INFORME DE SEGUIMIENTO Y EVALUACIÓN

SAPIENCIA

2025

SAPIENCIA
Agencia de Educación Postsecundaria de Medellín

Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

Seguridad de la Información – Propuesta del Plan 2026

FECHA: 22/12/2025

ELABORADO POR: EDISON SALGAR MARIN

DEPENDENCIA/PROCESO: SISTEMAS INFORMACION / SEGURIDAD

TABLA DE CONTENIDO

· INTRODUCCIÓN

La Agencia de Educación Postsecundaria de Medellín – SAPIENCIA cuenta con un sistema de detección, prevención y gestión de vulnerabilidades que ha permitido mejorar los niveles de seguridad de la información y la capacidad de respuesta ante incidentes.

Para el año 2026, se hace necesario proyectar este plan de trabajo con un enfoque de mejora continua, madurez del SGSI, y fortalecimiento de capacidades técnicas, considerando la evolución constante de las amenazas, los lineamientos del MINTIC y las buenas prácticas

· OBJETIVO GENERAL

Optimizar, fortalecer y madurar durante el año 2026 el sistema de detección y gestión de vulnerabilidades (IDS/IPS y controles asociados) de la Agencia, garantizando su actualización permanente, mayor precisión en la detección de amenazas y una respuesta oportuna ante incidentes de seguridad de la información.

· OBJETIVOS ESPECÍFICOS

- Evaluar periódicamente el desempeño del sistema IDS/IPS y sus integraciones.
- Reducir la tasa de falsos positivos y falsos negativos.
- Alinear la operación del sistema con los lineamientos del MINTIC y el SGSI institucional.
- Fortalecer las capacidades del equipo técnico y la concienciación de los usuarios.
- Garantizar el monitoreo continuo y la generación de información para la toma de decisiones.

· PLAN DE TRABAJO / CRONOGRAMA

El Plan de Trabajo 2026 tiene como finalidad fortalecer y optimizar el sistema de detección, prevención y gestión de vulnerabilidades de la Agencia de Educación Postsecundaria de Medellín – Sapiencia, mediante la evaluación continua, el ajuste técnico de los controles de seguridad, la capacitación del personal y el monitoreo permanente de los eventos de seguridad.

Fase	Actividad	Descripción	Periodo de Ejecución 2026	Responsable
Fase 1: Evaluación del Desempeño	Revisión de logs y reportes de eventos	Análisis de registros generados por IDS/IPS, firewall y herramientas de seguridad para identificar eventos relevantes y tendencias.	Primer trimestre 2026	Edison Salgar
	Análisis de reglas y políticas de detección	Evaluación de la efectividad de reglas configuradas, identificando falsos positivos y falsos negativos.	Primer trimestre 2026	Edison Salgar
	Evaluación de integraciones de seguridad	Revisión de la integración del IDS/IPS con firewall, antivirus, SIEM y otros controles de seguridad.	Primer trimestre 2026	Edison Salgar
Fase 2: Ajuste y Optimización del Sistema	Actualización de bases de datos de amenazas	Actualización de firmas de virus en Kaspersky y patrones de ataque en Fortigate, alineadas a amenazas emergentes.	Primer trimestre 2026	Edison Salgar
	Optimización del desempeño del sistema	Ajuste de parámetros de monitoreo en hipervisores Proxmox (sede C4ta) para mejorar rendimiento y tiempos de respuesta.	Primer semestre 2026	Edison Salgar
	Refinamiento de reglas de detección	Modificación de 12 reglas de firewall y 5 políticas de detección de vulnerabilidades, según perfil de riesgo institucional.	Segundo trimestre 2026	Edison Salgar
Fase 3: Capacitación y Concienciación	Capacitación técnica al equipo TI	Jornadas de formación sobre operación del IDS/IPS, análisis de eventos y respuesta a incidentes.	Primer semestre 2026	Edison Salgar
	Simulación y validación de ataques	Ejecución de pruebas controladas para medir tiempos de detección y respuesta del sistema.	Segundo semestre 2026	Edison Salgar
	Sensibilización a usuarios	Actividades de concienciación sobre amenazas emergentes, phishing y buenas prácticas de seguridad de la información.	Segundo semestre 2026	Edison Salgar

Fase 4: Auditoría y Cumplimiento	Evaluaciones internas de seguridad	Validaciones internas de configuraciones, controles y cumplimiento de lineamientos MINTIC y SGSI.	Trimestral	Edison Salgar
	Implementación de mejoras recomendadas	Aplicación de acciones correctivas y de mejora derivadas de auditorías y evaluaciones de seguridad.	Trimestral	Edison Salgar
Fase 5: Monitoreo Continuo y Respuesta a Incidentes	Monitoreo del IDS/IPS	Seguimiento permanente del comportamiento del sistema y eventos de seguridad.	Permanente	Edison Salgar
	Actualización de estrategias de mitigación	Ajuste continuo de estrategias de respuesta frente a nuevas amenazas y vulnerabilidades.	Permanente	Edison Salgar
	Generación de reportes de seguridad	Elaboración de reportes técnicos y ejecutivos para apoyo en la toma de decisiones.	Mensual	Edison Salgar

Fase 1: Seguimiento y Análisis

- Revisión y análisis de logs y reportes de eventos de seguridad.
- Evaluación de la efectividad de reglas y políticas de detección.
- Identificación y clasificación de falsos positivos y falsos negativos.
- Revisión del nivel de integración del IDS/IPS con otros controles de seguridad (firewall, SIEM, antivirus, etc.).

Fase 2: Ajuste y Optimización del Sistema

- Refinamiento y ajuste de reglas de detección.
- Actualización de bases de datos de amenazas, firmas y patrones de ataque.
- Mejora en la correlación de eventos de seguridad.
- Optimización del rendimiento del sistema para minimizar el impacto en la red y los servicios.

Fase 3: Capacitación y Concienciación

- Capacitación técnica periódica al equipo de TI y seguridad de la información.
- Ejecución de simulaciones controladas de ataques para medir tiempos de detección y respuesta.

- Jornadas de sensibilización a usuarios sobre amenazas emergentes, phishing, uso seguro de dispositivos y buenas prácticas.

Fase 4: Auditoría y Cumplimiento

- Validación de cumplimiento normativo: Se verificó el avance en el plan de mejoramiento derivado de la auditoría interna 2024, confirmando que el 100% de las acciones programadas para este bimestre fueron ejecutadas (actualización de licencias, parcheo de servidores, mitigación de vulnerabilidades).
- Implementación de mejoras: Se aplicaron las recomendaciones derivadas de las validaciones de seguridad, incluyendo el fortalecimiento de configuraciones en servidores AD, NAS y políticas de acceso en los dispositivos perimetrales.

Fase 5: Monitoreo Continuo y Respuesta a Incidentes

- Monitoreo permanente del IDS/IPS.
- Evaluaciones periódicas del desempeño del sistema.
- Actualización y pruebas del plan de respuesta a incidentes.
- Generación de reportes ejecutivos y técnicos para la toma de decisiones.

· RESULTADOS DEL SEGUIMIENTO A LA GESTIÓN

· N/A

· EVALUACIÓN DE SATISFACCIÓN

N/A

· CONCLUSIONES

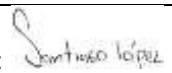
· N/A

· RECOMENDACIONES

· N/A

Cordialmente,

Edison Salgar
Ingeniero de Seguridad

Revisó: Profesional Gestión de la Información	Revisó: Apoyo a la Gestión	Aprobó: Subdirectora Administrativa, Financiera y de Apoyo a la Gestión (E)
Firma: 	Firma: 	Firma: 
Nombre: Oscar Eduardo Mengo	Nombre: Santiago López Jiménez	Nombre: Laura A. Sepúlveda Marín