PROPUESTA DE SERVICIOS

Servicio de Análisis de Vulnerabilidades y Pruebas de Seguridad Controladas

Cliente:	Instituto Tecnológico Metropolitano (ITM)
Ciudad:	Medellín, Colombia
Referencia:	COT-STAR-20260429-001
Fecha:	29 de abril de 2026
Validez:	30 días calendario

www.star-ti.com | enriqueavila@star-ti.com | +57 3017819820
Colombia · Venezuela · Estados Unidos
NIT: 900.968.161-7 | ISO 27001:2022 Certificado por SGS

TABLA DE CONTENIDO

1. Carta de Presentación 3
2. Quiénes Somos – STAR Solutions TI SAS 4
3. Justificación y Contexto de la Necesidad 5
4. Alcance del Servicio 5
5. Objetivos Específicos 6
6. Descripción Técnica de la Solución 6
7. Requerimientos por Parte del Cliente 7
8. Metodología de Ejecución 7
9. Cronograma Tentativo 8
10. Entregables 8
11. Supuestos y Exclusiones 9
12. Ética y Legalidad 9
13. Propuesta Económica 9
14. Condiciones Comerciales 10
15. Aceptación y Firma 10

1. CARTA DE PRESENTACIÓN

Medellín, 29 de abril de 2026

Señores
Instituto Tecnológico Metropolitano – ITM
Oficina de Infraestructura Tecnológica y Seguridad
Medellín, Antioquia

Respetados Señores Carlos Alberto Cortés e Iván Salazar:

En nombre de STAR Solutions TI SAS, extendemos un cordial saludo y agradecemos la confianza depositada al considerar nuestros servicios especializados en ciberseguridad para el Instituto Tecnológico Metropolitano.

Como resultado de la reunión sostenida el pasado 27 de abril de 2026, en la cual tuvimos el privilegio de conocer de primera mano las necesidades puntuales del ITM en materia de evaluación de seguridad, nos complace presentar la presente propuesta técnica y económica para la ejecución del Servicio de Análisis de Vulnerabilidades y Pruebas de Seguridad Controladas sobre su infraestructura tecnológica.

STAR Solutions TI SAS es una empresa colombiana especializada en integración de soluciones de ciberseguridad, con más de una década de presencia en Colombia, Venezuela y Estados Unidos. Contamos con certificación ISO 27001:2022 otorgada por SGS, y un equipo de profesionales certificados en CISSP, OSCP, CEH e ISO 27001 Lead Auditor. Somos partners autorizados de Bitdefender, HornetSecurity, Fortinet, Kaspersky, entre otros fabricantes líderes del mercado.

Esta propuesta ha sido elaborada de manera específica para el alcance definido: 5 sitios web transaccionales, 6 direcciones IP públicas, evaluación de la red Wi-Fi institucional y análisis de la red interna; todo ello con el rigor técnico y metodológico que una institución pública de la trayectoria del ITM merece.

Quedamos a disposición para resolver cualquier inquietud y esperamos poder acompañarles en el fortalecimiento de su postura de seguridad digital.

Atentamente,

Enrique Avila Celín
Chief Revenue Officer
STAR Solutions TI SAS
enriqueavila@star-ti.com | +57 3017819820
www.star-ti.com

2. QUIÉNES SOMOS – STAR Solutions TI SAS

STAR Solutions TI SAS (NIT: 900.968.161-7) es un integrador colombiano de soluciones de ciberseguridad con cobertura en Colombia, Venezuela y Estados Unidos. Certificados bajo la norma ISO 27001:2022 por SGS, ofrecemos a nuestros clientes la garantía de que operamos bajo los más altos estándares de gestión de seguridad de la información.

Nuestro portafolio se articula en tres pilares estratégicos:

STAR PROTECTION	STAR INSPECTION	STAR COMPLIANCE
Defensa proactiva: EDR/MDR, protección de correo, firewall, backup y seguridad de endpoints.	Análisis de vulnerabilidades, pentesting, ethical hacking y SOC-as-a-Service.	Auditorías ISO 27001:2022, consultoría SGSI y asesoría regulatoria.

Partners autorizados: Bitdefender (Platinum Colombia), HornetSecurity, Fortinet, Kaspersky, Vicarius, SOCRadar, Netwrix, Stellar Cyber, Proofpoint, entre otros. Equipo certificado: CISSP, OSCP, CEH, ISO 27001 Lead Auditor.

3. JUSTIFICACIÓN Y CONTEXTO DE LA NECESIDAD

El Instituto Tecnológico Metropolitano, como institución pública de educación superior con presencia digital activa —sitios transaccionales, infraestructura perimetral Fortinet, plataformas académicas y servicios en línea—, enfrenta un panorama de amenazas cibernéticas en constante crecimiento. La combinación de activos expuestos a internet, redes internas con múltiples usuarios y redes Wi-Fi de acceso institucional genera una superficie de ataque que requiere evaluación periódica y rigurosa.

De acuerdo con lo conversado en la reunión del 27 de abril de 2026 y confirmado por el Sr. Carlos Alberto Cortés e Iván Salazar (Oficial de Seguridad), el ITM ya cuenta con herramientas de protección de endpoints (Bitdefender) y solución perimetral (Fortinet), que ofrecen visibilidad operativa de amenazas internas. Sin embargo, no se ha ejecutado recientemente una evaluación de seguridad externa controlada y formal que permita:

- Validar la postura de seguridad frente a atacantes externos reales.
- Identificar vulnerabilidades en los activos públicos antes de que sean explotadas.
- Verificar qué información y recursos internos son visibles desde la red Wi-Fi pública.
- Cumplir con los requisitos de due diligence que exigen las normativas aplicables a entidades públicas colombianas.

El ITM tiene asignado presupuesto para este proyecto y la ejecución está proyectada para la última semana de junio de 2026. Esta propuesta responde directamente al estudio de mercado en curso y al alcance técnico definido por el equipo de infraestructura del ITM.

4. ALCANCE DEL SERVICIO

El servicio de Análisis de Vulnerabilidades y Pruebas de Seguridad Controladas abarcará los siguientes activos tecnológicos del ITM:

COMPONENTE	DESCRIPCIÓN
5 Sitios Web Transaccionales	Evaluación de seguridad web bajo metodología OWASP Top 10, análisis de configuración, autenticación, autorización y cifrado.
6 Direcciones IP Públicas	Escaneo externo de puertos y servicios expuestos, identificación de vulnerabilidades, simulación de ataques controlados en modalidad caja negra.
Red Wi-Fi Institucional	Evaluación desde la perspectiva de un usuario conectado a la Wi-Fi pública: visibilidad de activos, segmentación de red, posibilidad de movimiento lateral.
Red Interna	Análisis de la red interna: escaneo de servicios, identificación de activos expuestos, evaluación de controles de acceso y segmentación.

Cobertura de Pruebas

- Análisis de vulnerabilidades externo (enfoque caja negra)
- Simulación de ataques controlados sin afectación de la operación productiva
- Escaneo general de red interna
- Pruebas específicas sobre activos críticos identificados

Nota: La red Wi-Fi cuenta con una IP pública. El objetivo de la evaluación es determinar, estando conectado a dicha red dentro de las instalaciones, qué recursos internos son visibles y accesibles.

5. OBJETIVOS ESPECÍFICOS

- Identificar vulnerabilidades técnicas en aplicaciones web e infraestructura de red del ITM.
- Evaluar la exposición de los activos públicos frente a amenazas externas reales.
- Validar los controles de seguridad en redes internas y en la red Wi-Fi institucional.
- Determinar el nivel de riesgo (crítico, alto, medio, bajo) asociado a cada hallazgo mediante CVSS v3.1.
- Verificar la segmentación entre la red Wi-Fi pública y la red administrativa interna.
- Proporcionar recomendaciones técnicas prácticas y priorizadas para la remediación de hallazgos.
- Entregar una hoja de ruta de remediación que facilite la gestión y seguimiento por parte del equipo de TI del ITM.

6. DESCRIPCIÓN TÉCNICA DE LA SOLUCIÓN

El servicio se ejecutará mediante una combinación de herramientas automatizadas de clase mundial y técnicas de explotación manual realizadas por profesionales certificados (OSCP, CEH). Esto garantiza tanto la amplitud del análisis como la profundidad y precisión que solo la experiencia humana puede aportar.

Componentes del Servicio

- Escaneo automatizado de vulnerabilidades en infraestructura y aplicaciones web
- Pruebas manuales de explotación controlada por especialistas certificados
- Evaluación de configuraciones de red, servicios expuestos y políticas de segmentación
- Análisis de seguridad en aplicaciones web basado en OWASP Top 10 (últimas ediciones)
- Validación de controles de autenticación, autorización, sesión y cifrado
- Verificación de visibilidad de activos internos desde la red Wi-Fi institucional
- Identificación de vectores de movimiento lateral en red interna (si aplica)

Frameworks y Estándares Aplicados

ESTÁNDAR	APLICACIÓN
OWASP Testing Guide v4.2	Evaluación de seguridad de aplicaciones web transaccionales
PTES	Marco de referencia para la ejecución de pruebas de penetración
NIST SP 800-115	Guía técnica para pruebas y evaluaciones de seguridad de la información
CVSS v3.1	Clasificación estándar de severidad de vulnerabilidades identificadas
Ley 1273/2009	Marco legal colombiano sobre delitos informáticos
Ley 1581/2012	Marco legal colombiano sobre protección de datos personales

7. REQUERIMIENTOS POR PARTE DEL CLIENTE

Para garantizar la correcta y segura ejecución del servicio, el ITM deberá proveer los siguientes elementos antes del inicio de las actividades:

- Autorización formal y escrita para la ejecución de las pruebas (documento de Reglas de Compromiso - RoE)
- Ventanas de tiempo autorizadas para pruebas, especialmente sobre activos en producción
- Listado definitivo de activos: URLs de los 5 sitios web, 6 direcciones IP públicas y rangos de red interna a evaluar
- Acceso controlado a la red interna y a la red Wi-Fi institucional para las pruebas on-site
- Designación de contacto técnico responsable para coordinación y gestión de incidentes durante las pruebas
- Definición de sistemas críticos o restricciones operativas que deban excluirse de las pruebas activas

8. METODOLOGÍA DE EJECUCIÓN

El servicio se desarrollará en siete fases secuenciales, garantizando trazabilidad completa y comunicación permanente con el equipo de TI del ITM:

FASE	NOMBRE	ACTIVIDADES CLAVE
1	**Planeación y Alcance**	Revisión de activos, definición de Reglas de Compromiso (RoE), coordinación con equipo TI del ITM.
2	**Reconocimiento**	Recolección de información pública (OSINT), enumeración de servicios y subdominios, mapeo de superficie de ataque.
3	**Análisis de Vulnerabilidades**	Escaneo automatizado con herramientas especializadas, identificación inicial y preclasificación de hallazgos.
4	**Explotación Controlada**	Validación manual de vulnerabilidades por especialistas certificados, simulación de ataques reales en ambiente controlado.
5	**Post-explotación (controlada)**	Evaluación de impacto real, análisis de movimiento lateral potencial, verificación de profundidad de brecha.
6	**Generación de Reporte**	Documentación detallada de hallazgos, clasificación CVSS v3.1, evidencias técnicas y recomendaciones priorizadas.
7	**Cierre y Presentación**	Socialización ejecutiva de resultados con el equipo directivo y técnico del ITM, resolución de dudas, entrega formal.

9. CRONOGRAMA TENTATIVO

La ejecución del servicio se proyecta para iniciar en la última semana de junio de 2026, en concordancia con los tiempos del proceso de contratación pública del ITM:

FASE	DURACIÓN	SEMANA ESTIMADA (JULIO 2026)
Planeación y kickoff	**2 días hábiles**	Semana 1 (inicio)
Ejecución técnica (externa + Wi-Fi + interna)	**10 – 12 días hábiles**	Semanas 1 – 2
Análisis, correlación y redacción de informe	**5 días hábiles**	Semana 2 – 3
Revisión y QA interno del informe	**2 días hábiles**	Semana 4
Presentación y entrega de resultados	**1 día**	Semana 4

Duración total estimada: 3 a 4 semanas calendario desde el inicio de la ejecución.

10. ENTREGABLES

Al finalizar el servicio, el ITM recibirá los siguientes documentos y artefactos técnicos:

#	ENTREGABLE	DESCRIPCIÓN
1	**Informe Ejecutivo**	Documento de 5-10 páginas dirigido a la alta dirección: resumen de hallazgos, nivel de riesgo global y prioridades de remediación.
2	**Informe Técnico Detallado**	Documentación completa de cada vulnerabilidad encontrada: descripción, vector de ataque, impacto potencial, evidencias y procedimiento de remediación.
3	**Clasificación CVSS v3.1**	Matriz de vulnerabilidades con puntuación de severidad (Crítico, Alto, Medio, Bajo, Informativo) para cada hallazgo.
4	**Evidencias Técnicas**	Capturas de pantalla, logs de herramientas, scripts utilizados y trazabilidad completa del proceso de pruebas.
5	**Recomendaciones de Mitigación**	Guía práctica con pasos concretos para corregir cada vulnerabilidad, adaptada a la arquitectura tecnológica del ITM.
6	**Hoja de Ruta de Remediación**	Plan priorizado de remediación con clasificación por criticidad, responsables sugeridos y tiempos estimados de corrección.
7	**Presentación de Resultados**	Sesión de socialización presencial o virtual con el equipo técnico y directivo del ITM para revisión y resolución de dudas.
8	**Re-test de Vulnerabilidades**	Una vez el equipo de TI del ITM haya ejecutado las acciones de remediación sobre los hallazgos críticos y altos, STAR Solutions realizará una segunda evaluación focalizada para verificar la efectividad de los controles implementados y confirmar el cierre de los riesgos más relevantes. Se entregará un informe complementario de re-test con el estado actualizado de cada hallazgo.

11. SUPUESTOS Y EXCLUSIONES

Supuestos

- Los activos listados estarán disponibles y en funcionamiento durante las ventanas de prueba acordadas.
- El ITM proporcionará autorización formal y escrita (documento RoE) antes del inicio de las pruebas.
- No se realizarán pruebas de denegación de servicio (DoS/DDoS) que puedan afectar la operación.
- El listado definitivo de los 5 sitios web y las 6 IPs públicas será entregado por el equipo técnico del ITM al inicio del proyecto.
- El acceso a la red interna y Wi-Fi para las pruebas on-site será coordinado y habilitado por el equipo de infraestructura del ITM.

Exclusiones

- Corrección o remediación de vulnerabilidades encontradas (no incluida en el alcance; puede cotizarse por separado).
- El re-test cubre únicamente la verificación de hallazgos clasificados como Crítico y Alto. Hallazgos de nivel Medio, Bajo e Informativo podrán incluirse mediante adición de alcance.
- Monitoreo continuo de seguridad posterior a la entrega de resultados.
- Pruebas sobre activos fuera del alcance explícitamente definido y acordado en el RoE.
- Ingeniería social o phishing dirigido a empleados del ITM (salvo acuerdo explícito adicional).

12. ÉTICA Y LEGALIDAD

Todas las actividades del servicio serán realizadas bajo un estricto marco ético y legal, garantizando en todo momento la confidencialidad, integridad y disponibilidad de la información y los sistemas del ITM.

- Se requerirá consentimiento explícito y por escrito (documento de Reglas de Compromiso) para el inicio de cualquier actividad de pruebas.
- Cumplimiento con la Ley 1273/2009 (delitos informáticos en Colombia) y la Ley 1581/2012 (protección de datos personales).
- Toda la información obtenida durante las pruebas será tratada con absoluta confidencialidad y no será divulgada a terceros.
- STAR Solutions TI SAS cuenta con certificación ISO 27001:2022, lo que garantiza la gestión segura de la información de nuestros clientes.
- El equipo de trabajo firmará acuerdos de confidencialidad (NDA) si el ITM así lo requiere.

13. PROPUESTA ECONÓMICA

A continuación presentamos el valor del servicio, estructurado para ofrecer la mejor relación inversión-valor del mercado:

Stack de Valor – Lo que recibe el ITM

COMPONENTE DE VALOR	VALOR PERCIBIDO	INCLUIDO
Análisis de vulnerabilidades externo – 6 IPs públicas (caja negra)	$4.500.000	✓
Evaluación de seguridad web – 5 sitios transaccionales (OWASP Top 10)	$7.000.000	✓
Evaluación de red Wi-Fi institucional (visibilidad interna desde Wi-Fi pública)	$3.000.000	✓
Análisis de red interna (escaneo, segmentación, movimiento lateral)	$4.000.000	✓
Informe Ejecutivo para dirección (presentación ejecutiva incluida)	$2.500.000	✓
Informe Técnico Detallado con evidencias, CVSS v3.1 y recomendaciones	$3.000.000	✓
Hoja de Ruta de Remediación priorizada	$1.500.000	✓
Re-test de vulnerabilidades sobre hallazgos críticos y altos (posterior a remediación)	$3.800.000	✓
Sesión de cierre y Q&A con equipo técnico y directivo del ITM	$1.200.000	✓
Soporte post-entrega por 15 días para aclaración de hallazgos	$1.000.000	✓
Valor total de referencia del mercado:	**$31.500.000**	
Inversión STAR Solutions TI SAS (antes de IVA):	**$19.867.106**	**COP**

* Precios expresados en pesos colombianos (COP) antes de IVA, el cual será adicionado según corresponda.
* Propuesta válida por 30 días calendario desde la fecha de emisión.
* El servicio no incluye remediación de vulnerabilidades encontradas; este componente puede ser cotizado de manera independiente por STAR Solutions TI SAS.

14. CONDICIONES COMERCIALES

Forma de pago	50% al inicio del contrato / 50% a la entrega del informe técnico final.
Moneda	Pesos Colombianos (COP). Facturación a nombre de STAR Solutions TI SAS – NIT: 900.968.161-7.
IVA	19% sobre el valor del servicio, a cargo del ITM.
Validez de oferta	30 días calendario a partir del 29 de abril de 2026.
Inicio de ejecución	Proyectado última semana de junio de 2026, sujeto a firma del contrato y entrega de autorización formal.
Garantías	Confidencialidad garantizada mediante acuerdo de NDA. Certificación ISO 27001:2022 operativa.
Ampliación de alcance	Cualquier activo adicional fuera del alcance definido será cotizado por separado mediante adición al contrato.

15. ACEPTACIÓN Y FIRMA

La firma del presente documento por parte del representante autorizado del Instituto Tecnológico Metropolitano (ITM) constituye la aceptación formal de las condiciones técnicas, metodológicas y económicas descritas en esta propuesta, y da inicio al proceso contractual entre las partes.

Esta propuesta corresponde a la referencia COT-STAR-20260429-001, versión 001, emitida el 29 de abril de 2026.

POR STAR SOLUTIONS TI SAS

_____

Jorge Molano
Gerente General / Representante Legal
jorgemolano@star-ti.com
NIT: 900.968.161-7

POR INSTITUTO TECNOLÓGICO METROPOLITANO

_____

_____
Representante Autorizado – ITM
Cargo: _____
Fecha: _____