INTRANT	DIRECCIÓN ADMINISTRATIVO FINANCIERO	FO.GAF.02
		VERSIÓN 1.0
	FICHA TÉCNICA PARA ADQUISICIÓN DE BIENES Y SERVICIOS	FECHA DE REVISIÓN: 17 de marzo 2025

Solicitud No.	TIC-INT-71-25		
Fecha:	22	9	2025

Nombre del Bien/Servicio	Requerimiento de Auditoría Pen Test de Servicios Expuestos – Caja Gris
Descripción y Uso	Este requerimiento dispone la realización de una auditoría de penetración de tipo caja gris sobre los servicios expuestos y sistemas internos del Instituto Nacional de Tránsito y Transporte Terrestre, con información parcial suministrada al auditor para reproducir escenarios realistas de ataque. Su aplicación tiene por finalidad identificar vulnerabilidades, evaluar la eficacia de las medidas de seguridad implementadas y recomendar acciones de mejora, garantizando en todo momento la no afectación de los sistemas críticos; constituyendo así una referencia formal en contratos, pliegos técnicos o planes de pruebas para la definición de alcance, metodología, entregables y criterios de aceptación.
Objetivo	Realizar una auditoría de penetración (Pentesting) de los servicios expuestos y sistemas internos del Instituto Nacional de Tránsito y Transporte Terrestre, con información parcial proporcionada al auditor (caja gris), identificando vulnerabilidades y evaluando la eficacia de las defensas, asegurando cobertura completa sin afectar la operación crítica de los sistemas.

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
1	Servicio	**1. Alcance** **Ítem** / **Descripción** **Servicios a evaluar**: Expuestos a Internet y segmentos internos autorizados para pruebas controladas. **Tipo de pruebas**: Caja Gris (acceso limitado a credenciales de prueba y documentación parcial). **Sistemas incluidos**: Servidores web, correo, bases de datos, redes corporativas y dispositivos de seguridad perimetral. **Normativa**: Cumplimiento con normativa local (Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología) y estándares internacionales. **Pruebas adicionales**: Seguridad en APIs, aplicaciones web y móviles, revisión de resiliencia de controles internos.	1	UN

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
		2. Fases de la Auditoría a) *Reconocimiento y Descubrimiento* • Recolección de información pasiva y activa, complementada con la información parcial proporcionada. • Mapeo de red, topología lógica y servicios internos conocidos. • Identificación de hosts activos, servicios expuestos y dispositivos no documentados. b) Escaneo de Vulnerabilidades • Uso de herramientas automatizadas (Nessus, OpenVAS, Qualys, Nmap) y técnicas manuales. • Escaneo de puertos, detección de servicios y evaluación de configuraciones conocidas. • Identificación de vulnerabilidades conocidas (CVEs). • Evaluación de políticas de firewalling, segmentación de red y controles internos accesibles. c) Análisis de Configuraciones • Revisión de políticas de seguridad en equipos de red y servidores accesibles con credenciales parciales. • Comprobación de buenas prácticas de hardening. • Evaluación de permisos de acceso y control de privilegios. • Análisis de configuraciones de servidores web, correo, DNS, Active Directory, bases de datos, etc., según acceso disponible. d) Pruebas de Penetración • Simulación de ataques reales hacia servicios publicados y sistemas internos accesibles. • Explotación ética de vulnerabilidades confirmadas. • Evaluación de defensas perimetrales y respuesta ante intentos de intrusión. • Validación de protección contra ataques comunes (SQLi, XSS, RCE, CSRF, etc.). • Pruebas de resiliencia y revisión de controles internos, *usando credenciales parciales.* e) Análisis de Logs y Monitoreo • Revisión de registros de eventos críticos y centralización de logs accesibles. • Integración con FortiSIEM u otras plataformas de SIEM según permisos.		

<table>
<tr><th>Ítem</th><th>Bien/Servicio</th><th>Datos, Descripción o Especificaciones Técnicas del Bien o Servicio</th><th>Cantidad</th><th>Unidad de Medida</th></tr>
<tr><td></td><td></td><td>
Detección de actividad sospechosa histórica o persistente en sistemas accesibles.
3. Metodologías Reconocidas

OSSTMM (Open Source Security Testing Methodology Manual)
PTES (Penetration Testing Execution Standard)
NIST SP 800-115 — Security Testing and Assessment
ISO/IEC 27001 — Gestión de la Seguridad de la Información
Combinación de técnicas manuales y automatizadas, aplicando pruebas internas limitadas y externas.

4. Requisitos Técnicos del Proveedor
Experiencia y Referencias
<table>
<tr><th>Ítem</th><th>Requisito</th></tr>
<tr><td>Experiencia mínima</td><td>2 años en pruebas de seguridad o auditorías técnicas.</td></tr>
<tr><td>Auditorías previas</td><td>Al menos 2 auditorías de pentesting o escaneos de vulnerabilidades en los últimos 18 meses (referencias bajo NDA).</td></tr>
<tr><td>Experiencia en entornos locales</td><td>Servidores web (IIS/Apache), correo (Exchange, Zimbra), bases de datos (SQL Server, MySQL), redes empresariales (Windows Server, Active Directory).</td></tr>
</table>
Certificaciones Profesionales

Cada técnico o el equipo en conjunto debe contar con al menos 5 certificaciones ofensivas vigentes y verificables.
Certificaciones ofensivas válidas (entre otras):

CEH (Certified Ethical Hacker) — EC-Council
CompTIA PenTest+
OSCP (Offensive Security Certified Professional)
eWPT (eLearnSecurity Web Application Penetration Tester)

</td><td></td><td></td></tr>
</table>

<table>
<tr><th>Ítem</th><th>Bien/Servicio</th><th>Datos, Descripción o Especificaciones Técnicas del Bien o Servicio</th><th>Cantidad</th><th>Unidad de Medida</th></tr>
<tr><td></td><td></td><td>

OSWE (Offensive Security Web Expert)
GPEN (GIAC Penetration Tester)
GWAPT (GIAC Web Application Penetration Tester)
OSEP (Offensive Security Experienced Penetration Tester)
CRTO / CRTP (Certified Red Team Operator / Professional)
OSED (Offensive Security Exploit Developer)
OSCE³ (Offensive Security Certified Expert 3)
eCPPT (eLearnSecurity Certified Professional Penetration Tester)
CPENT (Certified Penetration Testing Professional)
LPT Master (Licensed Penetration Tester)
CRTL (Certified Red Team Lead)

Certificaciones adicionales para auditores senior o líderes: CISA, CISSP, CISM, CompTIA Security+.
Se requiere que cada técnico, o el equipo en conjunto, disponga de al menos 2 vulnerabilidades CVE (Common Vulnerabilities and Exposures) registradas.

Seguridad y Confidencialidad
<table>
<tr><th>Ítem</th><th>Requisito</th></tr>
<tr><td>NDA</td><td>Firma de acuerdo de confidencialidad antes de iniciar cualquier actividad.</td></tr>
<tr><td>Operación crítica</td><td>Garantía de que todas las pruebas se realizarán sin afectar la operación crítica.</td></tr>
<tr><td>Eliminación de datos</td><td>Compromiso de eliminación de toda información recolectada al finalizar la auditoría.</td></tr>
</table>
</td><td></td><td></td></tr>
</table>

Ítem	Bien/Servicio	Datos, Descripción o Especificaciones Técnicas del Bien o Servicio	Cantidad	Unidad de Medida
		6. Entregables **Tipo de Informe** — **Descripción** **Ejecutivo** — Resumen de riesgos y recomendaciones para la Dirección de Transformación Digital. ***Técnico*** — *Informe de evidencia detallada*, explotación ética, CVEs, hallazgos clasificados por criticidad (Alta/Media/Baja) para el Departamento de Seguridad y Monitoreo TIC. **Plan de remediación** — Informe de remediación priorizado con recomendaciones concretas de mejora. **Validación** — Validación de las correcciones implementadas en un rango no mayor de 90 días después de finalizada la auditoria.		

Nota 1: Las columnas donde no aplique favor colocar N/A (No deben quedar espacios en blanco).

Nota 2: En caso de los bienes, si el mismo necesita garantía o muestra se debe especificar (si aplica).

Nota 3: En caso de los servicios, el solicitante debe describir las especificaciones que requiere; Experiencia/credenciales, calificaciones y competencias del personal que realizará el servicio, experiencia especifica, plan de trabajo, cronograma, Metodología y enfoque, personal mínimo requerido y tiempo de ejecución.

Agregar Imagen (Si aplica)

ELABORADO POR:	APROBADO POR: (Director del área)