

Informe de Estudios Previos
Adquisición Plataforma de Pruebas de Penetración Automatizadas y Validación Continua de
Seguridad para el Indotel

Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital
Mayo 2026

INTRODUCCIÓN

El Instituto Dominicano de las Telecomunicaciones (INDOTEL) es el órgano regulador de las Telecomunicaciones en la República Dominicana, creado por la Ley General de Telecomunicaciones 153-98.

Comprometido en continuar garantizando la protección de su infraestructura tecnológica, el INDOTEL gestiona la adquisición de una Plataforma de Pruebas de Penetración Automatizadas y Validación Continua de Seguridad.

I. La necesidad que atender

El INDOTEL, como órgano regulador de las telecomunicaciones en la República Dominicana, tiene la responsabilidad de garantizar la seguridad de los datos y sistemas de las organizaciones que operan en este sector. Para ello, el INDOTEL debe contar con las herramientas y los recursos necesarios para la evaluación proactiva, descubrimiento de vectores de ataque reales y el robustecimiento de la infraestructura de la Tecnología de la Información frente a las amenazas presentes en el ciberespacio.

La solución de Pentesting es una importante herramienta de protección para el INDOTEL porque ayuda a cumplir con el objetivo de fortalecer sus capacidades de protección de las infraestructuras críticas nacionales e infraestructuras TI del Estado al proporcionarle las siguientes funcionalidades:

- Validación de seguridad basada en emulación de adversarios: Permite ejecutar ataques éticos de forma automatizada y sin afectación operativa, evaluando la resistencia real de la infraestructura frente a vectores de ataque modernos.
- Interfaz de usuario centralizada: Permite a los administradores de seguridad programar, ejecutar y gestionar pruebas de penetración tanto internas como externas (enfoque black-box y white-box) desde un único lugar, mejorando la eficiencia y consolidando la visibilidad del riesgo real sin necesidad de desplegar agentes permanentes e intrusivos en cada equipo de la red.
- Actualizaciones constantes con nuevas técnicas de ataque y exploits: Estas actualizaciones aseguran que la plataforma cuente siempre con las últimas tácticas, técnicas y procedimientos (TTPs) alineados al marco MITRE ATT&CK para proteger al INDOTEL frente a amenazas emergentes.

II. Costo Estimado

Luego de revisar propuesta y costo estimado, se determina que la cuenta a imputar para este proceso es la 2.2.5.9.01 LICENCIAS INFORMÁTICAS, por un monto de catorce millones quinientos mil pesos dominicanos con 00/100 (RD\$14,500,000.00)

III. Determinación tipo de contrato

El tipo de contrato para este proceso es de servicios, en el cual el oferente debe suministrar licencias y soporte para la solución de Pentesting, con las siguientes especificaciones:

1. Implementación e integración con la red del INDOTEL.
2. Ejecución automatizada y continua de pruebas de penetración (tanto de red interna como externa).
3. Emulación segura de adversarios dirigida a validar defensas de red, de endpoints y de accesos.
4. Análisis basado en el comportamiento real del atacante, priorizando vulnerabilidades en base a su capacidad de explotación en cadena.
5. Módulo de validación de seguridad de endpoints.
6. Módulo de validación de credenciales y debilidades de autenticación en Active Directory.
7. Licenciamiento con capacidad para evaluar hasta 700 objetivos / direcciones IP activas en simultáneo (*endpoints* o nodos de red).
8. Capacidad de evaluar la misma cantidad de objetivos o accesos asociados a entornos de movilidad e identidades.
9. Integración y validación de seguridad sobre vectores relacionados a ecosistemas en la nube (incluyendo identidades corporativas de Microsoft 365).
10. Soporte 24/7 por el proveedor mientras el contrato este en vigencia.

Este proceso se justifica como proceso de Licitación Pública Nacional (LPN) por el costo estimado, ya que el contrato tendrá vigencia de 2 años (24 meses).

IV. Riesgos

Hemos identificado el siguiente riesgo previsible en esta contratación:

- Sin la herramienta de pentesting la infraestructura tecnológica del INDOTEL no contaría con una plataforma de pruebas de penetración automatizadas y validación continua de seguridad ante amenazas del ciberespacio, por lo que es de vital importancia adquirir esta solución.

V. Garantías para la ejecución del contrato

Para este proceso se requiere la constitución de las siguientes garantías:

1. Garantía de seriedad de la oferta: póliza de garantía bancaria y/o póliza de fianza a favor del INSTITUTO DOMINICANO DE LAS TELECOMUNICACIONES, por un monto equivalente al 1% del valor de la oferta.
2. Garantía de buen uso del anticipo: Solo aplica en caso de Solicitar adelanto del 20%.
3. Garantía de fiel cumplimiento del contrato: Póliza de garantía bancaria y/o póliza de fianza. La vigencia de la garantía será de 01 año, contados a partir de la constitución de la misma hasta el fiel cumplimiento del contrato.

VI. Requisitos de selección del proveedor

La Empresa deberá cumplir con los siguientes requisitos:

- Debe contar con personal de apoyo en el país.
- Debe de ser socio o asociado (partner) del producto.
- El personal que trabaja en la implementación debe demostrar experiencia y certificaciones vigentes en materia de ciberseguridad, hacking ético, o auditorías de seguridad.
- Deberá certificar que el personal asignado posee la condición de Especialista o Asociado certificado por el proveedor directo de la solución.
- Debe demostrar experiencia en por lo menos dos (2) proyectos relativos a la implementación de plataformas de validación de seguridad corporativa o pruebas de penetración.

Además, el proveedor deberá aportar la siguiente documentación:

Requisitos legales:

1. Registro de Proveedores del Estado (RPE).
2. Certificación de la Dirección General de Impuestos Internos (DGII).
3. Certificación de la Seguridad Social en la Tesorería de la Seguridad Social (TSS).
4. Copia del Registro Mercantil expedido por la Cámara de Comercio y Producción correspondiente (vigente).
5. Copia de los Estatutos sociales vigentes debidamente registrado en la Cámara.
6. Copia de la nómina de accionistas y acta de la última asamblea realizada debidamente registrada por ante la Cámara de Comercio y Producción correspondiente.
7. Copia de la nómina de accionistas y acta de asamblea realizada mediante la cual se designe expresamente el actual gerente o consejo de administración, según aplique, que tiene potestad para firmar contratos a nombre de la empresa participante, debidamente registrada por ante la Cámara de Comercio y Producción correspondiente.

8. Documento de Identidad del representante legal (cédula o pasaporte)
9. Formulario de Compromiso ético de proveedores (as) del Estado debidamente firmado y sellado.
10. Formulario Información del Oferente Formulario SNCC.F.042.
11. Poder de representación, si aplica.

Requisitos Técnicos:

Oferta técnica formulario SNCC.F.034 que contenga la descripción y características del servicio requerido.

Requisitos Propuesta Económica:

1. Formulario de Presentación de Oferta Económica (SNCC.F.33).
2. Garantía de fiel cumplimiento del contrato.

DCCEF-I-000019-26

Por la Dirección de Ciberseguridad, Comercio Electrónico y Firma Digital:

Sandra Patricia Herrera Delmonte
Encargada de Ciberseguridad

César Moliné
Director de Ciberseguridad, Comercio Electrónico y Firma Digital