Dirección de Proyectos II

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

Producto 2. Seguimiento y control 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

Propósito del Reporte:

Este documento tiene como objetivo presentar un informe detallado sobre la ejecución y el estado actual del proyecto *Sistema de Detección de Intrusos (IDS)*, desarrollado como parte de la asignatura Dirección de Proyectos II. El reporte recopila los entregables generados, el desempeño del equipo, las actividades de aseguramiento de la calidad, los riesgos identificados y las acciones correctivas implementadas. Además, sirve como herramienta de seguimiento para garantizar que el proyecto cumpla con los estándares técnicos y los plazos establecidos, facilitando la transparencia y la comunicación con los interesados.

Estado Actual del Proyecto:

El proyecto se encuentra en su primera fase de desarrollo, habiendo cumplido con los objetivos iniciales planteados. Se han implementado y probado con éxito los módulos clave del sistema, incluyendo:

- Monitoreo de tráfico de red en tiempo real mediante Scapy.
- Escaneo de puertos utilizando Nmap.
- Verificación de dispositivos USB conectados con PyUSB.
- Análisis de archivos sospechosos.

La integración de estos módulos se realizó a través de una interfaz web desarrollada con Flask, la cual ha demostrado ser funcional y amigable para el usuario. El equipo ha completado todas las fases programadas (análisis, diseño, desarrollo, pruebas y documentación) dentro de los plazos establecidos, sin retrasos significativos.

Objetivos del Seguimiento:

1. **Monitorear el cumplimiento de los objetivos técnicos:** Asegurar que los módulos desarrollados cumplan con los requisitos funcionales y no funcionales definidos inicialmente.
2. **Evaluar la calidad del sistema:** Continuar con las pruebas de rendimiento y usabilidad para identificar áreas de mejora y garantizar la estabilidad del sistema en entornos reales.

3. **Gestionar riesgos emergentes:** Documentar y mitigar nuevos riesgos identificados durante las pruebas, como la sobrecarga del sistema en redes con alto tráfico o la compatibilidad con distintos sistemas operativos.
4. **Optimizar el trabajo en equipo:** Mantener una comunicación efectiva entre los integrantes, redistribuir tareas si es necesario y fomentar la colaboración para abordar los desafíos técnicos.
5. **Preparar la siguiente fase del proyecto:** Planificar las mejoras futuras, como la implementación de autenticación de usuarios, la optimización del rendimiento y la ampliación de funcionalidades.

1. Solicitudes de cambio.

Las Solicitudes de Cambio son herramientas fundamentales en la gestión de proyectos que permiten documentar, evaluar y autorizar modificaciones al alcance, diseño o funcionalidades de un sistema. En el contexto del proyecto IDS, cumplen estos propósitos clave:

Funciones principales
Control de modificaciones

- Registran cambios técnicos (como la lista JSON para USBs o la validación de archivos) para mantener trazabilidad.
- Evitan alteraciones no autorizadas que podrían generar riesgos (ej.: vulnerabilidades de seguridad).

Evaluación de impactos

- Analizan efectos en cronograma, costos, calidad y stakeholders (usuarios, equipo, clientes).
- Ejemplo: La solicitud SC-004 previó cómo afectaría a administradores y flujo de trabajo (p.15 del PDF).

Comunicación estructurada

- Formalizan acuerdos entre equipos (desarrollo, QA, gestión) y stakeholders (como el profesor asesor).
- Se vinculan con minutas de reunión (p.19) y bitácoras (p.17) del proyecto IDS.

Prevención de errores

- Documentan causas raíz (ej.: falsos positivos en USB) y acciones preventivas/correctivas.
- Referencian incidentes previos (p.12, p.16) para evitar repetición.

Importancia en el proyecto IDS
- Garantizan calidad: Alinean cambios con requisitos originales (p.4) y estándares de QA (p.9-11).
- Optimizan recursos: Priorizan modificaciones con mayor ROI (ej.: SC-003 redujo errores en 90% con 3 horas de trabajo).
- Facilitan mantenimiento: Historial de cambios (p.17) ayuda en futuras actualizaciones.

- Gestionan riesgos: Mitigan problemas como sobrecarga del sistema (p.13) o incompatibilidades (p.14).

Durante el desarrollo del IDS, se identificaron varias necesidades de cambio, ya sea por mejoras técnicas, experiencia de usuario o corrección de fallos. A continuación, se resumen los principales:

Nº	**Descripción del Cambio**	**Razón**	**Impacto**	**Aprobación**	**Fecha**
1	Detección automática de interfaz activa (WiFi/Ethernet)	Scapy fallaba con ciertas redes	Calidad y funcionalidad	Aprobado	15-mayo-2025
2	Validación de tipo de archivo y extensión	Prevenir errores al subir archivos	Seguridad y experiencia	Aprobado	17-mayo-2025
3	Lista externa para USB autorizadas	Facilitar edición sin modificar código	Usabilidad y mantenimiento	Aprobado	20-mayo-2025

1.1 Ejemplo de solicitud de cambio en nuestro proyecto.

Solicitud de cambio
Fecha: *14/05/2025*

Datos de la solicitud de cambio

Nro control de solicitud de cambio	SC-001
Solicitante del cambio	Equipo de Desarrollo IDS
Área del solicitante	Desarrollo y Aseguramiento de Calidad
Lugar	
Gerente del proyecto	Prof. Nolasco Hernández Javier

Categoría de cambio

Marcar todas las que apliquen:

☐ Alcance ☐ Cronograma ☐ Costos ☒ Calidad ☐ Recursos
☐ Procedimientos ☐ Documentación ☐ Otro

Causa / origen del cambio

☐ Solicitud de cliente ☒ Reparación de defecto ☐ Acción correctiva
☐ Acción preventiva ☐ Actualización / Modificación de documento
☐ Otros

Descripción de la propuesta de cambio

Implementar un script que detecte automáticamente la interfaz de red activa (WiFi/Ethernet) y ajuste Scapy para capturar tráfico sin errores. Incluir mensajes de advertencia al usuario si no se detecta tráfico.

Justificación de la propuesta de cambio

Garantizar la funcionalidad del módulo de monitoreo en entornos reales con múltiples interfaces (sección 6 del informe). Evitar fallos reportados durante pruebas (sección 7).

Impacto del cambio en la línea base

Alcance:Módulo de monitoreo de red (Scapy)

Cronograma:Implementación: 15-mayo-2025

Costo:Sin costos adicionales (utiliza recursos existentes).

Calidad:Mejora en la precisión de detección de tráfico en redes WiFi/Ethernet.

Implicaciones de recursos (materiales y capital humano)

Alcance: Solo afecta al módulo de monitoreo. Cronograma: 15-mayo-2025. Costo: Cero. Calidad: Aumenta confiabilidad. Recursos: 8 horas de desarrollo.

Implicaciones para los interesados

· Equipo de desarrollo: Capacitación en el nuevo script de detección de interfaz.
· Usuarios finales: Mayor confiabilidad en el monitoreo de red.
· Docente/Cliente: Validación requerida en el informe de avance.
· Administradores de red: Reducción de falsos negativos en alertas.

Aprobación

Ejemplo 2.

Solicitud de cambio
Fecha: *16/05/2025*

Datos de la solicitud de cambio

Nro control de solicitud de cambio	SC-003
Solicitante del cambio	Ricardo Rodríguez López
Área del solicitante	Desarrollo
Lugar	
Gerente del proyecto	Prof. Nolasco Hernández Javier

Categoría de cambio

Marcar todas las que apliquen:

☐ Alcance ☐ Cronograma ☐ Costos ☒ Calidad ☐ Recursos
☐ Procedimientos ☐ Documentación ☐ Otro

Causa / origen del cambio

☐ Solicitud de cliente ☐ Reparación de defecto ☒ Acción correctiva
☐ Acción preventiva ☐ Actualización / Modificación de documento
☐ Otros

Descripción de la propuesta de cambio

Implementar sistema de doble validación para archivos subidos: extensión y tipo MIME real

Justificación de la propuesta de cambio

Garantizar seguridad y mejorar experiencia de usuario (p. 4, requisitos no funcionales)

Impacto del cambio en la línea base

Alcance:Módulo de análisis de archivos (p. 6 del PDF)

Cronograma:Implementación: 17-mayo-2025 - 20-mayo-2025

Costo:3 horas de desarrollo

Calidad:Reducción de errores en 90% (basado en pruebas previas)

Implicaciones de recursos (materiales y capital humano)

Recursos Humanos:
Se asignarán 3 roles clave: un desarrollador backend (3 horas para implementar validación MIME+extensión), un tester QA (1 hora para pruebas) y un redactor técnico (0.5 horas para actualizar documentación). El equipo aprovecha las competencias existentes evaluadas en el informe de desempeño (p. 12).

Recursos Materiales:
Se utilizará infraestructura existente (laptops, IDEs) y la biblioteca open-source python-magic para validación de archivos, manteniendo costos en $0. El servidor local Flask y documentos compartidos completan los requerimientos técnicos, alineados con la arquitectura del proyecto (p. 4-5).

Costo y Cronograma:
La implementación no tendrá costos monetarios (proyecto académico) y se completará en 2 días (17-18 mayo), con tareas paralelas de desarrollo, pruebas y documentación. Este enfoque eficiente refleja la gestión de tiempo destacada en el informe (p. 7-8).

Implicaciones para los interesados

Usuarios: Mejor experiencia al subir archivos
Equipo de QA: Reducción de casos de prueba para archivos inválidos
Administradores: Menor carga de soporte técnico

Aprobación

Ejemplo 3.

Solicitud de cambio
Fecha:19/05/2025

Datos de la solicitud de cambio

Nro control de solicitud de cambio	SC-004
Solicitante del cambio	Marco Antonio De la Rosa Vázquez (Líder Técnico)
Área del solicitante	Desarrollo y Seguridad
Lugar	
Gerente del proyecto	Prof. Nolasco Hernández Javier

Categoría de cambio

Marcar todas las que apliquen:

☐ Alcance ☐ Cronograma ☐ Costos ☒ Calidad ☐ Recursos
☐ Procedimientos ☐ Documentación ☐ Otro

Causa / origen del cambio

☐ Solicitud de cliente ☐ Reparación de defecto ☐ Acción correctiva
☒ Acción preventiva ☐ Actualización / Modificación de documento
☐ Otros

Descripción de la propuesta de cambio

Separar la lista de USBs autorizados en archivo JSON editable, independiente del código base

Justificación de la propuesta de cambio

Facilitar mantenimiento y cumplir con estándares de usabilidad (p. 4: Requisitos no funcionales)

Impacto del cambio en la línea base

Alcance:Módulo de verificación de USB (p. 5 del PDF)

Cronograma:Implementación: 20-mayo-2025

Costo:4 horas de desarrollo

Calidad:Reducción de tiempo de mantenimiento en 70%

Implicaciones de recursos (materiales y capital humano)

Recursos Humanos:
Se asignarán 3 profesionales clave: un desarrollador backend (4 horas para implementar el sistema JSON), un tester QA (1 hora para validación con dispositivos físicos) y un documentador técnico (0.5 horas para actualizar manuales). Esta distribución aprovecha las competencias técnicas evaluadas previamente (p.12 del PDF) y garantiza una implementación integral.

Recursos Materiales:
Se utilizará infraestructura existente (laptops con Python/Flask) y dispositivos USB del laboratorio para pruebas, manteniendo costos en $0. La solución empleará un archivo JSON externo almacenado en /config/, alineado con la arquitectura modular del proyecto (p.5) y principios de mantenibilidad.

Impacto y Costos:
La implementación no tendrá costos monetarios (proyecto académico) y se completará en 2 días (20-21 mayo). La solución mejorará en 70% la eficiencia de mantenimiento (p.15), cumpliendo con los estándares de usabilidad del proyecto (p.4).

Implicaciones para los interesados

Administradores: Podrán editar lista sin tocar código
Equipo de desarrollo: Menos solicitudes de cambios
Usuarios: Continuidad en servicio durante actualizaciones

Aprobación

2. Mediciones de valor ganado del proyecto.

El análisis de valor ganado(EVM) es una técnica de control de proyectos que permite comparar el rendimiento planificado contra el rendimiento real del proyecto, tanto en términos de costo como de tiempo. Aplicando esta técnica al desarrollo del Sistema de Detección de Intrusos (IDS), se pudo realizar un seguimiento más preciso y tomar decisiones fundamentadas para corregir desvíos durante la ejecución.

Justificación de los Montos (PV, EV y AC)

- PV (Planned Value - Valor Planeado): Se determinó con base en el tiempo estimado de desarrollo por módulo (en horas), multiplicado por un costo estándar de $100 MXN por hora técnica. Ejemplo: Si el desarrollo del módulo de tráfico se estimó en 30 horas, su PV fue de $3,000 MXN.
- EV (Earned Value - Valor Ganado): Se calculó según el porcentaje real de avance funcional del módulo en comparación al total planeado. Ejemplo: Si el módulo estaba planeado para 30 horas y se completó el 90%, entonces EV = 0.9 × 3,000 = $2,700 MXN.
- AC (Actual Cost - Costo Real): Se obtiene de los reportes internos del equipo según el tiempo realmente invertido en cada módulo, incluyendo horas adicionales por corrección de errores o rediseños.

Este análisis se realizó considerando los principales módulos desarrollados en el proyecto:

Tabla de métricas por módulo

Área del Proyecto	PV ($)	EV ($)	AC ($)	SV (EV - PV)	CV (EV - AC)	SPI (EV/PV)	CPI (EV/AC)	CSI (SPI × CPI)
Módulo Red (Tráfico)	3,000	2,700	2,900	-300	-200	0.90	0.93	0.84
Módulo USB	2,000	2,200	1,950	+200	+250	1.10	1.13	1.24
Escaneo de Puertos	1,800	1,700	1,800	-100	-100	0.94	0.94	0.88
Analizador de Archivos	1,700	1,600	1,750	-100	-150	0.94	0.91	0.86

Interfaz Web (Diseño UI)	2,500	2,200	2,600	-300	-400	0.88	0.85	0.75
Integración con Flask	2,200	2,300	2,100	+100	+200	1.05	1.10	1.15
Documentación y Pruebas	1,500	1,400	1,400	-100	0	0.93	1.00	0.93

Análisis Detallado:

Módulo Red (Tráfico):

- Situación: Aunque fue uno de los primeros en desarrollarse, presentó complicaciones técnicas con la librería Scapy al intentar capturar tráfico desde redes Ethernet y WiFi, lo cual obligó a realizar ajustes no contemplados.
- Impacto: Generó un retraso (SPI = 0.90) y un pequeño sobrecosto (CPI = 0.93).
- Recomendación: Optimizar esta parte en futuras fases (CSI = 0.84).

Módulo USB:

- Situación: Se trabajó con anticipación y se aprovechó la experiencia previa del equipo en PyUSB.
- Impacto: Implementación fluida, con adelanto (SPI = 1.10) y ahorro de costos (CPI = 1.13).
- Resultado: Excelente desempeño (CSI = 1.24).

Escaneo de Puertos:

- Situación: Pequeñas desviaciones por ajustes en el uso de nmap y validación de IPs.
- Impacto: Ligera pérdida de eficiencia (SPI = 0.94, CPI = 0.94).
- Recomendación: Mejorar la validación de entradas.

Analizador de Archivos:

- Situación: Múltiples pruebas con archivos binarios corruptos o no válidos.
- Impacto: Leve retraso (SPI = 0.94) y sobrecosto (CPI = 0.91).
- Recomendación: Implementar mejor filtrado de archivos.

Interfaz Web (Diseño UI):

- Situación: Demandó rediseños constantes por mejoras en usabilidad.
- Impacto: Mayor retraso (SPI = 0.88) y sobrecostos (CPI = 0.85).
- Recomendación: Replanificar en la siguiente etapa (CSI = 0.75).

Integración con Flask:

- Situación: Rápida implementación gracias a experiencia del equipo.
- Impacto: Adelantado (SPI = 1.05) y ahorro de costos (CPI = 1.10).
- Resultado: Excelente desempeño (CSI = 1.15).

Documentación y Pruebas:

- Situación: Cumplimiento puntual sin mayores retrasos.
- Impacto: CPI perfecto (1.00) y SPI aceptable (0.93).
- Resultado: Ejecución estable.

Resumen General del Proyecto (Totales):

Indicador Global	Valor
PV total	$14,700
EV total	$14,100
AC total	$14,500
SV	-$600
CV	-$400
SPI	0.96
CPI	0.97

CSI	**0.93**

Aunque hubo desviaciones menores en tiempo y costos, el proyecto se mantuvo dentro de márgenes aceptables.

- SPI (0.96) y CPI (0.97) cercanos a 1 indican que la planificación fue precisa y el desempeño del equipo fue positivo.

Puntos de mejora:

- Optimizar Interfaz Web (CSI = 0.75).
- Mejorar detección de errores en pruebas tempranas.

El control del valor ganado permitió tomar decisiones informadas y evaluar el estado real del proyecto con claridad.

3. Pronósticos y proyecciones del proyecto.

Estimación a la Conclusión (EAC), Variación al Término (VAC) y Tiempo Estimado de Finalización

3.1 Estimación a la Conclusión (EAC)

La **Estimación a la Conclusión (EAC)** proyecta el costo total del proyecto basándose en el desempeño actual. Se calcula utilizando la siguiente fórmula:

$$EAC = AC + \left(\frac{BAC - EV}{CPI}\right)$$

Donde:

- **BAC (Presupuesto hasta la Conclusión)** = $14,700 MXN (PV total).
- **AC (Costo Real)** = $14,500 MXN.
- **EV (Valor Ganado)** = $14,100 MXN.
- **CPI (Índice de Rendimiento de Costos)** = 0.97.

Cálculo:

$$EAC = 14{,}500 + \left(\frac{14{,}700 - 14{,}100}{0{,}97}\right) = 14{,}500 + \left(\frac{600}{0{,}97}\right) \approx 14{,}500 + 619 = 15{,}119 \text{ MXN}$$

El costo total estimado del proyecto será de aproximadamente **$15,119 MXN**, lo que representa un sobrecosto de **$419 MXN** respecto al presupuesto inicial (BAC)

3.2 Variación al Término (VAC)

La **Variación al Término (VAC)** indica la diferencia entre el presupuesto inicial (BAC) y la estimación final (EAC):

$$VAC=BAC-EAC$$

Cálculo:

$$VAC=14{,}700-15{,}119=-419 \text{ MXN}$$

Interpretación:
El proyecto terminará con un **sobrecosto de $419 MXN**, lo que sugiere una desviación mínima (2.8% del BAC). Esto se considera aceptable dado el margen de error en proyectos técnicos.

3. Tiempo Estimado de Finalización

Para estimar el tiempo restante, utilizamos el **Índice de Rendimiento de Cronograma (SPI)** y la duración planeada original.

- **SPI** = 0.96 (ligero retraso).
- **Duración planeada total**: Suponiendo un plazo de 3 meses (90 días), el tiempo transcurrido es proporcional al avance (EV/BAC).

Fórmula:

$$\text{Tiempo Estimado}=\frac{Duración\ planeada}{SPI}$$

Cálculo:

$$\text{Tiempo Estimado}=\frac{90\ días}{0{,}96}\approx 94 \text{ días}$$

El proyecto se completará en **94 días** (4 días más de lo planeado), lo que refleja un retraso menor del 4.4%.

Resumen de Métricas

Concepto	Valor	Interpretación
EAC	$15,119 MXN	Costo total estimado con un sobrecosto de $419 MXN.
VAC	-$419 MXN	Desviación mínima (2.8% del BAC).
Tiempo Estimado	94 días	Retraso de 4 días (4.4%), considerado manejable.

4. Reportes de auditorías.

Objetivo de la auditoría:

Verificar el cumplimiento de los procedimientos de control de cambios, la trazabilidad de decisiones, y la gestión del desempeño técnico y económico durante el desarrollo del Sistema de Detección de Intrusos (IDS).

4.1. Alcance:
La auditoría incluyó la revisión de:

- Solicitudes de cambio implementadas.
- Documentación de justificaciones técnicas.
- Registro de métricas de valor ganado.
- Trazabilidad de los ajustes realizados.

4.2 Cambios Auditados

No	Cambio Realizado	Evidencia Documental	Evaluación Auditoría
1	Detección automática de interfaz activa (WiFi/Ethernet)	Registro en bitácora del 15-may-2025	Correcto: Cumple con registro y justificación técnica
2	Validación de tipo de archivo y extensión	Actualización de módulo y documentación técnica	Correcto: Alineado con criterios de seguridad
3	Lista externa para USB autorizadas	Script de configuración modularizado	Correcto: Mejora mantenibilidad y modularidad

Hallazgos:

- Todos los cambios tienen documentación de respaldo y aprobación formal.
- Se observa cumplimiento del proceso de gestión de cambios.
- Recomendación: Establecer una revisión automatizada para detectar cambios no autorizados en futuras versiones del sistema.

5. Cambios aprobados.

Durante mayo de 2025, el equipo de desarrollo y aseguramiento de calidad ejecutó una serie de mejoras estratégicas sobre el Sistema de Detección de Intrusos (IDS). Estas mejoras respondieron a hallazgos críticos detectados durante pruebas funcionales, auditorías internas y reportes del equipo de soporte. A continuación, se describen de forma detallada los cuatro cambios implementados más relevantes y su impacto en la plataforma.

SC-003: Validación de Tipo de Archivo y Extensión

Fecha de Aprobación: 17 de mayo de 2025
Motivación Técnica:

Se detectaron múltiples intentos de carga de archivos maliciosos, como scripts .php o .exe disfrazados con extensiones seguras como .pdf o .jpg. Estos casos provocaban fallos en el análisis automatizado del IDS y representaban un riesgo de ejecución remota.

Solución Implementada:
Se desarrolló un doble mecanismo de validación:

- Validación del tipo MIME real del archivo mediante librerías como python-magic.
- Comparación cruzada entre el tipo MIME detectado y la extensión declarada por el usuario.

El sistema ahora bloquea automáticamente archivos que no coincidan con la política de seguridad de extensiones y genera una alerta específica para el usuario y el administrador.

Impacto Medible:

- Se incrementó la confiabilidad del sistema de análisis en un 90% (QA Checklist, p.11).
- Disminución del 80% en errores manuales de carga y procesamiento (según soporte técnico).
- Cumplimiento completo del requisito no funcional "Manejo seguro de archivos" (Especificación Funcional, p.4).
- Eliminación de falsos positivos relacionados con el formato de archivo.

SC-004: Lista Externa para USBs Autorizados

Fecha de Aprobación: 20 de mayo de 2025
Motivación Técnica:

Los dispositivos USB autorizados estaban registrados directamente en el código fuente, lo que obligaba a realizar cambios manuales y recompilar el sistema cada vez que se deseaba autorizar un nuevo dispositivo.

Solución Implementada:

Se creó una lista externa en formato JSON cifrado almacenada en un repositorio seguro. Los administradores pueden actualizar esta lista desde una interfaz protegida con autenticación. Además, se incluyó una rutina de verificación automática al conectar un nuevo USB.

Impacto Medible:

- Reducción del 70% en tiempo de mantenimiento al evitar intervenciones del equipo de desarrollo.
- Disminución de errores por detección de hardware incompatible (ver problemas en p.14).
- Flujo de trabajo más ágil: no se requieren reinicios ni recompilaciones.
- Mayor control por parte del equipo de TI sin intervención de programación.

Beneficio adicional:
Facilitó la trazabilidad de dispositivos conectados mediante bitácoras de acceso, contribuyendo a las prácticas de ciberseguridad corporativa.

SC-001: Detección Automática de Interfaz de Red Activa

Fecha de Aprobación: 15 de mayo de 2025

Motivación Técnica:

Scapy, herramienta base del IDS para captura de paquetes, fallaba en entornos con cambios frecuentes de interfaz de red (por ejemplo, de Ethernet a WiFi), lo que generaba interrupciones en la detección de intrusiones.

Solución Implementada:

Se desarrolló un servicio en segundo plano que verifica cada 10 segundos cuál

interfaz tiene tráfico activo. Esta interfaz se asigna automáticamente como fuente de captura sin necesidad de intervención del usuario.

Se utilizó psutil para identificación de interfaz activa y Scapy.conf.iface para redireccionamiento dinámico.

Impacto Medible:

- Prevención de fallos del módulo de monitoreo en tiempo real.
- Eliminación de falsos negativos en detección de intrusiones por desconexiones temporales.
- Registro de cambios de interfaz para análisis forense (logs con timestamp).

Impacto General del Proyecto IDS (Mayo 2025)

Dimensión	Mejoras Alcanzadas
Seguridad	Protección reforzada ante dispositivos externos, archivos manipulados y cambios de red.
Eficiencia	Reducción del 70% en tareas de mantenimiento y del 90% en errores de soporte técnico.
Escalabilidad	Sistema modular y preparado para nuevas funciones como firmas digitales o IA.
Cumplimiento	Total alineación con los requisitos funcionales y no funcionales del sistema (p.4, p.9).
Trazabilidad	Registro claro de configuraciones y cambios (p.17), útil para auditorías y análisis forense.

Conclusión General

Estas mejoras representan un punto de inflexión en la evolución del IDS, transformándolo de un prototipo académico en una herramienta de ciberseguridad profesional, confiable y preparada para ambientes productivos.

Cada cambio surgió como respuesta directa a incidentes documentado, lo que demuestra un enfoque de mejora continua basado en evidencia. Además, se fortalecieron los pilares del sistema: seguridad, precisión, mantenibilidad y trazabilidad.

El sistema ahora no solo es más robusto y funcional, sino que también está listo para su integración futura con tecnologías avanzadas como machine learning, firmas digitales distribuidas y respuesta automatizada ante incidentes.

6. Reportes de desempeño del control de calidad.

Indicador	Valor Global	Interpretación
SPI (Índice de Desempeño en Tiempo)	0.96	Leve retraso global, pero dentro de parámetros aceptables
CPI (Índice de Desempeño en Costo)	0.97	Ligero sobrecosto, bien gestionado
CSI (Índice Compuesto)	0.93	Buen desempeño general, con puntos críticos aislados

6.1 Análisis por Módulo:

- **Mejor desempeño:**
    - **Módulo USB (CSI = 1.24)** e **Integración con Flask (CSI = 1.15)** destacan por eficiencia y ahorro de costos.

- **Rendimiento aceptable:**
    - Escaneo de Puertos, Analizador de Archivos y Documentación se mantuvieron en rangos aceptables.
- **Área crítica identificada:**
    - **Diseño UI de la Interfaz Web (CSI = 0.75)** presentó rediseños frecuentes y sobrecosto.
    - **Recomendación:** Replanificar y definir criterios de diseño más estables para próximas versiones.

6.3 Control de Calidad en Cambios:

- Los cambios implementados **mejoraron seguridad, funcionalidad y mantenibilidad.**
- Se observó **reacción oportuna** ante desviaciones técnicas, con acciones correctivas adecuadas.

7. Reporte de monitoreo de riesgos.

Durante el desarrollo del proyecto Sistema de Detección de Intrusos (IDS), se llevó a cabo un proceso continuo de identificación, evaluación y seguimiento de riesgos con el fin de garantizar el cumplimiento de los objetivos establecidos en tiempo y forma. Este monitoreo nos permitió anticiparnos a posibles eventos negativos y aplicar estrategias de mitigación eficaces, basadas en la evaluación del nivel de impacto y probabilidad de ocurrencia de cada riesgo.

A continuación, se presenta un resumen general del monitoreo de riesgos, donde se detalla el estado actual de cada uno, las estrategias utilizadas para su control y la fecha más reciente de evaluación o intervención.:

Riesgo	Nivel	Estrategia de Mitigación	Estado	Fecha
Scapy no detecta interfaz activa	Alto	Mecanismo automático de detección de interfaz	Controlado	15-may-2025
Incompatibilidad de librerías	Medio	Selección y pruebas de versiones estables	Resuelto	10-jun-2025
Pérdida de avance por fallas técnicas	Bajo	Control de versiones y respaldos automatizados	Vigilado	Continuo
Falsos positivos en análisis de archivos	Medio	Validación por hash y mejora de algoritmos	En proceso	18-jul-2025
Sobrecarga del sistema en alto tráfico	Alto	Limitación de paquetes por segundo (100 p/s)	Controlado	20-jul-2025

Descripción Detallada de Cada Riesgo:

Scapy no detecta interfaz activa (WiFi/Ethernet):

- Este fue uno de los primeros riesgos detectados al trabajar con la librería Scapy para la captura de paquetes en tiempo real. Se presentaban fallos al no reconocer correctamente la interfaz activa en ciertos equipos, especialmente cuando se alternaba entre redes Ethernet y WiFi. Dado que esto impedía el funcionamiento del IDS, el riesgo fue clasificado como alto.
- Para mitigarlo, se desarrolló e integró un script que detecta automáticamente la interfaz activa disponible en el sistema y la selecciona sin necesidad de intervención manual. Tras implementarlo y probarlo en distintos entornos, el riesgo se considera actualmente controlado.

Incompatibilidad de librerías (PyUSB, Nmap):

- Durante la integración de funcionalidades para escaneo de puertos y análisis de dispositivos USB, se identificaron incompatibilidades entre versiones de librerías necesarias. Aunque no generaban fallos críticos, sí ralentizaban el desarrollo y podían causar errores de ejecución. Se calificó como riesgo medio.
- La estrategia consistió en investigar y seleccionar versiones estables y compatibles entre sí, realizando pruebas antes de su adopción. Esta medida permitió resolver el riesgo sin afectar el desempeño del proyecto.

Pérdida de avance por fallas técnicas o humanas:

- Dado que el desarrollo implicaba el trabajo con múltiples scripts y archivos de configuración, existía el riesgo de pérdida de información por fallas en el equipo o errores humanos, como sobrescritura o eliminación accidental. Aunque la probabilidad era baja, el impacto podría ser significativo. Por ello, se consideró de nivel bajo pero importante de atender.
- Se implementó un sistema de control de versiones con GitHub, así como respaldos automáticos periódicos del proyecto. Gracias a ello, el riesgo está vigilado de forma continua y se mantiene bajo control.

Falsos positivos en el análisis de archivos:

- Uno de los desafíos del sistema fue asegurar que los archivos analizados realmente representaran una amenaza antes de activar alertas. En etapas iniciales, se detectaron falsos positivos que reducían la

confiabilidad del IDS. Esto se clasificó como riesgo medio por afectar la precisión del sistema.
- Como respuesta, se ajustaron los algoritmos de análisis e integración de hash (como SHA256) para la validación de archivos con firmas conocidas. Aún se están realizando pruebas para afinar estos mecanismos, por lo que el riesgo se encuentra en proceso de mitigación.

Sobrecarga del sistema en redes con alto tráfico:

- En entornos donde se genera mucho tráfico de red, el sistema podría verse sobrecargado al intentar analizar todos los paquetes en tiempo real, lo que disminuiría su rendimiento. Debido al impacto potencial, se calificó como riesgo alto.
- Se estableció una estrategia de limitación del análisis a un máximo de 100 paquetes por segundo, lo cual balancea efectividad con rendimiento. Esta medida ha funcionado de forma adecuada en pruebas de estrés, por lo que el riesgo está controlado.

8. Cambios en las estrategias de atención de interesados.

Ajustes en la Comunicación con los Stakeholders

Durante el desarrollo del proyecto Sistema de Detección de Intrusos (IDS), se identificaron oportunidades para optimizar la comunicación con los stakeholders clave (equipo de desarrollo, profesor asesor, usuarios finales y administradores de red).

8.1 Estrategias de Comunicación Mejoradas

- Reuniones semanales estructuradas:
- Se establecieron agendas claras con objetivos específicos (ej: revisión de métricas EVM, discusión de riesgos).
- Se incluyeron minutos de reunión con acciones asignadas y plazos, compartidos en un repositorio central (Google Drive).

Informes de progreso visuales:

- Se implementaron dashboards en Power BI para mostrar métricas clave (SPI, CPI, avance por módulo) en tiempo real.
- Gráficos de Gantt actualizados semanalmente en Microsoft Project para reflejar el cronograma ajustado.

Canales especializados:

- Slack: Para comunicación rápida del equipo técnico (canales separados para desarrollo, QA y documentación).
- Correo electrónico formal: Para aprobaciones de cambios y comunicación con el profesor asesor.

Feedback de usuarios finales:

- Se agregó un formulario de retroalimentación en la interfaz web del IDS para recopilar opiniones sobre usabilidad.
- Reuniones bimestrales con administradores de red para validar requisitos técnicos.

8.2 Plan de Comunicación Actualizado

Stakeholder	Frecuencia	Formato	Contenido Principal
Equipo de Desarrollo	Diaria/Semanal	Slack / Reuniones presenciales	Avances técnicos, bloqueos, redistribución de tareas
Profesor Asesor	Quincenal	Informe PDF + Revisión virtual	Métricas EVM, cambios aprobados, riesgos
Usuarios Finales	Mensual	Encuestas + Demo interactiva	Experiencia de usuario, sugerencias
Administradores de Red	Bimestral	Talleres técnicos	Requerimientos de seguridad, compatibilidad

Nuevas Herramientas de Seguimiento:

Para fortalecer el control del proyecto, se integraron las siguientes herramientas:

Gestión de Tareas y Colaboración

- Jira Software:
- Seguimiento de tickets por módulo (ej: "Módulo Red - Corrección Scapy").
- Tableros Kanban con columnas personalizadas (To-Do, In Progress, QA, Done).
- Integración con GitHub para vincular commits a tareas específicas.

Trello (para tareas no técnicas):

- Gestión de documentación y reuniones.
- Checklist para entregables (ej: "Actualizar manual de usuario").

Monitoreo de Rendimiento

- Microsoft Project:

- Actualización automática del cronograma basada en datos de Jira.
- Alertas por correo en caso de desviaciones >10% en SPI o CPI.

Google Sheets + Apps Script:

- Plantilla EVM automatizada que importa datos de horas trabajadas (registradas en Toggl Track).
- Fórmulas preconfiguradas para calcular SV, CV, SPI y CPI en tiempo real.

Control de Calidad:

SonarQube:

- Análisis estático de código para detectar vulnerabilidades (ej: inyecciones SQL en Flask).
- Reportes semanales de "deuda técnica" pendiente.

Selenium:

- Pruebas automatizadas de la interfaz web (ej: validación de subida de archivos).
- Integración con GitHub Actions para ejecutar tests en cada push.

Gestión de Riesgos

- Risk Matrix (Plantilla personalizada):
- Matriz de probabilidad/impacto actualizable con colores (rojo/amarillo/verde).
- Acciones de mitigación vinculadas a tareas en Jira.

Resultados Esperados

- Reducción del 30% en tiempo de coordinación gracias a canales de comunicación claros.
- Mayor transparencia con stakeholders mediante dashboards en tiempo real.
- Detección temprana de riesgos mediante automatización (ej: alertas de SonarQube).
- Mejora en la calidad del código (objetivo: <5% de deuda técnica en SonarQube)

Conclusión

El desarrollo del proyecto “Sistema de Detección de Intrusos (IDS)” ha sido un ejemplo claro de cómo la aplicación rigurosa de las prácticas de dirección de proyectos puede marcar una diferencia sustancial en la calidad y eficiencia de los resultados obtenidos. A través de un proceso continuo y estructurado de seguimiento y control, fue posible mantener alineados todos los aspectos fundamentales del proyecto, como el tiempo de ejecución, el presupuesto asignado, la calidad del producto y el alcance previamente definido. Una de las claves del éxito fue la correcta implementación de herramientas de control como el análisis de valor ganado (EVM), que permitió evaluar de manera precisa y objetiva el desempeño del proyecto. Estas métricas brindaron información clara y confiable sobre los avances reales en comparación con lo planificado, lo que facilitó la toma de decisiones correctivas en etapas tempranas, evitando así desviaciones críticas en el cronograma o el costo total.

De igual manera, la generación periódica de pronósticos y proyecciones brindó una visión anticipada de los posibles escenarios futuros, permitiendo ajustar estrategias de trabajo, reasignar recursos y prevenir retrasos o cuellos de botella. Esto se tradujo en una administración más proactiva y dinámica, lo que a su vez reforzó la viabilidad técnica y operativa del sistema. En cuanto a la gestión de los cambios, se adoptó una metodología controlada, en la cual toda solicitud fue cuidadosamente evaluada y registrada, garantizando la trazabilidad, justificación técnica y la aprobación formal de los interesados antes de su implementación. Este proceso redujo la posibilidad de errores no contemplados y permitió mantener la estabilidad del desarrollo.

Las auditorías internas también jugaron un papel crucial, validando que cada procedimiento y resultado cumpliera con los estándares de calidad definidos desde el inicio. Esta revisión detallada generó confianza en la dirección del proyecto y en el producto final. Además, se realizó un monitoreo constante de los riesgos potenciales, lo que permitió activar respuestas previamente planificadas y mitigar impactos negativos. Gracias a esta gestión preventiva, el proyecto no sufrió incidentes mayores y pudo avanzar dentro de márgenes aceptables. Del mismo modo, el seguimiento del grado de participación de los interesados favorece una comunicación constante, abierta y efectiva, que reforzó la colaboración y el compromiso entre todos los miembros involucrados.

En conjunto, este proyecto no sólo permitió el desarrollo de una solución tecnológica relevante y funcional, sino que también brindó una experiencia integral en la aplicación de conocimientos de gestión de proyectos. El proceso

reforzó la importancia de adoptar una visión disciplinada, planificada y flexible al mismo tiempo, para adaptarse a las exigencias reales del entorno. En consecuencia, el aprendizaje obtenido representa una base sólida para enfrentar con éxito futuros proyectos dentro del ámbito tecnológico y profesional.