ANEXO No. 1

ESPECIFICACIONES TÉCNICAS.

OBJETO:

Adquirir una solución tecnológica que comprenda la suscripción de licenciamiento, implementación, configuración y puesta en marcha de las herramientas de ciberseguridad que contribuyan a mantener la integridad, confidencialidad y disponibilidad de los servicios de Información para la Compra Pública.

ALCANCE:

Adquirir una solución tecnológica[1] que comprenda la suscripción de licenciamiento a doce (12) meses, incluido el servicio de implementación, configuración y puesta en marcha de las herramientas de ciberseguridad, teniendo en cuenta que actualmente la ANCP-CCE no cuenta con profesional idóneo para la realización de dichas actividades. De igual forma, se requiere que la solución se encuentre 100 % en la nube, permitiendo la administración desde una única consola, evitando reprocesos y carga operativa al centralizar la configuración de todas las políticas, y contando con Post Office Protocol (PoP) para el procesamiento de tráfico local con latencia. Las suscripciones deben estar a nombre de la ANCP-CCE garantizando la compatibilidad, actualizaciones y renovaciones que tengan lugar, esto con la finalidad de contar con una solución acorde con la necesidad de la Entidad para análisis de brechas de seguridad y la capacidad de realizar el escaneo sin limitaciones a nivel de direcciones IP, aplicaciones web, usuarios y dispositivos de la entidad.

Obligaciones especificaciones técnicas del bien y del servicio:

Para el desarrollo del objeto contractual, el contratista se compromete a cumplir con las siguientes obligaciones específicas:

1. Cumplir a cabalidad con el cronograma de actividades, el cual debe ser previamente aprobado por el supervisor del contrato.
2. Cumplir con el total de especificaciones técnicas descritas en el Anexo No.1
3. Entregar el total de herramientas con su respectivo licenciamiento, debidamente instalados, configurados, en funcionamiento e integrados con la infraestructura tecnológica y con las plataformas de la ANCP-CCE.

El licenciamiento a entregar es el siguiente:

4. La solución integral de Ciber-Seguridad y los licenciamientos del sistema de gestión ofertados deben contar con licenciamiento de un (1) año e incluir la última versión estable que este en el mercado, este requerimiento debe ser certificado por el fabricante.
5. Entregar una garantía directa por el fabricante por la vigencia de un (1 año), contado a partir del recibo a satisfacción por parte del supervisor del contrato, por concepto de defectos de fabricación.
6. Contar con el profesional idóneo y especializado para la realización de actividades de instalación, configuración, integración con la infraestructura tecnológica de la ANCP-CCE y puesta en marcha.
7. Entregar una garantía comercial directa con el contratista por la vigencia de un (1 año), contado a partir del recibo a satisfacción por parte del supervisor del contrato, el cual deberá incluir soporte técnico y mantenimiento, en el caso que se requiera. El soporte técnico 7X24 se deberá realizar por medio de línea de contacto telefónico, correo electrónico y deberá tener una herramienta de gestión de tickets con un Service Level Agreement (SLA).
8. Realizar las actualizaciones de software por la vigencia de la renovación, a versiones mayores estables (upgrades) y mejoras (updates).
9. Garantizar que la solución integral de Ciber-Seguridad, permita proteger los servidores que componen la infraestructura de los sitios y aplicaciones WEB de la entidad, que se encuentran distribuidos en ambientes on premise y cloud.
10. Realizar la transferencia de conocimiento sobre el manejo de las herramientas y documentación asociada a mínimo tres (3) funcionarios de la Entidad, los cuales deben ser designados por el supervisor del contrato

REQUERIMIENTOS TÉCNICOS ADICIONALES:

- Garantizar que la solución integral de Ciber-Seguridad, permita proteger los servidores que componen la infraestructura de los sitios y aplicaciones WEB de la entidad, que se encuentran distribuidos en ambientes on premise y cloud.
- Las vulnerabilidades, intrusiones, amenazas, perdida de información recién detectadas se deberán verificar para validar su autenticidad, y determinar cuáles se confirman como reales y no como falsos positivos.
- Contar con sistema multiusuario para la administración de derechos de acceso según tipos de usuarios, roles y privilegios
- Entregar de licencias para las herramientas de gestión de seguridad debe tener la capacidad de realizar el escaneo sin limitaciones a nivel de direcciones IP, aplicaciones web, dispositivos tecnológicos.

- La instalación, configuración y puesta funcionamiento de las herramientas de gestión de seguridad.
- El contratista debe realizar la transferencia de conocimiento y documentación asociada.

La solución de Ciber-Seguridad debe estar en capacidad de realizar las siguientes acciones y cumplir con las siguientes características técnicas:

- Desplegar un número ilimitado de escaneos sin costo adicional.
- Soporte en todas sus funcionalidades el protocolo IPv4 y el protocolo IPv6
- Escanee los activos previamente identificados de manera automática a través de la programación de tareas por hora, por día, por fecha, y por días recurrentes.
- Los escáneres deben ser gestionados por la plataforma, ofrecer actualizaciones de firmas de vulnerabilidad, y otras actualizaciones.
- Entregar una herramienta de análisis de vulnerabilidades que automatice evaluaciones frente a la detección de vulnerabilidades bajo un criterio estándar de seguridad.
- La Herramienta debe proporcionar una descripción de la posible solución para mitigar o corregir las vulnerabilidades encontradas en los sistemas, así como una manera rápida y fácil de visualizar sistemas son vulnerables dando clasificación como alta, media, baja y otros.
- La herramienta deberá permitir una visibilidad amplia y completa de las vulnerabilidades.
- La herramienta deberá tener plantillas preconfiguradas para la identificación de los diferentes activos de la red y así como la posibilidad de ofrecer auditorías de configuración, con el fin de comprender rápidamente dónde están las vulnerabilidades. dispositivos y aplicaciones.
- La herramienta deberá realizar Evaluaciones ilimitadas, lo que quiere decir que no hay límite para analizar una determinada cantidad de direcciones IP.
- La herramienta deberá permitir integrarse con SIEM.
- La herramienta deberá permitir integrarse con el Firewall.
- La herramienta deberá permitir auditoría personalizados que verificaran requisitos de configuración frente a los estándares de cumplimiento y buenas prácticas de seguridad de la información.
- Realizar transferencia de conocimiento para escaneo de vulnerabilidades a la red local, plataformas en nube y aplicaciones web, adicional de cómo realizar reportes especializados automáticos sin ningún costo adicional.
- La herramienta deberá tener las siguientes plantillas: escaneo avanzado, Detención de Badlock, detención de shellshock, Escaneo de red básico, Auditoria de Credenciales Parches, Detención de Drown, Descubrimiento de Host, Bypass AMT INTEL, Internal Scan PCI, Políticas Compliance para auditoria, Auditoria SCAP y OVAL, Escaneo Shadow Broker, Test de Aplicación Web.

- La herramienta debe realizar análisis de vulnerabilidades web mediante acceso con usuario y contraseña.
- La herramienta de análisis de vulnerabilidades deberá tener compatibilidad con diferentes sistemas operativos para su instalación, adicional la herramienta deberá permitir generar informes en función de vistas personalizadas (por ejemplo, tipos de vulnerabilidad específicos, vulnerabilidades por host/complemento, por equipo/cliente) en diferentes formatos como (HTML, CSV, XML y PDF).
- Las herramientas de análisis de seguridad deberán generar reportes / informes:
- Proporcionar la capacidad de automatizar los informes al poder programar informes.
- Admitir la capacidad de producir informes en los siguientes formatos de informe: PDF, CSV, HTML y otros.
- Los informes deben tener la capacidad de incluir nombres de host (NetBIOS, DNS) junto con direcciones IP.
- Proporcionar una biblioteca de plantillas de informes y paneles.