PARQUES NACIONALES
NATURALES DE COLOMBIA

ANEXO 1.

FICHA CONDICIONES Y ESPECIFICACIONES TÉCNICAS ESENCIALES

ESPECIFICACIONES TÉCNICAS MÍNIMAS EXIGIDAS
RENOVACIÓN LICENCIAS SOLUCION DE ANALISIS DE VULNERABILIDADES

Las siguientes son las especificaciones técnicas mínimas que deben cumplir las propuestas para la *"NC03-P3299063-008 - Adquisición de la renovación de solución de análisis de vulnerabilidades para PNNC, en el marco del fortalecimiento de la capacidad institucional"*

1. OBJETO
"NC03-P3299063-008 - Adquisición de la renovación de solución de análisis de vulnerabilidades para PNNC, en el marco del fortalecimiento de la capacidad institucional"

2. ALCANCE
Renovación y adquisición de una solución de la solución de análisis de vulnerabilidades para mínimo 128 direcciones IP y mínimo 128 aplicaciones WEB en modalidad de suscripción a dos (2) años con soporte y acompañamiento por parte del Partner y del fabricante.

3. DESCRIPCIÓN TÉCNICA DEL BIEN
Los siguientes son los requerimientos técnicos mínimos exigidos, que el proponente debe satisfacer para el cumplimiento del objeto contractual, por lo tanto, se relacionan los elementos proyectados a adquirir:

<table>
<tr><td>4</td><td>ESPECIFICACIONES TÉCNICAS DE LOS PRODUCTOS

Los siguientes son los requerimientos técnicos mínimos exigidos, que el proponente debe satisfacer para el cumplimiento del objeto contractual, por lo tanto, se relacionan los elementos proyectados a adquirir:

<table>
<tr><th>Item</th><th>Descripción</th><th>Cant</th></tr>
<tr><td>1</td><td>Renovación de la solución de análisis de vulnerabilidades por 2 años para Parques Nacionales Naturales de Colombia</td><td>256</td></tr>
<tr><td>2</td><td>Servicios de Soporte 24x7 2 Años</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>4.1</td><td>Especificaciones Generales</td></tr>
<tr><td>4.1.1</td><td>La solución tecnológica deberá traducir la información obtenida por medio de evaluación de vulnerabilidades, evaluación de líneas base de configuración y evaluación de cumplimiento</td></tr>
</table>

	regulatorio sobre todos los activos TI y aplicaciones web, con el fin de priorizar acciones y comunicar el riesgo cibernético.
4.1.2	La solución ofertada deberá soportar un licenciamiento flexible, el cual permita asignar el licenciamiento de acuerdo con las necesidades de evaluación y modificar dicha asignación para hacer evaluación de cumplimiento a recursos en la nube, contenedores o sistemas de identidad en caso de ser necesario.
4.1.3	La solución ofertada deberá ser de licencia exclusiva de la Entidad, no se aceptarán soluciones de uso compartido, licenciamiento open source y reúso de licenciamiento
4.1.4	La solución ofertada deberá proveer una visibilidad completa sobre toda la superficie de ataque, sobre un único portal que proporcione una vista unificada.
4.1.5	La solución ofertada permitirá anticipar las amenazas y priorizar los esfuerzos de mitigación con el fin de evitar ataques
4.1.6	La solución ofertada permitirá comunicar el riesgo cibernético, con la finalidad de tomar mejores decisiones.
4.1.7	La solución ofertada deberá contar con una vista de exposición, la cual permita enfocar los esfuerzos de seguridad brindando información clara y concisa de la exposición con respecto a la seguridad de la Entidad. De la misma forma deberá proporcionar una puntuación global unificada de la exposición obtenida a partir de diferentes fuentes de datos
4.1.8	La solución ofertada deberá contar con un Inventario de Activos centralizado, con el objetivo de proporcionar una visibilidad completa hacia todos los activos independientemente de la fuente de datos (Activos TI y Aplicaciones Web), permitiendo la agrupación por medio de etiquetas.
4.1.9	La solución ofertada deberá realizar una gestión de vulnerabilidades basadas en el riesgo, permitiendo una priorización dinámica de las tareas de remediación en función de las amenazas
4.1.10	La solución ofertada deberá realizar una evaluación de vulnerabilidades en entornos web de manera automatizada de manera completa y precisa.
4.1.11	La solución ofertada permitirá proveer métricas de evaluación de los programas de evaluación y remediación de la Entidad.
4.1.12	La solución ofertada permitirá realizar una evaluación de la exposición de manera comparativa entre unidades de negocio o ubicaciones a nivel interno de la entidad; de la misma forma con competidores de la industria de manera externa. Con el fin de obtener información que permitan una toma de decisiones certeras.
4.1.13	La solución ofertada deberá soportar funcionalidades de seguridad de doble factor de autenticación.
4.1.14	La solución ofertada deberá ser provista por un fabricante en el cuadrante de lideres de Gartner o Forrester, en su última evaluación para tecnologías de Gestión de Riesgo de Vulnerabilidades (Vulnerability Risk Management).
4.1.15	Con fin de garantizar el cumplimiento de los requisitos plasmados en el presente documento, el oferente deberá entregar junto con la oferta, los datahseet u hojas de datos y/o manuales de usuario que avalen el cumplimiento técnico de la solución ofertada. Se deberá presentar certificación del fabricante indicando productos y cantidades ofertadas.
4.1.16	Se deberá brindar soporte y mantenimiento directo con fábrica en la modalidad 7 x 24x365, conforme a la constancia de compromiso del servicio de soporte. El soporte requerido para la solución ofertada deberá ser provisto por el proponente durante el tiempo de garantía ofrecido. El proponente deberá atender y resolver cualquier problema técnico de la solución, en un esquema de atención 7 x 24 X 365 (telefónico, e-mail, acceso remoto en caso de que la

	ENTIDAD así lo requiera), este soporte deberá ser suministrado por personal especializado en la solución ofertada. La atención de un incidente debe ser máximo dentro 4 horas siguientes al reporte, y el tiempo que tomará la solución definitiva debe ser reportado por el fabricante a la entidad dentro de los siguientes 7 días calendario, siempre y cuando el incidente haya sido causado exclusivamente por el producto. El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico y sesiones remotas en horario Hábil y No Hábil. Para ello debe contar con un centro de servicio que cumpla con mínimo: * Software de Mesa de Servicio, donde se puedan registrar casos o incidentes de forma web, correo o teléfono. * Nivel de soporte 1 para atención remota, y 2 para soporte de especialista y escalamiento a fábrica. Al finalizar cada atención correctiva el proponente generará un informe de servicio en la que constará el resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones, así como las evidencias de estas actividades. De igual forma quedará constancia en la misma acta o informe de servicio si hubo cambio de software y/o en alguna configuración.
4.1.17	El fabricante debe permitir la apertura de casos por medio del su portal de contacto, chat o vía telefónica.
4.1.18	El soporte debe incluir acceso directo a ingenieros especializados de segundo nivel (Tier II).
4.1.19	El fabricante deberá contar con un equipo de Customer Success Management (CSM) en español.
4.1.20	La solución ofertada deberá proveerse como servicio en la nube
4.1.21	La solución ofertada deberá ser totalmente implementada y configurada por el proponente, de acuerdo con las mejores prácticas del fabricante. Y complementada con los servicios de QuickStart del fabricante para garantizar un adecuado despliegue.
4.1.22	Se deberá considerar capacitación directa de fabricante a nivel de la solución ofertada como mínimo para 1 integrantes del equipo de seguridad de la entidad en la solución de Gestión de Vulnerabilidades
4.2	**Especificaciones Gestión de Vulnerabilidades**
4.2.1	La solución ofertada deberá detectar, evaluar y priorizar las vulnerabilidades de los activos TI de la Entidad y hacer parte de una plataforma de gestión de ciberexposición.
4.2.2	La solución ofertada deberá estar en la capacidad de cubrir más de 82.000 CVEs IDs y 30.000 Bugtraq IDs, con una baja tasa de falsos positivos.
4.2.3	La solución ofertada podrá gestionar vulnerabilidades de sistemas operativos, dispositivos de red, dispositivos de seguridad, firewalls de siguiente generación, hipervisores, bases de datos, servidores Web e infraestructuras esenciales y las infracciones de cumplimiento.
4.2.4	La solución ofertada deberá proporcionar una consola de gestión en la nube para la gestión de la información de seguridad.
4.2.5	La solución ofertada deberá poder ejecutar descubrimiento de activos y vulnerabilidades a través de: • Monitoreo pasivo mediante el análisis de red a través de un puerto espejo para el descubrimiento de activos, incluyendo el descubrimiento pasivo de objetivos utilizando IPv6. Dicha tecnología deberá estar patentada. • Sensores activos para el descubrimiento de activos y análisis de vulnerabilidades incluyendo el uso de IPv6. Estos sensores se pueden desplegar en forma de escáneres o agentes.

4.2.6	La solución ofertada deberá hacer uso de sensores los cuales podrán desplegarse en una variedad de plataformas, incluyendo: Windows Workstations y Servers, Linux, Mac OS ya sea en dispositivos virtuales o físicos.
4.2.7	La solución ofertada deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación que denote la urgencia de atención a una vulnerabilidad. Dicha calificación deberá ser obtenida a partir de los siguientes factores: • La priorización deberá correlacionar información de vulnerabilidades con bases de inteligencia de amenazas para determinar la probabilidad de explotación. • El modelo de priorización deberá ser capaz de predecir si una vulnerabilidad tiene posibilidades de explotación en el futuro cercano. • La priorización deberá considerar elementos de evaluación diversos, como: edad de la vulnerabilidad, madurez del código de explotación, intensidad y fuentes de las amenazas, número de días desde que se conoció una actividad de amenaza sobre la vulnerabilidad.
4.2.8	La solución ofertada deberá poder desplegar el número de escáneres, monitores de red y agentes de escaneo donde sean necesarios sin que esto represente un incremento en costo.
4.2.9	La solución ofertada deberá poder equilibrar cargas a través de múltiples escáneres de forma dinámica con base en la disponibilidad de cada escáner desplegado.
4.2.10	La solución ofertada deberá proveer una vista de soluciones que permitan enfocar en las secciones más importantes primero. Dicha vista deberá proveer los siguientes datos: • Descripción de la solución. • Número de dispositivos asociados a la solución. • Número de instancias de vulnerabilidades asociadas a la solución. • La calificación dinámica de probabilidad de explotación más alta para las vulnerabilidades asociadas a la solución.
4.2.11	La solución ofertada deberá incluir la posibilidad de programar ventanas de escaneo.
4.2.12	La solución ofertada deberá etiquetar los activos por grupos en función de las necesidades de la organización con la finalidad de categorizar los resultados y asignar las tareas correspondientes.
4.2.14	La solución ofertada deberá contar con un esquema de perfiles de usuarios basados en roles y garantizar los niveles adecuados de acceso a la plataforma.
4.2.15	La solución ofertada deberá permitir una evaluación de vulnerabilidades y/o postura de seguridad de manera autenticada, por de los siguientes sets de credenciales y sin limitarse a Windows, SSH y SNMPv3.
4.2.16	La solución ofertada deberá contar con un módulo que permita la creación de filtros para mejorar las búsquedas. Estos filtros deberán poder ser por lo menos: protocolo, IP, activo, identificador de la vulnerabilidad, identificador CVE, CVSS, vulnerabilidades por su puntaje dinámico, explotabilidad, severidad.
4.2.17	La solución ofertada deberá permitir la clasificación de activos identificados de manera manual o dinámica, con base en diferentes atributos encontrados en el análisis con base en etiquetas o en grupos de trabajo, para poder usarse en escaneos posteriores.
4.2.18	La solución ofertada deberá proporcionar información de capacidad de explotación contra las plataformas de validación como Metasploit, CoreImpact y Canvas.
4.2.19	La solución ofertada deberá ejecutar escaneos de auditoría de cumplimiento por medio de plantillas incluídas por defecto al menos para los siguientes tipos de sistemas: Adtran AOS, Alcatel TiMOS, Amazon AWS, Google GCP, Arista EOS, Blue Coat Proxy SG, Brocade Fabric OS, Check Point GAiA, Cisco ACI, Cisco Firepower, Cisco IOS, Citrix XenServer, Database, Dell Force10 FTOS, Extreme XOS, F5, FireEye, Fortigate Forti OS, HP Procurve, Huawei VRP, IBM iSeries, Juniper Junos, Microsoft Azure, Mobile Device Manager, Mongo DB, NetApp API, Office

	365, OpenStack, NetApp Data ONTAP, PAN OS, Rackspace, RHEV, Salesforce.com, SonicWall SonicOS, Unix, VMWare vCenter/vSphere, Watchguard, Windows, ZTE Rosng
4.2.20	La solución ofertada deberá proporcionar por defecto plantillas de auditoria basadas en la política de cumplimiento de auditorías de CIS.
4.2.21	La solución ofertada deberá tener la capacidad de integrarse con sistemas tipo SIEM para incrementar la capacidad de visibilidad de amenazas de la entidad, así como de respuesta a vulnerabilidades. Por defecto debe tener la capacidad de integrarse al menos con las siguientes soluciones: Chronicle, IBM Qradar, LogRhytm, Splunk, Stellar Cyber, Sumo Logic.
4.2.22	La solución ofertada deberá tener la capacidad de integrarse con soluciones tipo Privileged Access Management (PAM), pudiendo hacerlo de forma nativa al menos con los siguientes fabricantes: Arcon, Beyond Trust, Centrify, Cyber Ark, Hashi Corp, Thycotic
4.2.23	La solución ofertada deberá proporcionar una integración con los sistemas de administración de parches, auditoría e informes de diferencias en los parches contra equipos valorados. Por lo menos se deben soportar: Microsoft WSUS/SCCM, Red Hat Satellite, HCL BigFix, Symantec Altiris, Dell KACE K1000.
4.2.24	La solución ofertada deberá ser PCI Certified
4.3	**Especificaciones Gestión de Vulnerabilidades en Aplicaciones WEB**
4.3.1	La solución ofertada deberá detectar, evaluar y priorizar las vulnerabilidades de las aplicaciones web de la Entidad; provista por el mismo fabricante de la solución de Gestión de Vulnerabilidades y hacer parte de una plataforma de gestión de ciberexposición.
4.3.2	La solución ofertada deberá poder escanear aplicaciones modernas desarrolladas en frameworks JavaScript, AJAX, HTML5 and Single Page Applications.
4.3.3	La solución ofertada permitirá observar las vulnerabilidades a lo largo del tiempo, según su nivel de riesgo, clasificación en OWASP Top 10, de la misma forma que sus descripciones e instrucciones de remediación.
4.3.4	La solución ofertada deberá ser tipo SaaS, de la misma forma tendrá capacidad para ser desplegada como un contenedor de Docker, permitiendo el escaneo de sitios públicos y privados.
4.3.5	La solución ofertada permitirá realizar escaneos sin degradación de performance en el sitio, por medio de escaneos seguros, permitiendo definir sitios que no deben ser escaneados a partir de la URL, o extensiones de archivos
4.3.6	La solución ofertada deberá contar con dos escaneos predefinidos que permitan detectar rápidamente problemas de ciberhigiene: - SSL/TLS Scan - Config Audit Scan
4.3.7	La solución ofertada deberá permitir el escaneo de terceros y componentes open source como CMS, sitios web y motores de lenguaje.
4.3.8	La solución ofertada deberá soportar escaneos con autenticación avanzada como: • HTTP Server Authentication • Web Application Authentication (Login Form, Cookie Authentication, Selenium Authentication, API Key, Bearer Authentication) • Client Certificate Authentication
4.3.9	La solución ofertada deberá contar con las siguientes plantillas de escaneo: • API • Config Audit • log4Shell • Overview • PCI • Quick Scan

	• Scan • SSL/TLS
4.3.10	La solución ofertada permitirá conocer el estado y progreso de una tarea de escaneo; de la misma forma generar tareas de escaneo programadas y envío de resultados por medio de correo electrónico.
4.3.11	La solución ofertada deberá contar con la capacidad de gestionar los hallazgos, donde se puedan observar todas las vulnerabilidades descubiertas en la infraestructura.
4.3.12	La solución ofertada deberá permitir la priorización de vulnerabilidades basada en una calificación dinámica de probabilidad de explotación que denote la urgencia de atención a una vulnerabilidad.
4.4	**RECURSO HUMANO**
4.4.1	Para garantizar la ejecución del proyecto el proponente deberá aportar dentro de los tres (3) días hábiles siguientes a la fecha de adjudicación del contrato suministrar, las hojas de vida de los ingenieros que realizarán la coordinación del proyecto, implementación y soporte postventa los cuales deberán cumplir con los siguientes perfiles: **Perfil Gerente de Proyecto** Profesional que servirá de enlace entre el supervisor del contrato y el contratista y que se encargará de velar por el adecuado cumplimiento del servicio mediante las reuniones programadas y las veces que se requiera con dedicación parcial o por demanda según los requerimientos de la ficha técnica. **Estudios y Formación**: Profesional en Ingeniería de Sistemas electrónica o afines con Especialización en Gerencia de Proyectos y/o Gerencia y Tecnologías de la Información y/o Gerencia en Informática y/o afines. El profesional debe contar con Certificado de aprobación ITIL V4 Experiencia mínima de dos (2) años en Gerencia de Proyectos o gerencia de tecnología o de seguridad de la información Tarjeta Profesional Vigente **NOTA:** -El oferente que resulte adjudicado deberá remitir en el término establecido las hojas de vida del personal que asignará al proyecto. -La hoja de vida deberá contar con los siguientes anexos/soportes: diploma o acta de grado de estudios y/o formación, documento de identidad, tarjeta profesional, experiencia profesional (Adjuntar certificaciones laborales NO COPIA DE CONTRATOS), certificado de vigencia y antecedentes disciplinarios expedido por la autoridad competente a su carrera.

5. Obligaciones Generales del Contratista.

1. Conocer y acatar las políticas de seguridad de la información de la entidad, suministradas por el supervisor.

2. Garantizar la oportuna y eficaz prestación del objeto contratado, respondiendo por la calidad de los bienes suministrados y con las características requeridas.
3. Mantener indemne a la entidad por las reclamaciones que se deriven con ocasión a la ejecución contractual.
4. Acatar y cumplir las instrucciones que el Supervisor le imparta en relación con el objeto contractual.
5. Presentar factura electrónica para el pago de los bienes y servicios contratados, validada previamente por la DIAN en caso de estar obligado a ello, conforme a las disposiciones señaladas en el Decreto 358 del 5 de marzo de 2020 en concordancia con la Resolución No. 000042 del 5 de mayo de 2020, y demás normas que lo modifiquen o adicionen.
6. Realizar los aportes al Sistema Integral de Seguridad Social en Salud y Pensiones de conformidad con el artículo 50 de la Ley 789 de 2002, Ley 797 de 2003, artículo 23 de la Ley 1150 de 2007 y demás normas que la complementen, sustituyan o modifiquen; en todos los casos si hubiere lugar a ello. El Contratista deberá presentar al Supervisor del contrato el pago correspondiente a los aportes de Salud y Pensión, la cual deberá adjuntarse en la plataforma transaccional SECOP II con el fin de efectuar el pago correspondiente.
7. Adicionar o prorrogar las garantías constituidas cuando la entidad lo requiera.
8. Asistir a las reuniones que sean convocadas por el Supervisor del contrato, para revisar el estado de ejecución de este, el cumplimiento de las obligaciones a cargo del contratista o cualquier aspecto técnico referente al mismo.
9. Mantener fijos los precios de los bienes ofrecidos durante la ejecución del contrato.
10. Cumplir las demás obligaciones que se deriven de los presentes estudios previos y de la naturaleza del contrato

6. Obligaciones Específicas del Contratista

1. Entregar el licenciamiento correspondiente a la renovación con la documentación correspondiente
2. Cumplir con las especificaciones establecidas en el anexo técnico
3. Determinar con el equipo técnico de la entidad las sesiones de capacitación sobre la herramienta.
4. Informar los canales de comunicación dispuestos para la prestación del soporte sobre la herramienta.
5. Disponer del personal solicitado con los perfiles y capacidades establecidos en el anexo técnico.
6. Instalar en la calle 74 No. 11 – 81 piso 1 de la ciudad de Bogotá, las nuevas actualizaciones de firmware que sean liberadas por el fabricante.
7. Aportar dentro de los tres (3) días hábiles siguientes a la fecha de inicio del contrato los documentos soporte del personal exigido como equipo de trabajo mínimo, requerido en el anexo No. 1 "ESPECIFICACIONES TÉCNICAS", para valoración del supervisor del contrato.
8. Efectuar el afinamiento de la solución, asumiendo plenamente la responsabilidad, por lo que Parques Nacionales Naturales de Colombia no asumirá ninguna responsabilidad ni costos adicionales por cualquier daño, desperfecto o evento que, por efecto de los procedimientos, maniobras, configuración o instalaciones, llegaren a afectar su adecuada puesta en normal funcionamiento.
9. Responder sin perjuicio de la garantía, por la calidad del licenciamiento a renovar.

7. REQUISITOS TÉCNICOS HABILITANTES: Ver numeral 5.1.3 del Estudio Previo

Proyectó: Fernando Bolívar Buitrago – Contratista GTIC