"CONSULTORÍA PARA EVALUAR LA SEGURIDAD EN LA RED DEL INSTITUTO DE PREVISIÓN MILITAR (ETHICAL HACKING) POR UN ENTE EXTERNO, SEGÚN CONCURSO PÚBLICO NO. IPM-CPN-GC-2022-003".

Nosotros, **ALFREDO FABRICIO ERAZO PUERTO**, Coronel retirado, mayor de edad, casado, hondureño, con Documento Nacional de Identificación número 0101-1966-01501, actuando en mi condición de Gerente y Representante Legal del **INSTITUTO DE PREVISIÓN MILITAR (I.P.M.)** Organismo con Personalidad Jurídica y Patrimonio Propio, según Decreto Número Ciento Sesenta y Siete guión Dos Mil Seis (167-2006) emitido por el Soberano Congreso Nacional el Veintisiete (27) de Noviembre del año Dos Mil Seis de(2006), con facultades suficientes para celebrar este contrato, nombrado por la Junta Directiva del Instituto de Previsión Militar, en Sesión Extraordinaria Número Ciento Cincuenta y Uno (151) mediante Resolución Número Cuatro Mil Novecientos ochenta y tres (4983) de fecha Nueve (09) de Marzo del año dos mil veinte (2020) y el Poder General de Representación y de Administración otorgado mediante Instrumento Público número Cincuenta y ocho (58) autorizado en esta ciudad ante los oficios del Notario David Alfonso Velásquez el Doce (12) de Marzo del año Dos Mil Veintiuno (2021) e inscrito bajo el número cuarenta y tres (43) del Tomo trescientos cinco (305) del Registro Especial de Poderes del Registro de la Propiedad del Departamento de Francisco Morazán y quien en lo sucesivo y para efectos del presente contrato me denominaré como **EL INSTITUTO** y **JUAN CARLOS INESTROZA LOZANO,** mayor de edad, hondureño, Ingeniero en Sistemas, casado, con Documento Nacional de Identificación No. 1007-1984-00146, con RTN número 10071984001467, de este domicilio, actuando en mi condición de Representante legal de la Sociedad **IT GLOBAL CORPORATION S. DE R.L. DE C.V.** con RTN 05019010309480 Sociedad constituida en instrumento público No. 95, de fecha 13 de julio de 2010, ante los oficios del Notario Amilcar Zelaya Lozano, la cual se encuentra debidamente inscrita con matricula número 2516110, número 6566, del Registro Mercantil de Francisco Morazán, Centro Asociado al IP, con facultades suficientes y para efectos de este contrato me denominaré como **EL CONTRATISTA**, hemos convenido en celebrar la presente **CONTRATACIÓN DE CONSULTORÍA PARA EVALUAR LA SEGURIDAD EN LA RED DEL INSTITUTO DE PREVISIÓN MILITAR (ETHICAL HACKING) POR UN ENTE EXTERNO, SEGÚN CONCURSO PÚBLICO NO. IPM-CPN-GC-2022-003,** Aprobado en Comité de Compras y Licitaciones No. 06-2023 del 15 de febrero de 2023 y Resolución de Gerencia de fecha 15 de febrero de 2023, el cual se regirá por las cláusulas y condiciones siguientes: **PRIMERA: OBJETO DEL CONTRATO**: La consultoría para evaluar la seguridad en la red del IPM según lo siguiente:

1. Propósito y Objetivo de la Contratación:
   1.1 Los servicios que se solicitan se listan a continuación:
      1.1.1 Pruebas de penetración a red interna
      1.1.2 Pruebas de penetración a red externa
      1.1.3 Análisis de Vulnerabilidades de páginas / sitios / aplicaciones web internas y externas.
      1.1.4 Análisis de Vulnerabilidades de redes inalámbricas.
      1.1.5 Pruebas de Ingeniería Social (Phishing) y llamadas telefónicas.
      1.1.6 Pruebas de seguridad a aplicaciones Móviles.

   1.2 Los datos necesarios para la elaboración del dimensionamiento de los servicios en cuestión.

   1.3 Los objetivos que se persiguen alcanzar al finalizar la entrega del servicio.

   1.4 Las características específicas mínimas que se esperan del servicio.

   1.5 Las características específicas mínimas que se esperan de los oferentes.

   1.6 Los criterios de calificación que se utilizarán para escoger al mejor oferente.

   Se espera como respuesta a los requerimientos de este documento, lo siguiente:

   1.7 Una (1) propuesta técnica donde se exprese claramente las actividades, metodología, cronograma y entregables para cada uno de los servicios requeridos.
   1.8 Una (1) propuesta económica comercial conteniendo los precios, presentados de forma separada para cada uno de los servicios requeridos.

1.9 El contratista deberá utilizar una metodología para ejecución de las pruebas, que deberá estar basada en las mejores prácticas conocidas y aplicadas a nivel internacional, como las siguientes:

1.9.1 Technical guide to information security testing and assessment – NIST USA.
1.9.2 Conducting a Penetration Test on an Organization – SANS Institute InfoSec.
1.9.3 Open Web Application Security Project® (OWASP).

2 Entorno de la Organización y Alcance del Servicio

El Instituto de Previsión Militar posee las siguientes características:

2.1 Cantidad de sucursales principales ubicadas en:

2.1.1 Sede principal – Tegucigalpa M.D.C Honduras, Edificio Principal IPM, Blv. Centroamérica

2.2 Cantidad de centros de datos y ubicación:

2.2.1 Un (1) Centro de Datos ubicado en la ciudad de Tegucigalpa M.D.C Honduras, edificio principal de IPM.

2.2.2 Un (1) Centro de Datos ubicado en la ciudad de San Pedro Sula, Honduras, edificio principal de IPM.

2.3 Se adjunta a continuación el detalle de la cantidad activos y su tipo para las pruebas técnicas de seguridad requeridas a realizar:

2.3.1 Dieciséis (16) direcciones IP Públicas – para pruebas a red externa.
2.3.2 Activos de la red interna a someter a las pruebas 200 equipos (entre servidores y equipos de telecomunicaciones).
2.3.3 Diez (10) aplicaciones WEB de uso externo y 15 aplicaciones WEB de uso interno.
2.3.4 Una (1) aplicación Móvil corriendo en Android e IOs
2.3.5 Quince (15) SSIDs de la red inalámbrica, ubicados en la misma localidad física.
2.3.6 Phishing a 150 buzones de correo electrónico, Realización de al menos 5 llamadas telefónicas utilizando técnicas de Ingeniería social.
2.3.7 150 Estaciones de trabajo PC, Portátiles.
2.3.8 50 Servidores virtuales/físicos
2.3.9 Firewall
2.3.10 Routers
2.3.11 Switches

2.4 Realizar plan de remediación de vulnerabilidades encontradas y apoyar con la resolución de estas.
2.5 Realizar pruebas de funcionamiento y efectividad de los controles de seguridad implementados en el Instituto de Previsión Militar. (Este debe ser un informe aparte en el cual se pueda evidenciar los mismos con imágenes) (Estas deben ser coordinadas y acompañadas por la Unidad de Seguridad de la Información.
2.6 Entrenamiento para personal de Seguridad de la Información del IPM (3 Personas), en temas de Hacking Ético al menos 50 horas. (El entrenamiento debe ser teórico práctico y utilizando contenidos oficiales de EC-Council última versión) (Tiene que ser presencial).
2.7 Re test: Ejecutar una nueva evaluación o pruebas a los equipos para medir la confiabilidad de los controles implementados, verificando si se subsanaron las vulnerabilidades encontradas.

3 Requerimiento

3.1 OBJETIVO GENERAL

El IPM busca la asesoría de una empresa con vasta experiencia en Ciberseguridad para la ejecución de varias Pruebas técnicas de seguridad de la información, como parte de su plan de mejora continua de la postura en materia de Seguridad informática para toda la organización.

3.2 OBJETIVOS ESPECÍFICOS

El IPM contratará los servicios que como entregable final le permitan cumplir con los siguientes objetivos:

3.2.1 Analizar y evaluar la infraestructura tecnológica crítica de la organización.

3.2.2 Identificar los posibles riesgos y obtener recomendaciones puntuales conducentes a su mitigación.

3.2.3 Evaluar la cultura de los colaboradores del IPM en términos de seguridad informática.

3.2.4 Remediación vulnerabilidades críticas y altas.

3.2.5 Generar capacidades técnicas para ejecutar hacking ético al personal del IPM.

3.2.6 Re Test, verificando la subsanación de vulnerabilidades críticas y altas.

4 Características del Servicio

Las pruebas para ejecutar no deberán en ningún momento crear un incidente que suspenda la disponibilidad de la información, de los servicios que serán revisados y que están en producción del IPM.

El servicio de consultoría que se contrate deberá contemplar las siguientes características mínimas

4.1 Actividades mínimas esperadas:

4.1.1 Ejecutar Pruebas de penetración a la Red Externa sobre las direcciones IP Públicas.

a. Reconocimiento de red:
Se espera se determine vía la utilización de herramientas específicas detalles de los siguientes puntos:

- Puertos abiertos, cerrados y filtrados
- Servicios activos
- Protocolos expuestos identificados
- Tipos de servicios y nivel de parchado
- Tipos de sistemas operativos y sus versiones
- Cuentas de usuario por defecto

b. Evaluación Automatizada:
Se espera que el oferente utilice para la ejecución de sus actividades herramientas que se enfocan en encontrar y confirmar vulnerabilidades en los equipos y servicios dentro del alcance en la red externa, tales como: NMAP, Nessus entre otras.

c. Explotación de vulnerabilidades en base a riesgo y verificación de resultados:
Una vez obtenidos los resultados de las herramientas automatizadas, el Analista revisa cada uno de éstos, en busca de vulnerabilidades que le permitan ganar acceso a algún sistema, emulando las tácticas y métodos de un atacante malicioso. El analista utilizará las herramientas necesarias para determinar la viabilidad de la explotación de las vulnerabilidades, y el impacto que resultaría al explotarlas de manera exitosa.

Con estos datos, se evalúan uno a uno los puertos abiertos encontrados y se determina la posibilidad de realizar un descubrimiento más profundo dependiendo del servicio disponible. Para tal efecto, se realiza la exploración profunda de los diferentes servicios encontrados. Esto implica determinar la versión del mismo, buscar debilidades comunes de configuración y vulnerabilidades conocidas.

Posteriormente, se realizan ataques de fuerza bruta utilizando la información recopilada en las etapas anteriores sobre los servicios que requieran autenticación. De esta manera se ponen a prueba los mecanismos contra este tipo de ataques y la complejidad de las contraseñas.

En cada explotación exitosa de una o más vulnerabilidades, se recopila evidencia relevante (capturas de pantalla, listados, o información extraída) y se documenta la forma en que se logró vulnerar el sistema.

Detalles técnicos que el analista ejecuta en el procedimiento:

- Recolección de respuestas de red.
- Test de traspaso de firewall con TTL firewalking.
- Utilizar ICMP y Lookup inversos para determinar la existencia de máquinas de red.
- Utilizar fragmentos TCP con FIN, NULL y XMAS en los puertos 21, 22, 25, 80 y 443 de los hosts encontrados en la red.
- Utilizar TCP SYN (half open) para enumerar puertos que estén cerrados, filtrados o abiertos en todos los hosts encontrados en la red.
- Utilizar fragmentos TCP para puertos y servicios disponibles en los hosts.

- Utilizar paquetes UDP para enumerar puertos abiertos en todos los hosts encontrados de la red.
- Intentar identificar los protocolos estándar.
- Intentar identificar los protocolos no estándar.
- Intentar identificar protocolos encriptados.
- Identificar fecha, hora y Up-Time del sistema.
- Identificar la predictibilidad de los números de secuencia TCP.
- Identificar la predictibilidad de los números de secuencia TCP ISN.

d. Elaboración de reporte:

En el reporte se incluyen las vulnerabilidades reportadas por las herramientas mencionadas, y ratificadas de manera manual por el analista. Estos hallazgos se clasificarán de acuerdo a su nivel de criticidad, basándose en la facilidad de explotar una vulnerabilidad y el impacto que esta explotación podría tener en la infraestructura de Grupo IPM.

Se incluirán también todas las vulnerabilidades utilizadas para realizar las penetraciones en los diferentes sistemas y se describirán los hallazgos guardados al momento de ser encontrados. Cada una de las vulnerabilidades explotada será acompañada del detalle de la metodología utilizada por el Analista.

El reporte incluirá un resumen ejecutivo, que describirá de manera breve y concisa los descubrimientos de la evaluación, así como una sección en la que se incluyen los detalles técnicos y recomendaciones para corregir las vulnerabilidades encontradas.

El reporte debe contener gráficos generales y especifico de niveles de riesgo por vulnerabilidades (critico, alto, medio).

4.1.2 Ejecutar Pruebas de penetración a la Red Interna, usando una herramienta especializada y líder en la industria:

a. Reconocimiento de red:

Se espera se determine via la utilización de herramientas específicas detalles de los siguientes puntos:

- Puertos abiertos, cerrados y filtrados
- Servicios activos
- Protocolos expuestos identificados
- Tipos de servicios y nivel de parchado
- Tipos de sistemas operativos y sus versiones
- Cuentas de usuario por defecto

b. Evaluación Automatizada:

Se espera que el oferente utilice para la ejecución de sus actividades herramientas que se enfocan en encontrar y confirmar vulnerabilidades en los equipos y servicios dentro del alcance en la red interna, tales como: NMAP, Pentera, Nessus.

c. Explotación de vulnerabilidades en base a riesgo y verificación de resultados:

Una vez obtenidos los resultados de las herramientas, el Analista revisa cada uno de éstos, en busca de vulnerabilidades que le permitan ganar acceso a algún sistema, emulando las tácticas y métodos de un atacante malicioso. El analista utilizará las herramientas necesarias para determinar la viabilidad de la explotación de las vulnerabilidades, y el impacto que resultaría al explotarlas de manera exitosa.

Con la información obtenida de estas herramientas, el analista se encargaría de utilizar, por ejemplo, hashes de contraseñas o credenciales en texto claro, para intentar comprometer más equipos de los que ya fueron comprometidos durante la prueba automatizada.

Dentro de las actividades a realizar por el analista posterior a análisis automatizado deberían estar SMBSpray (compromiso de protocolo SMB a partir de hashes o

contraseñas obtenidas), evaluación de antivirus en equipos no comprometidos, movimiento lateral en la red, etc.

En cada explotación exitosa de una o más vulnerabilidades, se recopila evidencia relevante (capturas de pantalla, listados, o información extraída) y se documenta la forma en que se logró vulnerar el sistema.

d. Elaboración de reporte:
Se entregará a IPM el reporte generado por la herramienta utilizada. Este informe incluirá todas las vulnerabilidades que fueron encontradas por el software, los accesos exitosos para la explotación de dichas vulnerabilidades y las recomendaciones que brinda la plataforma para remediarlas.

En el reporte se incluyen las vulnerabilidades reportadas por las herramientas mencionadas, y ratificadas de manera manual por el analista. Estos hallazgos se clasificarán de acuerdo a su nivel de criticidad, basándose en la facilidad de explotar una vulnerabilidad y el impacto que esta explotación podría tener en la infraestructura de Grupo IPM.

Se incluirán también todas las vulnerabilidades utilizadas para realizar las penetraciones en los diferentes sistemas, describiendo en detalle cada uno de los hallazgos. Cada una de las vulnerabilidades explotada será acompañada del detalle de la metodología utilizada por el Analista.

4.1.3 Ejecutar un análisis de vulnerabilidades de páginas /sitios / aplicaciones web.

a. Reconocimiento de página web:
Se requiere se lleve a cabo una evaluación del sitio por completo a través de una herramienta que realiza una copia de todas las páginas y crea un mapa de sitio. Con estos datos se identifican los lenguajes de programación y aspectos del ambiente con que fue construida la página o servicio web. Además, se trata de identificar la base de datos que utiliza la página o cualquier otro servicio que sea consumido por la misma.

b. Evaluación Automatizada:
El Analista deberá realizar un escaneo automatizado utilizando herramientas que se enfoquen en encontrar vulnerabilidades en las páginas o servicios web objeto del alcance. Algunas de las herramientas que se espera se utilicen son: Burp, Nmap, DirBuster.

Deberán tomarse en cuenta los siguientes detalles técnicos incluidos en el procedimiento:

Descubrimiento de sitios/aplicaciones

- Gestión de extensiones de archivos en aplicaciones web.
- Cuentas de usuario por defecto o adivinables en servicios y aplicaciones web.
- Puertos abiertos, cerrados y filtrados
- Servicios activos
- Autenticación: Transporte de credenciales, Manejo de contraseñas, Finalización de sesiones y caché.
- Autorización: Lectura de archivos arbitrarios, Limites de privilegios
- Gestión de sesiones: Mecanismo de manejo de sesiones, Cookies fijación de sesiones.
- Validación de datos: Inyección de código, HTTP Spliting, Inclusión de archivos arbitrarios, Cross-site scripting, Inyección de SQL, Inyección de LDAP, XML, SSI, Xpath.
- Manejo de errores.

c. Verificación de resultados:
Se deben revisar los resultados de las herramientas automatizadas para verificar que no existen falsos positivos. Se toman los resultados de las herramientas automatizadas y se verifica que las vulnerabilidades encontradas existan y se analiza el impacto de seguridad que tiene cada una. Estos resultados verificados se deben integrar al reporte final.

d. Evaluación Manual:

Se requiere ejecutar la explotación de las vulnerabilidades relevantes y previamente validadas buscando si se podría llegar a comprometer la confidencialidad e integridad de la aplicación. La metodología para realizar dicha explotación puede variar dependiendo de la aplicación, procurando siempre efectuar acciones que no afecten la disponibilidad o que presenten el riesgo mínimo para la misma.

e. Elaboración de reporte.

El reporte debe incluir las vulnerabilidades detectadas. Estos hallazgos se clasificarán de acuerdo a su nivel de criticidad, basándose en la facilidad de explotar una vulnerabilidad y el impacto que esto puede tener en la infraestructura del cliente.

El reporte incluirá un resumen ejecutivo, que describirá de manera breve y concisa los descubrimientos de la evaluación, así como una sección en la que se incluyen los detalles técnicos. Así mismo, se deben incluir las recomendaciones pertinentes para corregir las vulnerabilidades encontradas

4.1.4 Ejecutar un análisis de vulnerabilidades de redes inalámbricas.

a. Pruebas de seguridad a red inalámbrica:

- Niveles de cifrado:

Se debe revisar si los niveles de cifrado utilizados son los óptimos para asegurar que la información se está transmitiendo de forma segura

- Detección de puntos de acceso no autorizados

  Se detectarán los puntos de acceso no autorizados por la organización

- Nivel de señal en el perímetro

  Se evaluará la potencia y el alcance de la red inalámbrica para verificar que ésta se encuentre dentro del rango de la organización.

- Revisión de políticas, configuración y arquitectura mediante entrevista

  Se requiere que, vía entrevista al personal encargado de seguridad de la información, se soliciten las políticas pertinentes a las redes inalámbricas y se haga una revisión de las mismas para verificar y determinar el nivel de seguridad en la red.

b. Elaboración de reporte

Se debe entregar un reporte que incluya todos los hallazgos que surgieron durante dicha evaluación, así como las observaciones proporcionadas por el experto en seguridad y las recomendaciones a tomar en cuenta para la remediación de las vulnerabilidades encontradas.

4.1.5 Ejecutar pruebas de Ingeniería Social (Phishing) y llamadas telefónicas.

a. Reunión de planificación, donde se determinen conjunto de usuarios que van a estar sujetos a las pruebas, se definan plantillas de script a utilizar, etc.
b. Definición del vector de ataque.
   Se debe determinar cuáles serán los objetivos de la prueba y se debe elaborar la plantilla del mensaje a enviar.
c. Realización de Ataque de Phishing.
   Sera el proceso mediante el cual se envía(n) mensaje(s) a los usuarios determinados en el alcance de las pruebas.

d. Elaboración de reporte.
   Se requiere un informe mediante el cual se muestre las estadísticas de cuántos usuarios han sido "vulnerados" con el ataque de phishing

4.1.6 Ejecutar pruebas de seguridad a aplicaciones móviles.

a. Levantamiento de Información:

Consiste en el levantamiento de tanta información como sea posible de la aplicación móvil y muchos datos son obtenidos a través de Grupo IPM, tales como:

b. Análisis del ambiente:
   a. Propósito de las aplicaciones móviles y funcionalidades

   b. Quienes son las partes interesadas que hacen uso de la aplicación

c. Cuál es el proceso interno que interviene para el funcionamiento de la aplicación

c. Análisis de la arquitectura:
d. Interfaces de red

e. Datos utilizados

f. Comunicación con otras fuentes

g. Gestión de sesión

h. Runtime

i. Servicios de backend

d. Modelado de ataque
Derivado del levantamiento de información, se deberá hacer un modelado de ataque para identificar las amenazas que podrían explotar una vulnerabilidad en la aplicación móvil.

e. Métodos de ataque
En esta fase se deberán definir los métodos de ataque que podrían materializar las posibles vulnerabilidades en la aplicación. Estos métodos de ataque son los que se utilizarán para probar las vulnerabilidades basándose en el Top 10 de OWASP para aplicaciones móviles.

f. Controles
Se debe hacer un levantamiento de información y entendimiento de qué clase de controles de seguridad han sido implementados proactivamente como medida para prevenir los ataques.

g. Análisis de vulnerabilidades
Al probar cada uno de los escenarios creados que se hayan identificado como posibles amenazas y complementando con el Top 10 de OWASP podrá determinarse la existencia de vulnerabilidades como, por ejemplo: en el código, en la llamada y manipulación a funciones específicas, bypass de autenticación, búsqueda de credenciales, lectura de archivos utilizados por la aplicación después del llamado de cierta función, etc. Se requiere que el analista determine si será necesario el análisis del tráfico que pasa a través de la red y que se origina desde las aplicaciones hasta los recursos a los cuales realiza la petición, esto dependerá de los resultados del análisis. Es importante que este análisis se haga en apego a lo estipulado por el Top 10 de OWASP.

h. Elaboración de reporte
Una vez terminadas las fases descritas anteriormente el analista procederá a informar todas las conclusiones y hallazgos encontrados. Entre estos, estarán las vulnerabilidades clasificadas por impacto, evidencia encontrada y recomendaciones a seguir para mitigar y/o eliminar la debilidad.

4.1.7 Realizar plan de remediación de vulnerabilidades encontradas y apoyar con la resolución de estas.
   a. En coordinación de la Unidad de Seguridad de la Información y la División de Tecnología del IPM.
   b. Elaboración de Reporte. Una vez terminadas las fases descritas anteriormente el analista procederá a informar todas las conclusiones y hallazgos encontrados. Entre estos, estarán las vulnerabilidades clasificadas por impacto, evidencia encontrada y recomendaciones a seguir para mitigar y/o eliminar la debilidad.

4.1.8 Realizar pruebas de funcionamiento y efectividad de los controles de seguridad implementados en el Instituto de Previsión Militar. (Este debe ser un informe aparte en el cual se pueda evidenciar los mismos con imágenes) (Estas deben ser coordinadas y acompañadas por la Unidad de Seguridad de la Información).
   a. Realizar pruebas que evidencien el funcionamiento de los controles implementados.
   b. En coordinación de la Unidad de Seguridad de la Información y la División de Tecnología del IPM.
   c. Elaboración de Reporte. Una vez terminadas las fases descritas anteriormente el analista procederá a informar todas las conclusiones y

hallazgos encontrados. Entre estos, estarán las vulnerabilidades clasificadas por impacto, evidencia encontrada y recomendaciones a seguir para mitigar y/o eliminar la debilidad.

4.1.9 Entrenamiento para personal de Seguridad de la Información del IPM (3 personas), en temas de Hacking Ético al menos 50 horas. (El entrenamiento debe ser teórico práctico y utilizando contenidos oficiales de EC-Council última versión).

a. Para 3 personas.
b. Instalación, configuración y uso de Kali Linux, para realizar hacking ético.
c. Contenido oficial de EC-Council. (última versión).
d. Debe ser Presencial, no en línea. Prácticas, configuraciones y contenidos. (El IPM dispondrá de los tiempos, coordinado con el oferente)

El oferente deberá considerar que, en la ejecución del servicio solicitado en el presente cartel, no se afecte en ningún momento la disponibilidad ni integridad de los servicios tecnológicos o la información almacenada en equipos del IPM o que se trasmitan por medio de la red de comunicación de este.

El contratista deberá documentar y evidenciar las pruebas realizadas, entregando toda la evidencia-documentación recopiladas al departamento de Seguridad Informática.

e. Entregables mínimos requeridos

Para cada uno de los servicios especificados anteriormente, se entregará el informe con los hallazgos que incluyen recomendaciones específicas para la mitigación de las vulnerabilidades encontradas. Dicho informe será entregado en un plazo máximo de 15 días después de finalizadas todas las pruebas el cual deberá incluir al menos:

1. Un Documento con Sección Ejecutiva final, con al menos:

- Resumen del estado general de los sistemas de información.
- Recomendaciones generales
- Información encontrada o detectada

2. Un Documento con Sección Técnica final, con al menos:

- Detalle de tareas, pruebas y herramientas utilizadas.
- Riesgos de seguridad identificados y clasificados.

3. Plan de Remediación de Vulnerabilidades y el informe de la remediación de estas.
4. Informe Ejecutivo y Técnico, sobre la efectividad de los controles técnicos implementados en el IPM.
5. Certificados para los colaboradores de Seguridad de la Información.
6. Presentaciones, con el contenido antes detallado.

4.3 Herramientas

1. El oferente deberá presentar junto con su oferta el listado de las herramientas de seguridad que utilizará en el desarrollo de las pruebas que formarán parte de este proceso de contratación, deberá incluir al menos dos herramientas de uso licenciado y de pago (uso comercial) para las pruebas de penetración automatizadas de la red externa e interna.

f. Características del Oferente

Por la naturaleza del servicio solicitado, se solicita una empresa con un mínimo de 10 años en la industria de Seguridad de la información, hacking ético y Ciberseguridad.

Adicionalmente todos los oferentes deberán cumplir con las siguientes características mínimas:

a. Certificaciones

Poseer en su planilla al menos:

a. Un (1) gestor de proyecto con grado de maestría en gestión de proyectos con más de 5 años de experiencia
b. Un (1) profesionales certificados como Licensed Penetration Tester
c. Dos (2) profesionales certificados como Ethical Hackers
d. Al menos (3) profesional certificados como Auditores de la Norma ISO 27,001
e. Dos (2) profesionales certificados como auditores de la Norma ISO 22,301
f. Dos (2) profesionales certificados como Lead CyberSecurity Professional Certificate o CISM.

b. Experiencia en servicios similares

Presentar al menos las siguientes referencias:

a. Cuatro (4) cartas de referencia de servicios de Pruebas técnicas de Seguridad similares a las solicitadas en este RFP en las cuales se deben de evidencias las siguientes pruebas:

   Análisis de vulnerabilidades de páginas/sitios web.

   Análisis de vulnerabilidades de redes inalámbricas.

   Pruebas de Ingeniería Social.

Lo anterior debe ser en empresas, similares o más grandes que el IPM. Todo lo anterior especificado en las bases del concurso. **SEGUNDA: MONTO DEL CONTRATO:** El monto del contrato es por **CUATROCIENTOS NOVENTA Y SEIS MIL OCHOCIENTOS LEMPIRAS EXACTOS (L. 496,800.00)**, valor que incluye el ISV, el cual será retenido por el IPM. **TERCERA: FORMA DE PAGO: EL INSTITUTO** realizará sus pagos bajo la modalidad de cronograma de trabajo según informe aprobado por la Unidad de Seguridad de la Información del IPM. **CUARTA: SUPERVISIÓN POR PARTE DEL INSTITUTO:** la Unidad de Seguridad de la Información del IPM asignará una persona que se encargará de verificar la calidad de los servicios solicitados.- **QUINTA: GARANTÍA DEL CONTRATISTA: UNA GARANTÍA DE CUMPLIMIENTO DE CONTRATO** equivalente al 10% del monto del contrato, según art.106 de la Ley de Contratación del Estado, por un valor de **CUARENTA Y NUEVE MIL SEISCIENTOS OCHENTA LEMPIRAS EXACTOS (L. 49,680.00)** la cual tendrá una vigencia de ocho (8) meses, contados a partir de la fecha en que se inicie el presente contrato.- **SEXTA: INCUMPLIMIENTO DEL CONTRATO:** En caso de incumplimiento comprobado por parte del **CONTRATISTA** en las clausulas convenidas y en el objeto del presente contrato, **EL INSTITUTO** hará efectiva la garantía de cumplimiento de contrato, con previa notificación a **EL CONTRATISTA**. De igual forma el Proveedor pagará la indemnización que conforme a Ley corresponda.- **SÉPTIMA: MULTAS: EL INSTITUTO** cobrará al **CONTRATISTA** una multa correspondiente al 0.036% del monto restante del contrato incumplido. **OCTAVA: CAUSAS DE RESOLUCIÓN DEL CONTRATO:** Las partes contratantes podrán invocar cualesquiera de las causales de resolución del contrato tales como: **1)** El grave o reiterado incumplimiento de las cláusulas convenidas, **2)** La falta de constitución de las garantías a cargo del **CONTRATISTA** dentro de los plazos correspondientes; **3)** La declaración de quiebra o suspensión de pagos del **CONTRATISTA,** o su comprobada insolvencia financiera; **4)** Los motivos de interés públicos o las circunstancias imprevistas calificadas como caso fortuito o fuerza mayor que surjan a la celebración del contrato, que imposibiliten o agraven desproporcionadamente su ejecución; **5)** El incumplimiento de las obligaciones de pago más allá del plazo previsto en el contrato; **6)** El mutuo acuerdo de las partes; **7)** Las demás que establezca expresamente este contrato, las especificaciones técnicas y las Leyes vigentes en la República; y, **8)** En caso de existir alguna orden de cambio y/o modificación no aprobada por la Unidad de Seguridad de la Información del IPM o alguna modificación no contemplada por el **INSTITUTO.**- **NOVENA: CESIÓN, SUB CONTRATACIÓN, TRASPASO DEL CONTRATO: EL CONTRATISTA** no podrá ceder, subcontratar o traspasar lo estipulado en el presente contrato. **DÉCIMA: SOLUCIÓN DE CONFLICTOS:** Si existiera alguna desavenencia en la interpretación y ejecución de este contrato y la misma no fuera

solucionada por el buen entendimiento extrajudicial o la conciliación, ambas partes nos sometemos a la jurisdicción y competencia del Juzgado de Letras Civil de Francisco Morazán. Para todo lo no previsto en el presente contrato, se aplicaran las disposiciones legales del ordenamiento jurídico vigente de la República de Honduras que le sean aplicables. **DÉCIMA PRIMERA: CLAUSULA DE INTEGRIDAD:** Las partes en cumplimiento a lo establecido en el Artículo 7 de la Ley de Transparencia y acceso a la información pública (LTAIP) y con la convicción de que evitando las prácticas de corrupción podremos apoyar la consolidación de una cultura de transparencia, equidad y rendición de cuentas en los procesos de contratación y adquisiciones del Estado, para así fortalecer las bases del Estado de Derecho, nos comprometemos libre y voluntariamente a: 1. Mantener el más alto nivel de conducta, ética, moral y de respeto a las Leyes de la República así como los valores de: **INTEGRIDAD, LEALTAD CONTRACTUAL, EQUIDAD, TOLERANCIA, IMPARCIALIDAD Y DISCRECIÓN CON LA INFORMACIÓN CONFIDENCIAL QUE MANEJAMOS, ABSTENIÉNDONOS DE DAR DECLARACIONES PÚBLICAS SOBRE LAS MISMAS.** 2. Asumir una estricta observancia y aplicación de los principios fundamentales bajo los cuales se rigen los procesos de contratación y adquisiciones públicas establecidos en la Ley de Contratación del Estado tales como: Transparencia, igualdad y libre competencia. 3. Que durante la ejecución del contrato ninguna persona que actué debidamente autorizada en nuestro nombre y representación y que ningún empleado o trabajador, socio o asociado autorizado o no, realizará a) **Prácticas Corruptivas:** entendiendo estas como aquellas en las que se ofrece dar, recibir o solicitar directa o indirectamente, cualquier cosa de valor para influenciar las acciones de la otra parte; b) Prácticas Colusorias: entendiendo estas como aquellas en las que denoten, surgieran o demuestren que existe un acuerdo malicioso entre dos o más partes o entre una de las partes y uno o varios terceros, realizado con la intención de alcanzar un propósito inadecuado incluyendo influenciar en forma inapropiada las acciones de la otra parte. 4. Revisar y verificar toda la información que deba ser presentada a través de terceros a la otra parte, para efectos del contrato y dejamos manifestado que durante el proceso de contratación o adquisición causa de este contrato, la información intercambiada fue debidamente revisada y verificada, por lo que ambas partes asumen y asumirán la responsabilidad por el suministro de información inconsistente, imprecisa o que no corresponda a la realidad para efectos de este contrato. 5. Mantener la debida confidencialidad sobre toda la información a la que se tenga acceso por razón del Contrato, y no proporcionarla, ni divulgarla a terceros y a su vez, abstenernos de utilizarla para fines distintos. 6. Aceptar las consecuencias a que hubiere lugar, en caso de declararse el incumplimiento de alguno de los compromisos de esta cláusula por el Tribunal competente y sin perjuicio de la responsabilidad civil o penal, en la que incurra. 7. Denunciar en forma oportuna ante las autoridades correspondientes, cualquier hecho o acto irregular cometido por nuestros empleados o trabajadores, socios o asociados del cual se tenga un indicio razonable y que pudiese ser constitutivo de responsabilidad civil y/o penal. Lo anterior se extiende al sub-contratista, con los cuales el contratista o consultor contrate así como los socios, asociados, ejecutivos y trabajadores de aquellos. El incumplimiento de cualquiera de los enunciados de esta cláusula dará lugar a: De parte del contratista o consultor: i. A la inhabilitación para contratar con el Estado, sin prejuicio de las responsabilidades que pudieren deducírsele a. La aplicación al trabajador, ejecutivo, representante, socio, asociado o apoderado que haya incumplido esta cláusula, de las sanciones o medidas disciplinarias derivadas del régimen laboral, en su caso entablar las acciones legales que correspondan. b. De parte del contratante a la eliminación definitiva del Contratista o Consultor y a los subcontratistas responsables o que pudiendo hacerlo no denunciaron la irregularidad de su Registro de proveedores y contratistas que al efecto llevare para no ser sujeto de elegibilidad futura en procesos de contratación. ii. A la aplicación del empleado o funcionario infractor de las sanciones que correspondan según Código de conducta Ética del servidor público, sin perjuicio de exigir la responsabilidad administrativa, civil y/o penal a las que hubiere lugar. **DÉCIMA SEGUNDA: RESPONSABILIDADES: El CONTRATISTA** se hace responsable por cualquier accidente de trabajo y pago de planilla de sus empleados, brindar todas las medidas de Bioseguridad exigidas por SINAGER. Además asume todas las responsabilidades legales, sociales y laborales prescritas en todas las leyes que se mantengan en

vigencia en el país y que se deriven de las relaciones obreras patronales que mantengan con todos los trabajadores que presten el servicio objeto del presente contrato de Servicios, obligaciones que correrán por cuenta de EL **CONTRATISTA.**- **DÉCIMA TERCERA:** EL **CONTRATISTA** se compromete a facilitar cualquier tipo de información a los Auditores Externos contratados por el **INSTITUTO,** referente a los montos y ejecución del presente contrato. **DÉCIMA CUARTA: VIGENCIA DEL CONTRATO:** La vigencia del presente contrato es de cinco (5) meses a partir de la orden de inicio. En fé de lo cual firmamos el presente contrato, manifestando nuestra conformidad con todas y cada una de las cláusulas, condiciones y disposiciones incluidas y nos obligamos a su fiel cumplimiento. Dado en la Ciudad de Tegucigalpa, Municipio del Distrito Central, a los doce (12) días del mes de abril del año Dos Mil Veintitrés (2023).

CORONEL RETIRADO

ALFREDO FABRICIO ERAZO PUERTO

EL INSTITUTO

INGENIERO EN SISTEMAS

JUAN CARLOS INESTROZA LOZANO

EL CONTRATISTA