Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

INF-0557/26

INFORME SOLICITUD DE ASISTENCIA

INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES

INDOTEL

JUNIO 11, 2026.-

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Informe

Luego de un cordial saludo, sirva la presente para exponer consideraciones de la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), respecto al proceso de compra para la **adquisición de plataforma de pruebas de penetración automatizadas y validación continua de seguridad,** el cual se nos ha presentado como dirección ejecutiva del gabinete de innovación y desarrollo digital.

Observaciones:

- Se adjunta carta de solicitud
- Se adjunta justificación de compra
- Se adjunta términos de referencia

A groso modo se solicita:

- **1 plataforma de pruebas de penetración automatizada y validación continua de seguridad debe cumplir con los siguientes aspectos técnicos y logísticos**:
  - Pruebas de Penetración Automatizadas: La solución debe permitir la ejecución autónoma y automatizada de pruebas de penetración reales (tanto internas como externas) de extremo a extremo sin interrumpir la operación de la red.
  - Validación de Vectores de Ataque Explotables: La herramienta deberá verificar de manera activa si las vulnerabilidades descubiertas en la infraestructura son realmente explotables, descartando falsos positivos.
  - Enfoque de Ataque de Caja Negra (Black-box): La plataforma debe ser capaz de iniciar evaluaciones sin necesidad de instalar agentes permanentes en los objetivos de la red ni requerir credenciales previas. 4. Descubrimiento Dinámico de Activos: La solución deberá detectar automáticamente todos los dispositivos vivos, puertos abiertos,

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

servicios expuestos y sistemas operativos presentes en los segmentos de red asignados.

- Emulación de Malware con Técnicas Avanzadas: La solución debe emular de manera segura el comportamiento de malware y código malicioso en memoria para verificar la efectividad de las herramientas de protección locales (EDR/antivirus).
- Análisis de Movimiento Lateral: La herramienta debe realizar de manera automatizada acciones de movimiento lateral en la red, simulando el comportamiento real de un atacante que busca escalar privilegios.
- Simulación de Ataques a Active Directory: La solución debe validar la seguridad del Active Directory, evaluando la robustez de las contraseñas, políticas de autenticación y configuraciones heredadas susceptibles a explotación.
- Inyección Segura de Exploits: La solución ofertada deberá inyectar de manera controlada exploits e instrucciones para validar la efectividad de los firewalls.
- Validación de Técnicas de Evasión: La solución debe evaluar si los controles actuales protegen contra ataques que se ocultan a través de la ofuscación, el cifrado o la ejecución directa en la memoria.
- Detección de Canales de Comando y Control (C2): La solución debe simular comunicaciones hacia servidores externos de Comando y Control (C2) para comprobar si los sistemas de monitoreo de red detectan y bloquean dicho tráfico.
- Validación frente a Amenazas de Ransomware: La solución debe emular de forma segura las etapas lógicas de ataques de ransomware (cifrado en memoria, propagación, etc.) para medir el tiempo y la capacidad de respuesta interna.
- Evaluación de Mitigaciones contra Adversarios Activos: La solución debe intentar establecer persistencia simulada y extracción de credenciales (p. ej., volcado de LSASS) para verificar si los controles de seguridad bloquean estas acciones.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Pruebas de Resistencia del Endpoint: La solución debe desafiar de manera activa los endpoints del INDOTEL mediante la simulación de ejecuciones de scripts maliciosos para comprobar su nivel de endurecimiento (hardening).
- Evaluación de Superficie de Ataque Externa: La solución debe identificar y mapear los activos expuestos a Internet del INDOTEL y simular vectores de intrusión perimetral.
- Validación de Controles Web y de Navegación: La solución debe simular intercepciones y ataques hacia aplicaciones web internas para evaluar su robustez y resistencia frente a inyecciones de código.
- Validación de la Cadena de Ataque Completa: La solución debe enlazar múltiples hallazgos menores para demostrar visualmente el camino crítico completo (kill chain) que seguiría un atacante real para comprometer un activo crítico.
- Visualización del Vector de Ataque (Live Path View): La solución debe permitir visualizar en tiempo real e interactivamente el mapa de la red y las rutas exactas de ataque que se lograron consolidar con éxito.
- Biblioteca Actualizada de Amenazas: La solución debe contar con una biblioteca de amenazas preconfiguradas que replique los incidentes de ciberseguridad globales más recientes a demanda.
- Clasificación del Riesgo basada en Explotabilidad: La solución debe priorizar los eventos y debilidades descubiertas no por puntajes teóricos (CVSS), sino de acuerdo a la criticidad real del camino de ataque consolidado.
- Análisis de Causa Raíz de la Explotación: La solución debe investigar de manera automática e indicar cuál es la vulnerabilidad o mala configuración base que desató todo el vector de ataque analizado.
- Simulaciones Basadas en Inteligencia de Amenazas: La solución debe ofrecer la emulación de nuevas tácticas de ataque siempre que sea necesario y demandado por parte del INDOTEL.
- Remediación Focalizada y Priorizada: La solución debe generar directrices claras indicando los puntos de estrangulamiento

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

específicos (choke points) donde una sola acción correctiva corte múltiples vectores de ataque.

- Validación Post-Remediación: La solución debe permitir ejecutar re-testeos instantáneos y automatizados sobre las debilidades corregidas para validar que el riesgo ha sido efectivamente mitigado.
- Evaluación de Identidades en la Nube: La solución debe permitir evaluar vectores de ataque dirigidos a credenciales corporativas comprometidas, accesos mal configurados o fugas de datos que impacten a entornos en la nube.
- Interfaz de Operación Centralizada: La solución debe contar con una consola web intuitiva, ágil y de fácil uso para los administradores que gestionen el programa de validación de seguridad.
- Pruebas Programables 24/7: La plataforma debe permitir programar ejecuciones de pruebas de penetración automáticas de forma continua o en ventanas específicas las 24 horas del día, los 7 días de la semana.
- Retención de Historial de Ataques y Logs: La solución debe permitir retener de forma segura los registros históricos de los ataques simulados y reportes según determine el administrador.
- Generación de Informes Técnicos y Ejecutivos: La solución debe incorporar la exportación automatizada de reportes detallados para el equipo técnico y resúmenes ejecutivos de alto nivel que muestren la postura de riesgo.
- Mitigación Guiada del Riesgo Real: La herramienta debe aportar los pasos detallados de ingeniería o configuración necesarios para neutralizar las fallas explotadas en la infraestructura.
- Soporte Técnico Directo: La solución debe incluir soporte telefónico y técnico directo disponible ante cualquier falla de funcionamiento de la plataforma o duda en la interpretación de los ataques ejecutados.
- Validación de Seguridad en Capa de Correo: La solución debe evaluar si el filtrado institucional y las identidades en la nube son vulnerables ante la suplantación, bypass de autenticación multifactor o uso malicioso de tokens.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Alineación con Marcos Internacionales (MITRE ATT&CK): La solución debe permitir mapear cada acción de ataque ejecutada directamente contra la matriz de tácticas y técnicas de MITRE ATT&CK para fines normativos y de auditoría.
- Optimización de Parámetros de Pruebas: Debe permitir la optimización y personalización de la intensidad, el alcance, los objetivos bloqueados y las exclusiones de red de forma granular según la evolución de la infraestructura de INDOTEL.
- Análisis y Detección de Vulnerabilidades Operativas: La herramienta debe poder evaluar pasiva y activamente los servicios de red expuestos en los endpoints descubiertos, contrastándolos con debilidades conocidas.
- Reportes Detallados de la postura de Seguridad del INDOTEL: La herramienta debe generar informes detallados que incluyan recomendaciones técnicas de mitigación accionables para que las áreas operativas ejecuten planes sólidos de remediación.
- Capacitación al equipo técnico del INDOTEL: El oferente deberá capacitar al personal, con un total de siete (7) personas, en la configuración, despliegue, interpretación de resultados y mejores prácticas operativas de la plataforma ofertada.
- Adaptación a las Nuevas Amenazas: La solución deberá permitir la actualización constante y automática de su motor de emulación para responder a las nuevas amenazas y técnicas de hacking que aparezcan en el ciberespacio.
- Soporte Técnico 24/7: La solución debe contar con un equipo dedicado al soporte del fabricante o proveedor autorizado, para atender cualquier tipo de eventualidad con una disponibilidad de 24/7.
- Módulo de Orquestación y Automatización de la Remediación: La plataforma debe incluir de forma nativa un componente que consolide, deduplique y enriquezca los hallazgos de red, endpoints e identidades. Debe traducir las rutas de ataque complejas en flujos de trabajo de remediación automatizados, permitiendo asignar tareas con priorización basada en el riesgo real del entorno operativo.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Mecanismo de Parada de Emergencia y Limpieza (Safe Exploitation): La solución debe permitir a los administradores detener de forma instantánea cualquier ataque o simulación en curso mediante un comando centralizado (Panic Button). Asimismo, el motor de la plataforma debe garantizar la eliminación y limpieza automatizada de cualquier instrucción, script temporal o código inyectado en memoria tras la finalización de cada prueba, asegurando la resiliencia operativa y la estabilidad de los sistemas de producción de INDOTEL.
- Validación de Credenciales de la Dark/Deep Web La solución debe integrar de forma nativa fuentes de inteligencia de amenazas que busquen de manera continua correos institucionales comprometidos, contraseñas expuestas y hashes filtrados en la Dark Web y Deep Web. La herramienta debe realizar de forma automatizada y segura ataques de relleno de credenciales (credential stuffing) contra el perímetro de INDOTEL y el Active Directory para verificar el impacto real de dicha filtración.
- Soberanía y Certificación del Repositorio de Datos: Debido a la alta sensibilidad de los mapas de red y caminos de ataque generados por la plataforma, el oferente debe certificar que la infraestructura en la nube (SaaS) donde se alojará la consola cuenta con certificaciones internacionales vigentes de seguridad de la información, tales como ISO/IEC 27001 o SOC 2 Tipo II, garantizando el cifrado de los datos en tránsito y en reposo.
- Descubrimiento Externo Autónomo (EASM): El módulo de evaluación perimetral no debe limitarse a escanear rangos provistos manualmente; debe tener la capacidad de realizar reconocimiento autónomo utilizando técnicas de fuentes abiertas (OSINT) para descubrir de manera constante e independiente el inventario de activos expuestos, subdominios, certificados y servicios web asociados al dominio de INDOTEL, simulando la fase exacta de recolección de información de un atacante real.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Conclusión:

Luego de revisar la documentación aportada, verificar la solicitud y sus soportes, evaluamos las especificaciones técnicas y consideramos que cumplen con todos los aspectos necesarios requeridos y no solapan ningún proyecto que haya de ejecutarse desde la Agenda Digital 2030, esta aprobación tiene vigencia hasta el 11 de septiembre 2026.

Mario Adames
Encargado departamento Asistencia Técnica Especializada
Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)

MF/ma