IMPUESTOS INTERNOS

REPÚBLICA DOMINICANA

Ficha Técnica
Proceso de Excepción/ Proveedor Único

DGII-CCC-PEPU-2023-0023

"Renovación plataforma de Emulación de Pentesting".

Santo Domingo, Distrito Nacional

Octubre, 2023

1 Objeto.

La **Dirección General de Impuestos Internos**, le invita a presentar su propuesta para el procedimiento No. **DGII-CCC-PEPU-2023-0023,** correspondiente a la contratación de **"Renovación plataforma de Emulación de Pentesting"**, de acuerdo con las condiciones fijadas en la presente Ficha Técnica.

"Las relaciones con las empresas proveedoras comerciales se realizarán en el marco de las normas y leyes vigentes, a fin de garantizar que dichas empresas realicen sus negocios con integridad y respeto. Se procurará mantener una relación comercial de beneficio mutuo, basada en las más altas normas de conducta comercial y ética"[1].

2 Documentos a Presentar:

a) **Oferta Económica,** el cual deberá estar firmado y con el sello social de la compañía.
   - Descripción del bien o servicio requerido
   - ITBIS transparentado.
   - La Oferta deberá presentarse en pesos dominicanos (RD$).
   - Validez de la oferta

DIRECCIÓN GENERAL DE IMPUESTOS INTERNOS

b) **Copia de la Cédula del representante de la compañía** (persona que firmará el contrato con DGII).

c) **Poder que autorice a la persona que contrata** (En caso de que la persona que vaya a firmar no sea la autorizada a los fines; según la Asamblea General).

d) **Copia de Acta de Asamblea General Ordinaria, vigente,** a través de la cual se designe expresamente el actual gerente de la sociedad comercial / consejo de administración (Dependiendo del órgano de administración que aplique) que tiene potestad para firmar contratos a nombre de la sociedad comercial.

e) **Copia de Registro Mercantil actualizado,** emitido por la Cámara de Comercio y Producción correspondiente.

f) **Perfil de la Empresa.**

g) **Propuesta Técnica de los servicios ofrecidos,** describiendo os servicios solicitados y los requerimientos de la presente ficha.

h) **Carta de autorización del FABRICANTE** que le autoriza a ofrecer los bienes y servicios que oferta, y a comercializar de manera válida los servicios de soporte tal cual como es requerido por cada lote en el cual participa.

i) **Currículo de mínimo 3 técnicos certificados por el Fabricante** para dar soporte a las tecnologías ofrecidas con copia de certificación de dichos técnicos, por cada lote en el cual participa.

j) **Matriz de escalación a incidentes** confirmando los tiempos de respuesta indicadas en el RP03.

[1] Código de Ética de la Dirección General de Impuestos Internos (DGII).

k) **Cronograma** propuesto de mantenimientos preventivos a lo largo de la duración del contrato

3 Especificaciones Técnicas.

Renovación de plataforma de emulación de Pentesting.

En el marco del fortalecimiento del Centro de Operaciones de Seguridad (SOC) de la Dirección General de Impuestos Internos (DGII) con fines de seguir incrementando la detección y gestión de vulnerabilidades técnicas, las pruebas de penetración y detección de amenazas en la infraestructura tecnológica de la institución y descubrir su exposición real a nivel de seguridad en un tiempo optimo e ir disminuyendo el riesgo cibernético se requiere de la renovación de la Plataforma de Emulación de Pentesting, una herramienta tecnológica que ha permitido alcanzar la eficiencia y ha servido de apoyo al personal del área para optimizar sus niveles de protección a corto, mediano y largo plazo.

Esta herramienta ha permitido implementar un servicio de automatizado que brinda un reporte detallado de las vulnerabilidades explotables y permita llevar a cabo proyectos de Pentesting puntuales dentro de la organización.

DIRECCIÓN GENERAL DE IMPUESTOS INTERNOS

Por tal razón y con fines de cubrir las necesidades presentadas se requieren lo siguientes:

ítem	Descripción	Especificaciones Técnicas	Cantidad Solicitada
1	Up to 3,000 Endpoints	Pentera Core Software - Up to 3000 Endpoints	3000
2	Pentera Pack	12 Meses Licencia Validada	12

4 Requerimientos al Proveedor

El oferente debe satisfacer los requisitos enumerados a continuación. Para experiencia en la validación de la oferta a presentar, se requiere que el oferente coloque la correspondiente tabla de requerimientos completada y con las referencias necesarias para constatar el cumplimiento.

Ítem	Descripción
RP01	El oferente debe contar con la **certificación del fabricante**, que le autoriza a ofrecer los bienes y servicios que oferta, y a comercializar de manera válida los servicios de soporte tal cual como es requerido.
RP02	El soporte debe ser entregado por técnicos certificados por el Fabricante para dar soporte a las tecnologías ofrecidas. A este efecto, el oferente presentará el currículo y certificación de dichos técnicos (mínimo 3).
RP03	El oferente debe presentar una **matriz de escalación** para atención a incidentes, confirmando los tiempos de escalación. Se requiere que la recepción del caso vía telefónica se realice a los diez (10) minutos de contactar al oferente adjudicatario, el involucramiento del personal competente dentro de los sesenta (60) minutos de

	apertura del incidente, y de ser necesario, escalación al FABRICANTE dentro de los primeros ciento (120) veinte minutos a la apertura del incidente. La matriz debe identificar, para cada nivel de escalación, el número de contacto telefónico y la dirección de correo electrónico. En el caso de los dos mayores niveles jerárquicos en la matriz de escalación, también debe incluirse el nombre del gerente responsable y el número celular correspondiente.
RP04	El oferente debe presentar un **cronograma** propuesto de mantenimientos preventivos a lo largo de la duración del contrato.
RP05	Los trabajos de instalación, implementación u otros servicios de soporte serán realizados en la Sede Central de la DGII.

5 Requerimientos Técnicos:

Requerimiento	Descripción
RT01	La propuesta de los oferentes debe incluir todo hardware, software y licenciamientos necesario para el debido funcionamiento de los servicios que estamos adquiriendo. Una vez se produzca la adjudicación, no se aceptarán nuevos costos adicionales por hardware, software, servicios profesionales y licenciamientos que no hayan sido contemplados con antelación en su oferta. **Nota: Es responsabilidad del oferente el pedir aclaración sobre cualquier aspecto de estos términos de referencia cuando a juicio de dicho oferente, la aclaración le resultase necesaria para la correcta interpretación de los términos y condiciones.**
RT02	La disponibilidad de soporte requerido es de Domingo a Jueves 9:00 AM-6:30 AM y de 9:00 AM a 5:30 PM de Lunes a Viernes a partir de la fecha de entrega de las licencias. Esto incluye los días de festivos.
RT03	La solución debe tener la capacidad de instalación, configuración, mantenimiento sin necesidad de agentes.
RT04	La solución debe tener la capacidad de desafíar la seguridad de los endpoints con cargas útiles éticas para emular un ataque real escenarios.
RT05	La solución debe permitir pruebas de penetración con 1 clic y de forma completamente automatizado.
RT06	La solución debe cubrir la evaluación de vulnerabilidades, la validación del control de seguridad, validación de la solidez de las credenciales, integridad de la segmentación, higiene de datos confidenciales, pruebas de equipos de red y auditorías de acceso privilegiado.
RT07	La solución debe orientarse a debilidades de factor que se pueden romper, priorizando la remediación esfuerzos solo en vulnerabilidades con potencial de impacto comercial real mientras se eliminan falsos positivos. Todas las herramientas de simulación generan por definición (simulación) más alarmas falsas.
RT08	La solución debe ofrecer capacidad de realizar emulación de ataques reales y actuales sin agentes.

DIRECCIÓN GENERAL DE IMPUESTOS INTERNOS

Requerimiento	Descripción
RT09	La solución debe ofrecer capacidad de emular ataques de ransomware con encryption y dejar evidencias.
RT10	La solución debe ofrecer la capacidad de Soporte de puerto troncal para acceso a PenTest de múltiples VLAN.
RT11	La solución debe ofrecer la capacidad de Identificación y consulta automática de DC de Active Directory.
RT12	La solución debe ofrecer la compatibilidad con el formato CIDR de rango (s) de IP.
RT13	La solución debe ofrecer la capacidad de testear Servidores web / con diversas técnicas de descubrimiento y enumeración de aplicaciones.
RT14	La solución debe ofrecer acceso directo a WiKi con información de remediación completa de los hallazgos.
RT15	La solución debe generar un informe del tipo ejecutivo al momento de concluir las pruebas.
RT16	La solución debe ofrecer la capacidad de movimiento lateral y ejecutar acciones de explotación y post-explotación
RT17	La solución debe ofrecer la capacidad de ejecutar técnicas de evasión de EDR/NGAV.
RT18	La solución debe Sondear una red determinada identificando direcciones IP activas, puertos y detalles de topología y descubrimiento de todos los hosts, servidores y dispositivos relacionados.
RT19	La solución debe escanear los hosts activos en busca de vulnerabilidades conocidas.
RT20	La solución debe realizar intercepción de tráfico de red y datos relacionados con el host para extraer credenciales de los usuarios con especial atención a los usuarios privilegiados, incluidas las cuentas de dominio de AD y las cuentas locales.
RT21	La solución debe utilizar varias medidas para recuperar contraseñas de texto sin formato de usuarios, hosts y servidores descifrando hash de contraseñas a partir de datos almacenados o transportados desde un sistema mediante una combinación de técnicas de diccionario y de fuerza bruta.
RT22	La solución debe Interceptar las comunicaciones entre dos partes y transmita los datos a otro dispositivo (de terceros), incluidas las técnicas basadas en la red MITM.
RT23	La solución debe utilizar múltiples métodos para la ejecución remota de código en un sistema determinado mediante el uso de capacidades de evasión de defensa para evitar los mecanismos de detección AV / EDR y abrir un canal C&C para controlar el ataque al dispositivo objetivo.
RT24	La solución debe tener capacidades remotas y locales para escalar usuarios sin privilegios a poder ejecutar código con altos permisos.
RT25	La solución debe gestionar un procedimiento de extracción dedicado de material de autenticación para poder pivotar lateralmente a nuevos puntos finales en la red.
RT26	La solución debe realizar la limpieza de los residuos creados por el ataque.

DIRECCIÓN GENERAL DE IMPUESTOS INTERNOS

6 Duración del Suministro

La Convocatoria del proceso se hace sobre la base de un suministro para un período aproximado de **(12) meses,** contados a partir de **la entrega de las licencias,** conforme se establezca en el Cronograma de Entrega de Cantidades Adjudicadas.

7 Requisito de Entrega

Todo el licenciamiento y contratos requerido en la presente ficha, debidamente entregado y registrado a nombre de la DGII, con la documentación que lo comprueba, emitida por parte del fabricante y validado en su sitio web.

8 Cronograma de Entrega.

Ítem	Periodo de Entrega
Renovación de Plataforma de Emulación de Pentesting	• Entrega de licencias 10 días calendario luego de firmado el contrato o la Orden de compra.

DIRECCIÓN GENERAL DE IMPUESTOS INTERNOS