocido. Revisa la extensión, contenido y metadatos de archivos subidos. Informa si son sospechosos o potencialmente maliciosos.
INTERFAZ WEB	Flask + Bootstrap	✓ Completado	Permite acceso intuitivo a todos los módulos desde un único panel. Incluye navegación por pestañas, validaciones de entrada y alertas al usuario.
DOCUMENTACIÓN TÉCNICA	PDF	✓ Completado	Se elaboró manual de instalación paso a paso, pruebas de módulos y diagrama general del sistema.

- Entregables completados: 6 de 6
- Porcentaje de alcance logrado: 100%

Exclusiones Justificadas y Planes Futuros

Aunque el proyecto logró entregar el 100% del alcance definido formalmente, existieron funcionalidades complementarias que se discutieron durante la ejecución y que, por razones técnicas y estratégicas, fueron excluidas de esta primera fase. A continuación, se documentan estas decisiones:

<i>Elemento No Implementado</i>	<i>Justificación Técnica</i>	<i>Plan de Implementación Futura</i>
<i>Sistema de autenticación de usuarios</i>	Implicaba el diseño de roles, base de datos de usuarios y seguridad adicional. Se priorizó la funcionalidad core del IDS.	Será incorporado en la Fase 2 , con un presupuesto estimado de \$15,000 MXN .
<i>Registro histórico de alertas</i>	Requería base de datos persistente y lógica adicional para filtrado y búsqueda. Por tiempo limitado, se pospuso.	Será desarrollado en el siguiente sprint del proyecto.

Estas exclusiones no afectan el desempeño ni la funcionalidad básica del sistema IDS. Al contrario, reflejan una gestión prudente del alcance, evitando saturar la primera versión del sistema y permitiendo una implementación más sólida y enfocada.

Lecciones aprendidas durante el desarrollo del proyecto

El desarrollo del Sistema de Detección de Intrusos (IDS) representó un proceso integral de aprendizaje y mejora continua para todos los integrantes del equipo. Más allá de cumplir con los objetivos técnicos, este proyecto permitió identificar buenas prácticas, áreas de oportunidad, errores comunes y estrategias efectivas que fortalecieron nuestras competencias en gestión de proyectos, desarrollo de software y colaboración en equipo. A continuación, se detallan las principales lecciones aprendidas a lo largo de las diferentes fases:

1. Planificación realista y con márgenes de contingencia

Uno de los aprendizajes más importantes fue la necesidad de contar con una planificación minuciosa y realista desde el inicio del proyecto. Aunque se elaboró un cronograma bien estructurado, se subestimó la complejidad técnica de ciertos módulos, especialmente en lo relativo al uso de herramientas como Scapy para el monitoreo de red o nmap para el escaneo de puertos. Esto generó ligeras desviaciones en los tiempos estimados. Aprendimos que es fundamental incorporar márgenes de contingencia en el cronograma, así como realizar validaciones tempranas para ajustar tiempos y recursos conforme a la dificultad técnica real de las tareas.

2. Capacidad de adaptación ante problemas técnicos

Durante el proceso de implementación surgieron varios retos técnicos inesperados, como incompatibilidades con redes WiFi, problemas al ejecutar scripts en distintos sistemas operativos o dificultades en la integración con Flask. Estas situaciones obligaron al equipo a desarrollar habilidades de resolución de problemas en tiempo real, buscando documentación oficial, foros técnicos y soluciones creativas. Esta experiencia reforzó la importancia de la flexibilidad, la disposición al aprendizaje autodidacta y la necesidad de prever entornos de prueba diversos desde el inicio del proyecto.

3. Comunicación efectiva y trabajo colaborativo

Una fortaleza clave del equipo fue el establecimiento de una comunicación constante y fluida. Se realizaron reuniones semanales de seguimiento, se usaron herramientas colaborativas como GitHub y Trello, y se mantuvo un canal abierto de mensajería para resolver dudas rápidamente. Esto favoreció una distribución equitativa de tareas, facilitó la integración entre módulos y permitió mantener la motivación alta durante las semanas de mayor carga. Esta experiencia reafirmó que una comunicación clara, respetuosa y orientada a objetivos es esencial para el éxito de cualquier proyecto multidisciplinario.

4. Gestión controlada de cambios

A lo largo del desarrollo, surgieron diversas solicitudes de cambio: algunas originadas por hallazgos técnicos (como la necesidad de detectar automáticamente interfaces de red activas), otras por recomendaciones del profesor, y otras por mejoras propuestas desde el propio equipo (como la optimización de la interfaz

web). Estas solicitudes se documentaron en una bitácora de cambios, lo que permitió analizarlas, priorizarlas e implementarlas sin perder el control del proyecto ni desviarse del alcance aprobado. Aprendimos que contar con una política clara de evaluación y aceptación de cambios es clave para mantener la coherencia del proyecto.

5. Valor de la documentación continua

Inicialmente, se dio mayor prioridad a la programación que a la documentación, lo que dificultó la integración entre módulos y la comprensión de funciones ajenas. Al reconocer este error, se implementó un sistema de documentación técnica desde el código fuente hasta los manuales de usuario. Esta decisión mejoró la comunicación interna, facilitó la presentación del proyecto y preparó el camino para futuras actualizaciones. Esta lección nos enseñó que la documentación no debe dejarse al final, sino desarrollarse en paralelo con el producto.

6. Monitoreo constante del rendimiento del proyecto

Gracias a la implementación de la metodología del valor ganado (EVM), se pudo dar seguimiento a la eficiencia del proyecto en términos de tiempo y costo. Esto permitió detectar desviaciones en tiempo real y tomar decisiones oportunas, como reasignar tareas o simplificar funcionalidades secundarias. Evaluar métricas como el SPI (Índice de Desempeño de Cronograma) y el CPI (Índice de Desempeño de Costos) resultó valioso para visualizar el avance de forma objetiva, lo que sin duda será incorporado en futuros desarrollos.

7. Experiencia de usuario como parte fundamental del producto

Una de las lecciones más reveladoras fue entender que el éxito de un sistema no se basa únicamente en su funcionalidad técnica, sino también en su usabilidad. La retroalimentación recibida sobre la interfaz gráfica, los botones de navegación, los mensajes de alerta y la organización visual fue clave para realizar mejoras significativas. Aprendimos que es necesario involucrar al usuario final en las fases de prueba para garantizar que el producto final sea amigable, intuitivo y funcional.

8. Preparación para futuras fases de desarrollo

Finalmente, este proyecto nos permitió identificar áreas que podrían ampliarse en una segunda etapa, como la autenticación de usuarios, el almacenamiento de registros históricos y la implementación de paneles de análisis más avanzados. El hecho de haber dejado documentados estos elementos nos da una base sólida para escalar el sistema en el futuro de manera ordenada y eficiente.

Final de Cierre y Reflexión del Proyecto

Al concluir el desarrollo del IDS, se llevó a cabo una reunión formal de cierre del proyecto, cuyo objetivo fue reflexionar sobre los logros, dificultades y aprendizajes obtenidos durante todo el proceso. Esta reunión consolidó el cierre formal del proyecto desde una perspectiva técnica y de gestión.

Durante la sesión se abordaron los siguientes temas:

- Evaluación del desempeño por módulo: Se revisó el cumplimiento de los entregables según el alcance definido. Se destacaron los módulos que cumplieron al 100% y aquellos que enfrentaron dificultades técnicas.
- Reconocimiento de aportes individuales: Cada integrante compartió sus experiencias, aportaciones y desafíos. Este ejercicio fortaleció el sentido de colaboración y la valoración del trabajo del equipo.
- Sugerencias para mejoras futuras: Se discutieron ideas para optimizar la organización del código, la segmentación de tareas, y la documentación desde etapas más tempranas. También se propuso implementar autenticación de usuarios en una segunda fase.

Esta actividad reforzó los principios aprendidos en la materia sobre la importancia del cierre formal de los proyectos, destacando:

- La validación final de los entregables.
- La reflexión crítica como motor de mejora continua.
- La documentación de recomendaciones para futuras versiones del sistema o nuevos desarrollos tecnológicos.

Acta de reunión



AASUNTO: CIERRE FORMAL DEL PROYECTO IDS

Fecha: 17 de mayo de 2025

Hora: 16:00 a 17:00 Hrs

Lista de asistentes

- Marco Antonio De la Rosa Vázquez
- Luis Daniel García Martínez
- Jessica Banelly Cortez Alcalá
- Ricardo Rodríguez López

Agenda

1. Propuestas de mejora y posibles desarrollos futuros del IDS.
2. Confirmación del cumplimiento de entregables y criterios de calidad.
3. Acuerdos para el cierre formal del proyecto.

Responsabilidades y plazos

- Subir versión final de entregables al repositorio
- Respaldo proyecto en nube (Google Drive)
- Subir código y documentación final a GitHub
- Firmar y entregar acta de aceptación del producto

Resumen de discusiones

Temas tratados:

- Revisión del cumplimiento de objetivos generales y específicos.
- Evaluación del cronograma y desviaciones menores.
- Análisis del desempeño del equipo y coordinación.
- Reflexión sobre lecciones aprendidas por módulo.
- Sugerencias para futuras mejoras y versiones del IDS.
- Confirmación del cumplimiento de entregables y criterios de calidad.

Acuerdos:

- Consolidar los entregables y subirlos al repositorio final del equipo.
- Incluir todas las mejoras aplicadas en la documentación técnica.
- Formalizar el cierre del proyecto con el acta de aceptación del producto.
- Aplicar los aprendizajes para futuros proyectos de ciberseguridad

Observaciones

Se valoró el compromiso del equipo y la mejora continua durante el proceso.

Se acordó guardar respaldo del proyecto en la nube y GitHub.

Repositorio del proyecto

El repositorio del proyecto IDS (Sistema de Detección de Intrusos) constituye una recopilación estructurada y respaldada de todos los componentes técnicos y documentales generados a lo largo del desarrollo del proyecto. Su objetivo principal es centralizar los entregables en un espacio digital accesible para su consulta, reutilización, mejora o auditoría futura, garantizando la trazabilidad del trabajo realizado.

Este repositorio no solo facilita la revisión académica y técnica del proyecto, sino que también promueve la transparencia, la colaboración y la posibilidad de continuidad en versiones futuras del sistema.

Contenido del Repositorio:

Código Fuente Completo del Proyecto:

- Archivo principal app.py que gestiona las rutas e integra los módulos.

Módulos independientes de:

- Monitoreo de tráfico de red (network_monitor.py)
- Escaneo de puertos (port_scanner.py)
- Detección de dispositivos USB (usb_detector.py)
- Análisis de archivos (file_analyzer.py)
- Plantillas HTML (templates/) para la interfaz web.
- Archivos estáticos (static/) como CSS, imágenes y scripts.

Documentación Técnica:

- Manual del desarrollador: explica estructura del proyecto, dependencias y funcionamiento interno de cada módulo.
- Requisitos técnicos y configuraciones del entorno (archivo requirements.txt).
- Comentarios técnicos sobre versiones de librerías utilizadas y su compatibilidad.

Evidencias del Funcionamiento:

- Capturas de pantalla del sistema en operación.
- Resultados de pruebas realizadas a cada módulo por separado y de forma integrada.

Reportes Académicos:

- Producto 1: Ejecución del Proyecto
- Producto 2: Seguimiento y Control del Proyecto
- Producto 3: Cierre Formal del Proyecto (este documento)

Enlace al Repositorio Oficial del Proyecto

El repositorio se encuentra almacenado en una plataforma de colaboración digital, accesible para el equipo, el docente y otros interesados.

[enlace directo aquí — GitHub: <https://github.com/danyfreaking/Proyecto-IDS.git>

Conclusión

El desarrollo del proyecto titulado Sistema de Detección de Intrusos (IDS) representó una experiencia académica y técnica enriquecedora, en la que se integraron múltiples disciplinas, herramientas y metodologías vistas a lo largo del curso. Este proyecto no solo fue un ejercicio práctico de implementación de software, sino una aproximación realista a los procesos de planificación, ejecución, control y cierre que conlleva un proyecto tecnológico formal.

La construcción de este sistema permitió abordar una problemática concreta del ámbito de la ciberseguridad: la necesidad de contar con una herramienta integral que detecte comportamientos sospechosos o no autorizados dentro de una red o sistema informático. A través del uso de tecnologías como Python, Flask, Scapy, PyUSB y Nmap, se logró desarrollar una solución funcional, modular y accesible que abarca el monitoreo de tráfico de red, escaneo de puertos, verificación de dispositivos USB y análisis de archivos. Todos estos componentes fueron integrados en una interfaz web intuitiva, diseñada para facilitar su uso incluso por usuarios no técnicos.

Durante el ciclo de vida del proyecto, se aplicaron buenas prácticas de gestión, tales como la segmentación por fases, el establecimiento de cronogramas realistas, la asignación clara de responsabilidades y la documentación constante de avances y cambios. La supervisión continua del progreso mediante indicadores de valor ganado permitió realizar ajustes en tiempo real y asegurar el cumplimiento de los objetivos. A pesar de los retos técnicos, como la compatibilidad de ciertas librerías o la detección de interfaces de red, el equipo logró resolverlos mediante investigación, colaboración y adaptación. Desde una perspectiva formativa, el proyecto también fue una oportunidad para fortalecer habilidades blandas fundamentales, como el trabajo en equipo, la comunicación asertiva, la toma de decisiones bajo presión y la gestión del tiempo. Cada miembro del equipo pudo aportar desde su experiencia y habilidades particulares, lo que generó un ambiente de colaboración enriquecedor. La realización de reuniones de control, la generación de actas y minutas, así como el cumplimiento riguroso de entregables, simulaban con fidelidad la dinámica profesional de los proyectos reales del ámbito TI.

La validación final del producto, respaldada por el acta de aceptación firmada, certifica que el sistema cumple con los requisitos funcionales, técnicos y de calidad definidos en la etapa inicial. Asimismo, la sesión de cierre permitió reflexionar sobre los logros alcanzados y sobre las áreas en las que se podría mejorar para futuras versiones, como la inclusión de un módulo de autenticación o una mejor estrategia para pruebas automatizadas.

En conclusión, el proyecto IDS no solo alcanzó sus metas técnicas y de gestión, sino que también se consolidó como una experiencia integral de aprendizaje. El producto entregado es funcional, pertinente y aplicable a escenarios reales. A su vez, el proceso dejó aprendizajes duraderos que servirán de base para futuros desarrollos, fortaleciendo las competencias profesionales del equipo. Este cierre no representa un fin, sino el punto de partida hacia nuevos desafíos y oportunidades de mejora continua.