1. DATOS GENERALES:

Objeto de Contratación:	Estudio Ethical Hacking
Tipo de proceso de contratación:	Consultoría
Presupuesto Referencial:	10,023.22 dólares
Área Requirente:	Departamento de Tecnología y Comunicaciones
Partida presupuestaria:	53.06.01.2023.001.002.023 - Consultoría, Asesoría e Investigación Especializada
CPC:	831410311 PRESTACION DE ASESORAMIENTO Y ASISTENCIA EN CUESTIONES RELACIONADAS CON LA GESTION DE LOS RECURSOS INFORMATICOS DE LAS SOCIEDADES O INSTITUCIONES COMO, LA CONSULTORIA EN MATERIA DE SISTEMAS DE SEGURIDAD
Vigencia dela Oferta:	120 días
Costo de los Pliegos:	50.00 dólares
Entrega de ofertas:	La oferta deberá ser enviada a través del sistema de Contratación Pública (SOCE), la misma deberá estar firmada electrónicamente. Es importante señalar que la firma manuscrita escaneada no es considerada como firma electrónica. No se tomará en cuenta si la oferta es enviada a través de correos electrónicos. Para el envío de la oferta es responsabilidad de del oferente revisar la Circular Nro. SERCOP-SERCOP-2020-0022-C, de fecha 27 de octubre de 2020, a través de la cual el SERCOP emite las directrices para el uso de firma electrónica en relación al RGLOSNCP.
Dirección apertura de ofertas:	Departamento de Tecnología y Comunicaciones

Proveedor(es) invitado(s):	

2. PRESUPUESTO REFERENCIAL

CODIGO CPC	DESCRIPCION	UNIDAD	CANTIDAD	VALOR UNITARIO	VALOR GLOBAL
831410311	Estudio Ethical Hacking	Unidad	1	10,023.22	10,023.22
	Total precio referencial sin IVA:				10,023.22

3. TERMINOS DE REFERENCIA

a) Antecedentes

El artículo 225 de la Constitución de la República, establece que las personas jurídicas creadas por acto normativo de los gobiernos autónomos descentralizados para la prestación de servicios públicos son parte del sector público.

El artículo 315 de la Constitución de la República del Ecuador, establece que el Estado constituirá empresas públicas para la gestión de sectores estratégicos, la prestación de servicios públicos, el aprovechamiento sustentable de recursos naturales o de bienes públicos y el desarrollo de otras actividades económicas.

La Ley Orgánica Empresas Públicas dispone en el Art. 11.- "El Gerente General, como responsable de la administración y gestión de la empresa pública, tendrá los siguientes deberes y atribuciones: 1. Ejercer la representación legal, judicial y extrajudicial de la empresa pública (…) 4. Administrar la empresa pública, velar por su eficiencia empresarial e informar al Directorio trimestralmente o cuando sea solicitado por éste, sobre los resultados de la gestión de aplicación de las políticas y de los resultados de los planes, proyectos y presupuestos, en ejecución o ya ejecutados. (…)".

La Ordenanza que Regula la Creación, Organización y Funcionamiento de la Empresa Pública Municipal de Aseo de Cuenca – EMAC EP, en su artículo primero dispone: "Créase la Empresa Pública Municipal de Aseo de Cuenca - "EMAC EP", como una persona jurídica de derecho público, con patrimonio propio, dotada de autonomía presupuestaria, financiera, económica, administrativa y de gestión, que opera sobre bases comerciales y cuyo objetivo es la prestación de servicios públicos de barrido, limpieza, recolección, transporte, tratamiento y disposición final de residuos sólidos no peligrosos y peligrosos, así como del mantenimiento, recuperación, readecuación y administración de áreas verdes y parques en el cantón Cuenca incluyendo el equipamiento en ellas construidas o instaladas, sus servicios complementarios, conexos y afines

que pudieren ser considerados de interés colectivo, así como otros servicios que resuelva el Directorio, los mismos que se prestarán en base a los principios de obligatoriedad, generalidad, uniformidad, eficiencia, universalidad, accesibilidad, regularidad, calidad, responsabilidad, continuidad, seguridad y precios equitativos.

(…) La Empresa tendrá su domicilio principal en la ciudad de Cuenca, Provincia del Azuay, República del Ecuador, pudiendo prestar sus servicios en el ámbito cantonal, provincial, regional, nacional o internacional, directamente o a través de la creación de empresas filiales, subsidiarias, agencias o unidades de negocio, de conformidad con la ley (…)".

Un Ethical Hacking es un método de evaluar la seguridad de un sistema o red informática simulando un ataque de un usuario malicioso, usualmente conocido como hacker. El proceso involucra un análisis activo del sistema en busca de cualquier posible vulnerabilidad que pueda resultar de una configuración inapropiada, fallo en el software o hardware, o una debilidad en el proceso operacional o contramedida técnica. Este análisis es generado desde la posición de un hacker potencial y puede involucrar la explotación real de vulnerabilidades de segundad. Todos los problemas de seguridad que sean detectados serán presentados a la EMAC EP en conjunto con una propuesta o recomendación de soluciones técnicas. La intención de una prueba de intrusión es el de determinar la posibilidad de un ataque real, la cantidad de impacto en el negocio de una explotación real si es descubierta.

b) Objetivos

Objetivo general

Identificar posibles vulnerabilidades existentes en servicios e infraestructura tecnológica, las cuales podrían llegar a ser explotadas por un intruso o usuario malicioso para obtener el control de recursos críticos y datos sensibles almacenados en los mismos.

Objetivo específico

- Realizar análisis y explotación de vulnerabilidades interno y externo a la infraestructura tecnológica de la EMAC EP.
- Realizar el análisis de ingeniería social para medir el nivel de sensibilización en seguridad de la información del personal de la EMAC EP.
- Elaborar el Plan de Remediación de las vulnerabilidades encontradas.
- Presentar y explicar los resultados del análisis realizado.

c) Alcance

Esta Consultoría permitirá realizar una evaluación de vulnerabilidades de seguridad de la información y ethical hacking a la infraestructura tecnológica de la EMAC EP, así como realizar el análisis de vulnerabilidades de código fuente, base de datos, simulación de ataques a través de ingeniería social, elaboración de informes relacionados a cada uno de los análisis y presentación del plan de remediación, sobre la infraestructura tecnológica proporcionada por la Empresa Pública Municipal de Aseo de Cuenca.

A continuación de desglosa el análisis esperado y no limitado a:

Análisis externo:

Identificación de los Objetivos:

- Recolección de direcciones Ip de los objetivos.
- Búsqueda de información relacionada con el cliente en sitios públicos.
- Búsqueda de Información en Medios Digitales e Internet.
- Enumeración subdominios y portales.

Escaneo de vulnerabilidades:

- Escaneo de vulnerabilidades con herramienta licenciada sobre servidores específicos.
- Escaneo de vulnerabilidades con herramienta open source sobre servidores específicos.
- Escaneo de vulnerabilidades con herramienta licenciada a aplicaciones web.
- Escaneo de vulnerabilidades con herramienta open source a aplicaciones web.
- Escaneo manual de vulnerabilidades en aplicaciones web.
- Escaneo manual de vulnerabilidades en servidores.
- Detección de puertos abiertos sobre equipos analizados.
- Detección de sistemas operativos.

Validación y Explotación:

- Identificación de vulnerabilidades explotables.
- Identificación de exploits acorde a las vulnerabilidades.
- Ejecución de pruebas de pentesting sobre las vulnerabilidades encontradas en servidores.
- Ejecución de pruebas de pentesting sobre las vulnerabilidades encontradas en aplicaciones web.
- Ejecución de pruebas de pentesting sobre las vulnerabilidades encontradas en servicios y puertos específicos.

Documentación

- Análisis estadístico: Porcentajes de distribución de vulnerabilidades por severidad, por dispositivo, con gráficas y tablas.
- Informe Técnico de resultados y Anexos.
- Plan de Mitigación de Vulnerabilidades a corto, mediano y largo plazo.
- Informe Ejecutivo de resultados
- Presentación de resultados.

Las pruebas de pentesting sobre el punto “validación y explotación” dependeran de los resultados obtenidos en el escaneo de vulnerabilidades, sin embargo, las pruebas de penetración que podrían llegar a ejecutarse pero no limitarse (en los casos que sean aplicables) a las siguientes:

Obtención de la información.

- Identificación del Objetivo.
- Google Hacking
- Análisis de listas negras y reputación.
- Análisis de registros DNS

- Análisis de registros externos.
- Obtención de rangos de direcciones IP.
- Escaneo y análisis de puertos.
- Escaneo y análisis de vulnerabilidades
- Análisis de direcciones IPs públicas para identificar vulnerabilidades
- Ataques de vulnerabilidades conocidas
- Ataques de autenticación
- Escalamiento de privilegios
- Suplantación de credenciales
- Usuarios o claves en aplicaciones en texto plano
- Manejo de sesiones
- Obtención de evidencias y depuración de falsos positivos.
- Pruebas de explotación avanzada.
- Ataques específicos controlados.
- Pruebas de penetración controladas.
- Pruebas de cracking.
- Ataques de inundación de tráfico, envenenamiento y spoofing.
- Inyección de código malicioso.
- Desbordamiento de buffer
- Fuerza bruta sobre el servicio de acceso remoto
- Fuerza bruta sobre el servicio de autenticación de las Aplicaciones
- Ataque de aplicaciones web
- Análisis y aprovechamiento de vulnerabilidades de los servidores, mediante el uso de programas exploit
- Análisis de la topología de los equipos de seguridad perimetral Backdoors “Puerta trasera”
- CGI Abuses. “Common Gateway Interface”
- Finger Abuses
- Análisis de Aplicación Móvil y código fuente
- FTP. “Pruebas de configuración y debilidades en versiones específicas”
- Gain a Shell Remotely “Ejecución de comandos en el servidor”
- Gain Root Remotely “Obtener cuenta administrador remotamente”
- NIS “Network Information Systems”
- Remote File Access “Posibilidad de re-escribir archivos del servidor utilizando puertos conocidos”
- Inyección SQL, XML, LDAP.
- Pruebas de acceso con credenciales débiles o por defecto.
- Usuarios y claves quemadas en la aplicación.
- Pruebas de fuerza bruta sobre portales web.
- Pruebas de Fuerza bruta sobre servicios como FTP/SSH/TELNET.
- Pruebas de Detección de Malware
- DOS y DDOS
- Sql Injection.
- Local File Inclusion y Remote File Inclusion
- CRSF y XSS

Análisis interno

Identificación de los Objetivos:

- Recolección de direcciones Ip de los objetivos.
- Identificación de esquema de red.
- Identificación de aplicaciones web a analizar.

Escaneo de vulnerabilidades:

- Escaneo de vulnerabilidades
- Detección de puertos abiertos sobre equipos analizados y sistemas operativos
- Detección de sistemas operativos.

Validación y Explotación (ETHICAL HACKING):

- Identificación de vulnerabilidades explotables
- Identificación de exploits acorde a las vulnerabilidades
- Ejecución de pruebas de pentesting sobre las vulnerabilidades encontradas
- Ejecución de pruebas de pentesting sobre las vulnerabilidades encontradas en los aplicativos web (WEB Hacking)

Documentación:

- Matriz de vulnerabilidades sobre dispositivos analizados.
- Evidencias sobre pruebas de explotación.
- Análisis estadístico: Porcentajes de distribución de vulnerabilidades por severidad, por dispositivo o VLAN, con gráficas y tablas bajo dos escenarios (Dentro de dominio/ fuera de dominio).
- Informe Técnico de resultados y Anexos.
- Plan de Mitigación de Vulnerabilidades a corto, mediano y largo plazo.
- Presentación de resultados.

Las pruebas de pentesting sobre el punto “validación y explotación” dependeran de los resultados obtenidos en el escaneo de vulnerabilidades, sin embargo, las pruebas de penetración que podrían llegar a ejecutarse pero no limitarse (en los casos que sean aplicables) a las siguientes:

- Escaneo y análisis de puertos.
- Detección y análisis de servicios activos.
- Detección remota de SO.
- Identificación de dispositivos de Red y sus configuraciones.
- Identificación de servidores y su configuración.
- Identificación y exploración de aplicaciones web.
- Generación de evidencia.
- Escalada de privilegios.
- Escaneo y análisis de vulnerabilidades
- Escaneo de vulnerabilidades de Base de Datos
- Explotación de las vulnerabilidades detectadas.
- Identificar el estado actual de los parches instalados en los sistemas operativos, servidores y base de datos
- Evaluación de las seguridades tecnológicas implementadas en el servicio de acceso a Internet
- Evaluación de configuración de seguridad establecida en la red alámbrica/inalámbrica

- Evaluación de la configuración y diseño de las conexiones VPN
- Fuerza bruta sobre el servicio de acceso remoto
- Fuerza bruta sobre el servicio de autenticación de las Aplicaciones
- Explotar vulnerabilidades de los servidores Web con el uso de programas exploit
- Ataques de denegación de servicio para la red Ethernet e inalámbrica
- Pruebas de penetración a equipos de red, equipos de seguridad sistemas operativos, aplicaciones de red y aplicaciones web de forma controlada y sin comprometer la información.
- Pruebas de cracking por fuerza bruta sobre aplicaciones de administración y acceso remoto a equipos de networking, equipos de seguridad, sistemas operativos, aplicaciones de red y aplicaciones web.
- Captura de información sensible en la red (sniffing).
- Ataques de inundación de tráfico, envenenamiento y spoofing.
- Utilización de exploits preparados y diseñados para robo de información.
- Ataques de robo de sesiones.
- Hacking de Base de Datos.
- Inyección de SQL, SSI, LDAP
- Ataques XSS y CSRF.F31
- Fuzzing de aplicativos web.
- Banner Grabbing.
- Cross-Site Request Forgery (CSRF).
- Travesía de Trayectoria (Path Traversal)
- Inyección de comandos del sistema operativo
- XSS Secuencias de Comandos entre sitios (Cross Site Scripting)
- Falsificación de petición en sitios cruzados (Cross Site Request Forgeries)
- Control de autorización erróneo sobre aplicaciones del sitio Web
- Escalamiento de privilegios.
- Suplantación de credenciales.
- Usuarios y claves quemadas en la aplicación.
- Ataques a la aplicación web con los privilegios de un usuario autorizado.
- Ataques sobre protocolos de capa 2 y capa 3
- Ataques sobre Código HTML, PHP generado por la aplicación
- Ataques sobre componentes JAVA/ActiveX , Flash y AJAX
- Ataques Command execution.
- Verificación y explotación controlada de las vulnerabilidades.

Se elaborará un plan de remediación, producto de los análisis de vulnerabilidades realizados y de los resultados efectivos de las pruebas de penetración. Este plan contemplará las acciones correctivas necesarias para solucionar en corto, mediano y largo plazo los hallazgos basados en el nivel de criticidad encontrado, estas acciones serán sustentas por estándares o mejores prácticas del sector de la seguridad informática.

Se entregará un documento formal tipo guía, sobre el correcto endurecimiento y fortalecimiento de las configuraciones de seguridad que se deben incluirse en los servidores de la institución, basados en estándares internacionales, normativa y buenas prácticas.

Se dictará una charla de concienciación a todo el personal de la institución en temas relacionados con seguridad informática, ciberataques, amenazas, fraudes informáticos en la red en otros tópicos, los cuales permitirán a la institución tomar conciencia frente a este tipo de amenazas latentes.

d) Metodología de trabajo

La metodología a aplicarse en la consultoría y presentada por la empresa oferente deberá tomar como base las buenas prácticas de ciberseguridad como son: Metodologías de ethical hacking, Implementación en normas ISO/IEC 27001/27002, OSSTMM Open Source Security Testing Methodology Manual, OWASP Open Web Application Security Project, ISSAF Information Systems Security Assessment Framework, PCI DSS Payment Card Industry Data Security Standard, Sans Institute Security Testing Best Practices, CERT Security Testing Best Practices, NIST Security & Risk Management Best Practices.

El oferente deberá detallar en su propuesta, la metodología a seguir para evaluar las vulnerabilidades y ethical hacking a la infraestructura tecnológica de la EMAC EP, la cual deberá especificar los estándares y normas internacionales y/o uso de buenas prácticas, tomando como línea base cualquiera de las mencionadas en el párrafo anterior.

La firma consultora presentará el cronograma de trabajo dentro de los 4 días posteriores a la firma del contrato, considerando los plazos establecidos en los términos de referencia. El plan y cronograma de trabajo se definirá en coordinación con el administrador del contrato.

Los cambios al cronograma de trabajo que realice el Contratista, deberá ser comunicado y justificado oportunamente al Administrador del Contrato.

En caso eventual de que la firma consultora, requiera a través de petición, accesos y conexiones especiales, estas peticiones serán revisadas por el Administrador del Contrato.

e) Información que dispone la entidad y que se pondrá a disposición del proveedor

La entrega de información, objeto de la consultoría, se realizará una vez firmado el contrato, en el que deberá incluirse un acuerdo de confidencialidad. La EMAC EP entregará al Consultor la siguiente información:

- Información a ser evaluada (direcciones IP, servicios, motores de base de datos, segmentos de red, aplicaciones, entre otra información que sea requerida por la empresa).
- Acceso al código fuente
- Usuarios para la ingeniería social.

f) Productos y servicios esperados

La consultoría para la evaluación de vulnerabilidades y ethical hacking a desarrollarse en la EMAC EP, se compone de los siguientes productos productos:

Análisis externo:

- Análisis estadístico: Porcentajes de distribución de vulnerabilidades por severidad, por dispositivo, con gráficas y tablas.
- Informe Técnico de resultados y Anexos.
- Plan de Mitigación de Vulnerabilidades a corto, mediano y largo plazo.
- Informe Ejecutivo de resultados
- Presentación de resultados.

Análisis interno:

- Matriz de vulnerabilidades sobre dispositivos analizados.
- Evidencias sobre pruebas de explotación.
- Análisis estadístico: Porcentajes de distribución de vulnerabilidades por severidad, por dispositivo o VLAN, con gráficas y tablas bajo dos escenarios (Dentro de dominio/ fuera de dominio).
- Informe Técnico de resultados y Anexos.
- Plan de Mitigación de Vulnerabilidades a corto, mediano y largo plazo.
- Presentación de resultados.

Guía sobre el correcto endurecimiento y fortalecimiento de las configuraciones de seguridad que se deben incluirse en los servidores de la institución, basados en estándares internacionales, normativa y buenas prácticas.

Registro de asistencia a la charla dictada al personal.

g) Plazo de ejecución

El presente proyecto se estima un plazo de ejecución máximo de 30 días luego de comunicada luego de la notificación de la entrega del anticipo.

h) Personal Técnico/Equipo de Trabajo/Recursos

El personal técnico que se requiere para la Consultoría es un Líder o Gerente del Proyecto y dos Consultores de Seguridad:

Nro.	Función	Nivel de estudio	Titulación Académica	Cantidad
1	Líder o Gerente del Proyecto	Tercer nivel con título	Ingeniería Informática, Sistemas, electrónica, telecomunicaciones. Certificación en Gestión de Proyectos.	1
2	Consultor de Seguridad	Tercer nivel con título	Ingeniería Informática, Sistemas, electrónica, telecomunicaciones. Certificación en al menos 2 de los siguientes temas: CISSP, CEH, OSCP, ISO 27001, ISO 27005	2

El personal mínimo que se presente para ser líder o gerente de proyecto no podrá participar como consultor o viceversa.

Se verificará la titulación académica a través de la página web de la SENESCYT y si el o los consultores son extranjeros y sus títulos no se encuentran registrados en el Ecuador, deberán presentar el título profesional conferido por la entidad de educación superior del extranjero, conforme lo establece el artículo 38 de la LOSNCP.

Se deberá presentar copia del documento que acredita la certificación solicitada, o el link que permita verificar la validez de la certificación.

Equipos de trabajo

Nro.	Descripción del equipo	Nro. de unidades	Características
1	Equipos de Computación	3	Computador portátil, asignado a cada participante.
2	Software	1	El consultor deberá acreditar que dispone de herramientas para Análisis de vulnerabilidades.

i) Formas y condiciones de pago

50 % como anticipo y 50 % contra la entrega y aceptación de los productos por parte del Administrador del Contrato.

4. OBLIGACIONES DE LAS PARTES

Obligaciones del Contratista:

Firmar el Acuerdo de Confidencialidad y no Divulgación de la Información proporcionado por la EMAC EP.

Entregar a satisfacción de la EMAC EP, los entregables del presente documento.

Obligaciones de la Contratante:

a) Dar solución a las peticiones y problemas que se presentaren en la ejecución del contrato, en un plazo máximo de 5 días contados a partir de la petición escrita formulada por el contratista, y aceptados por el Administrador de Contrato.
b) Brindar todas las facilidades para que el contratista cumpla a entera satisfacción con el objeto de la contratación.
c) Realizar los pagos respectivos, previo la presentación de los documentos habilitantes correspondiente.
d) Suscribir el (las) acta(s) entrega recepción y realizar el respectivo Informe de satisfacción.
e) La EMAC EP nombrará un administrador del contrato que deberá mantener una comunicación constante con el contratista y la Jefatura de Tecnología y Comunicaciones de la EMAC EP.
f) Podrá solicitar el movimiento y reconfiguración de equipos en el caso de traslado de oficinas a una nueva ubicación geográfica, sin que esto represente un costo adicional al presente servicio.
g) La EMAC EP otorgará al contratista adjudicado, un espacio físico para el almacenaje de suministros y repuestos.
h) Realizar el trámite para la suscripción de contrato complementario, en el caso de requerirlo con las justificaciones correspondientes en un término de 15 días.

5. MULTAS

Se aplicará una multa del uno por mil (1X1.000) por cada día de retrazo en la ejecución de las obligaciones contractuales. Las multas se calcularán sobre el porcentaje de las obligaciones que se encuentran pendientes de ejecutarse conforme lo establecido.

La CONTRATANTE queda autorizada por el CONSULTOR para que haga efectiva la multa impuesta, de los valores que por este contrato le corresponde recibir al mismo, sin requisito o trámite previo alguno.

Las multas causadas no serán revisadas ni devueltas por ningún concepto al CONSULTOR.

6. REAJUSTE DE PRECIOS

La EMAC EP, no reconocerá reajuste de precios, por lo que el consultor renuncia expresamente a solicitar el mismo.

7. GARANTÍAS

En forma previa a la suscripción de los contratos derivados del presente procedimiento, se deberán presentar las garantías que fueren aplicables de acuerdo a lo previsto en los artículos 74, 75 y 76 de la LOSNCP, en cualquiera de las formas contempladas en el artículo 73 ibídem.

Garantía de fiel cumplimiento del contrato: Se rendirá por un valor igual al cinco (5%) del monto total del mismo en una de las formas establecidas en el artículo 73 de la LOSNCP, la que deberá ser presentada previo a la suscripción del contrato. No se exigirá en los contratos cuya cuantía sea menor a multiplicar el coeficiente 0.000002 por el Presupuesto Inicial del Estado del correspondiente ejercicio económico.

Garantía de buen uso del anticipo: Si por la forma de pago establecida en el contrato, la Entidad Contratante debiera otorgar anticipos de cualquier naturaleza, sea en dinero, giros a la vista u otra forma de pago, el contratista para recibir el anticipo, deberá rendir previamente garantías por igual valor del anticipo, que se reducirán en la proporción que se vaya amortizando aquél o se reciban provisionalmente las obras, bienes o servicios. Las cartas de crédito no se considerarán anticipo si su pago está condicionado a la entrega -recepción de los bienes u obras materia del contrato.

El monto del anticipo lo regulará la Entidad Contratante en consideración de la naturaleza de la contratación.

Garantía Técnica: Cuando fuere del caso, las garantías técnicas de los bienes materia del contrato que deben ser entregadas por el contratista, cumplirán las condiciones establecidas en el artículo 76 de la LOSNCP. En caso contrario, el adjudicatario deberá entregar una de las garantías señaladas en el artículo 73 de la LOSNCP por el valor total de los bienes.

Los términos de la garantía técnica solicitada deberán observar lo establecido en las Resoluciones emitidas por el Servicio Nacional de Contratación Pública en lo que respecta a la aplicación de la vigencia tecnológica, en los casos pertinentes.

La entidad contratante no podrá exigir garantía adicional alguna a las previstas en la Ley Orgánica del Sistema Nacional de Contratación Pública. Sin embargo, podrá requerir los seguros o condiciones de protección para las personas que presten sus servicios en la provisión, entrega y colocación de bienes y en cualquier tipo de prestación de servicios, que considere pertinentes.

Las garantías se devolverán conforme lo previsto en el Artículo 77 de la LOSNCP y 263 del RGLOSNCP.

8. INDICES FINANCIEROS

Los índices financieros constituirán información de referencia respecto de los participantes en el procedimiento y en tal medida, su análisis se registrará conforme el detalle a continuación:

Índice	Indicador solicitado	Observaciones
Solvencia*	mayor o igual a 1,0	
Endeudamiento*	menor a 1,5	
Otro índice resuelto por la entidad contratante *		

Los factores para su cálculo estarán respaldados en la correspondiente declaración de impuesto a la renta del ejercicio fiscal anterior a la presentación de la oferta y/o los balances presentados al órgano de control respectivo, para los obligados a llevar contabilidad.

9. REQUISITOS MÍNIMOS

9.1 Equipo mínimo

Nro.	Descripción del equipo	Nro. de unidades	Características
1	Equipos de Computación	3	Computador portátil, asignado a cada participante.
2	Software	1	El consultor deberá acreditar que dispone de herramientas para Análisis de vulnerabilidades.

9.2 Personal Técnico Mínimo

Nro.	Función	Nivel de estudio	Titulación Académica	Cantidad
1	Líder o Gerente del Proyecto	Tercer nivel con título	Ingeniería Informática, Sistemas, electrónica, telecomunicaciones. Certificación en Gestión de Proyectos.	1
2	Consultor de Seguridad	Tercer nivel con título	Ingeniería Informática, Sistemas, electrónica, telecomunicaciones. Certificación en al menos 2 de los siguientes temas: CISSP, CEH, OSCP, ISO 27001, ISO 27005	2

9.3 Experiencia mínima del Personal Técnico

Nro.	Función	Descripción	Tiempo mínimo	Fuente o medio de verificación
1	Líder o Gerente del Proyecto	Cinco (5) proyectos relacionados con la seguridad de la información, evaluación de vulnerabilidades, pruebas de penetración, ethical hacking o análisis de riesgos tecnológicos	Dentro de los últimos 5 años	Certificados y/o acta(s) entrega-recepción, que avalen la experiencia profesional
2	Consultor de Seguridad	Cinco (5) proyectos relacionados con la seguridad de la información, evaluación de vulnerabilidades, pruebas de penetración, ethical hacking o análisis de riesgos tecnológicos	Dentro de los últimos 5 años	Certificados y/o acta(s) entrega-recepción, que avalen la experiencia profesional

9.4 Experiencia General y Específica Mínima

Experiencia General

Nro.	Tipo de experiencia	Descripción	Temporalidad	Número de proyectos	Monto mínimo
1	General	Demostrará experiencia general en Consultoría en procesos de implementación, mantenimiento y soporte de productos y servicios en Seguridad de la información y ciberseguridad	5 años	Al menos 1	2,505.81

Nota: La experiencia se comprobará a través de presentación de actas de entrega recepción provisional o definitiva, contratos, facturas o certificaciones debidamente legalizadas entre el oferente y personas naturales o jurídicas.

Experiencia específica

Nro.	Tipo de experiencia	Descripción	Temporalidad	Número de proyectos	Monto mínimo
1	Específica	Demostrara experiencia específica en procesos de consultorías de evaluación de	5 años	Al menos 1	1,202.79

		vulnerabilidades y ethical hacking.			

9.5 Otros Parámetros resueltos por la entidad contratante

No aplica

CARTA COMPROMISO: Respecto al equipo en el cual aplica vigencia tecnológica, cumplir con lo dispuesto en Artículo 127 de la Resolución N° RE-SERCOP-2016-0000072, en su numeral 3: "La aceptación expresa del oferente respecto de permitir la inspección de los bienes de que trata este artículo, por parte del administrador del contrato designado por la entidad contratante, en cualquier tiempo durante la vigencia del contrato, para efectos de evaluar el cumplimiento de las condiciones de vigencia tecnológica ofertadas, contractualmente establecidas, incluyendo la exigencia de reemplazo del equipo, de ser necesario para cumplir con el principio de vigencia tecnológica", para la cual deberá presentar en su oferta técnica una Carta de compromiso.

10. SISTEMA DE CALIFICACIÓN DE LA PROPUESTA

10.1 Verificación de cumplimiento de integridad y requisitos mínimos de la oferta

Parámetro	Cumple	No Cumple	Observaciones
Integridad de la Oferta			
Equipo mínimo			
Personal técnico mínimo			
Experiencia mínima del personal técnico			
Experiencia general y específica mínima			
Especificaciones técnicas / Términos de referencia			
Patrimonio (Personas Jurídicas) *			
Porcentaje de Valor Agregado Ecuatoriano Mínimo (VAE)			
Otros parámetros resueltos por la entidad			

10.2 Evaluación por Puntaje:

No aplica

11. INFORME DE PERTINENCIA

No aplica

FECHA: 26 de julio de 2023

FIRMA	FIRMA	FIRMA
Firmado electrónicamente por: JUAN FERNANDO VICUNA POZO	Firmado electrónicamente por: JOAO DARVIN PARDO RODRIGUEZ	Firmado electrónicamente por: JUAN FERNANDO VICUNA POZO
Realizado por: Juan Fernando Vicuña Pozo Jefe de Tecnología y Comunicaciones Número de Certificación SERCOP : X1U59bRb9L	**Revisado por**: Joao Darwin Pardo Rodríguez Administrador de Infraestructura Número de Certificación SERCOP : POvQ1gU0fT	**Aprobado por**: Juan Fernando Vicuña Pozo Jefe de Tecnología y Comunicaciones Número de Certificación SERCOP : X1U59bRb9L