	Imprenta Nacional de Colombia **REQUERIMIENTO DE BIENES Y SERVICIOS**	GAA-FO-1 20/04/2023 Versión 4

Fecha de la Solicitud: 15 de diciembre de 2023 Solicitud: 20231100021643

Dependencia: **OFICINA DE SISTEMAS E INFORMÁTICA**

Coordinador área solicitante: **ALEXANDER ROZO PATIÑO**

Requerimiento para adquisición de: **SERVICIOS**

1. **Objeto del contrato**

Renovación de la Plataforma de Seguridad informática perimetral Palo Alto PA-450 y endpoint Cortex XDR Prevent de la Imprenta Nacional de Colombia, incluyendo una solución de control de acceso a la red (NAC).

2. Condiciones técnicas *(Descripción detallada y específica de las condiciones técnicas del bien y/o servicio a contratar, donde se indique: unidad de medida, ítems, cantidades y los servicios conexos y/o necesarios para cumplir con el objeto de la contratación).*

Código UNSPSC	*Descripción del bien o servicio*	*Unidad de Medida**	*Cantidad**	*Precio techo según estudio de mercado*
	Renovación de la Plataforma de Seguridad informática perimetral Palo Alto PA-450 y endpoint Cortex XDR Prevent de la Imprenta Nacional de Colombia, incluyendo una solución de control de acceso a la red (NAC – Network Access Control).	Año	1	$ 115.856.184

* Únicamente aplica para bienes

3. Justificación de la solicitud o necesidad en la adquisición del bien o servicio (Exponga los argumentos, razones de por qué y para qué se requiere la contratación)

La Imprenta Nacional requiere contratar la renovación de la Plataforma de Seguridad, con el objeto de asegurar la ejecución de políticas de la Seguridad de la Información, manteniendo la seguridad de los elementos esenciales de la Infraestructura Tecnológica de la Imprenta Nacional de Colombia, la Entidad requiere realizar renovación de la Plataforma de Seguridad Informática que utiliza actualmente y que debe contemplar conceptos de seguridad adaptativa y predictiva; para que de esta manera no se llegue a afectar la prestación de los servicios de información que actualmente se brindan a los usuarios a través de los Sistemas de Información e Internet.

Con la sofisticación de los atacantes que existe hoy en día, la entidad requiere fortalecer su estrategia de Ciber-seguridad a fin de disminuir el riesgo de recibir un ataque y así mismo

disminuir la superficie de ataque disponible. Por esta razón la entidad requiere contar con una solución de vanguardia que cuente con el respaldo de un fabricante experto en el sector de Ciberseguridad.

En la visión de la Imprenta Nacional de Colombia, actualmente se cuenta con una solución que basada en la aplicación de los conceptos de Zero Trust Network Access (ZTNA), en donde no se permite el acceso a la información confidencial de la entidad; para complementar este sistema es necesario asegurar que el individuo este autorizado, el dispositivo este permitido, la ubicación sea autorizada y el instante en el que se accede a la información sea la correcta; por lo tanto es necesario incluir una solución que permita realizar el control de acceso a la red (NAC – Network Access Control) como complemento a la plataforma de seguridad actual de la empresa compuesta por la seguridad perimetral Palo Alto PA-450 y endpoint Cortex XDR Prevent.

.

Procesos Misionales (Para adquisición de productos y servicios de comercialización)

N° O.P			
N° Cotización			
No. Contrato Cliente		Saldo del contrato a la fecha	

Procesos de apoyo

Describa la justificación por la cual se requiere adquirir el producto y/o servicio requerido para el funcionamiento de los procesos de producción y áreas administrativas.

4. Requisitos evaluables de orden técnico

4.1 Requisitos de orden técnico:

El contratista se compromete a renovar la Plataforma de Seguridad Informática, cumpliendo con las siguientes especificaciones técnicas:

- Renovación solución perimetral Palo Alto PA-450 (S/N: 23201011003 y 23201011564), con vigencia hasta el 30 de noviembre de 2024; teniendo en cuenta que la entidad actualmente tiene en uso un sistema de seguridad perimetral de tecnología NextGeneration Firewall en alta disponibilidad de marca Palo Alto y referencia PA-450. Este sistema de seguridad perimetral actualmente maneja las siguientes utilidades o módulos de seguridad: Advanced Threat Prevention, Advanced URL Filtering, Wildfire, DNS Security y SDWAN; el servicio de licenciamiento, garantía y soporte se adquirió inicialmente con vigencia hasta el 30 de noviembre de 2023. El oferente debe proveer los servicios de garantía, soporte y actualización,

además del licenciamiento Support, Advanced Threat Prevention, Advanced URL Filtering, Wildfire, DNS Security y SDWAN para dispositivos en Alta Disponibilidad HA marca Palo Alto.

- Renovación del licenciamiento (340 licencias, con S/N: 0220980000020565) Cortex XDR Prevent, con vigencia hasta el 30 de noviembre de 2024; teniendo en cuenta que la entidad actualmente tiene en uso una solución con trecientas cuarenta (340) licencias para protección de punto final (End Point) Cortex XDR Prevent marca Palo Alto, El servicio de licenciamiento, garantía y soporte se adquirió inicialmente y caduca el día 30 de noviembre de 2023. El oferente debe proveer los servicios de garantía, soporte y actualización, además del licenciamiento de Cortex XDR Prevent, que incluye 30 días de retención de alertas, marca Palo Alto.
- El proponente debe acreditar que es un canal habilitado para Colombia en distribución y venta de la marca ofertada para la solución perimetral y Cortex XDR, como mínimo en nivel Register.
- El proponente debe tener un Ingeniero(a) de sistemas, electrónico, telecomunicaciones o afín, con dos (2) años de experiencia certificada en ciberseguridad y certificaciones de fábrica PCNSA y PCNSA, el ingeniero(a) debe tener vinculación laboral a la empresa para la ejecución del contrato
- El proponente debe entregar carta de compromiso de la ejecución del proyecto, de acuerdo a las necesidades de la Entidad.
- Brindar el soporte técnico necesario, en modalidad 7/24
- Ofrecer una solución de control de acceso a la red (NAC – Network Access Control), con las especificaciones técnicas que se describen en el numeral 4.1.4 y Otros requisitos técnicos.

4.1.1 Plazos

Plazo de entrega:	Cinco (5) días hábiles	Plazo de reposición:	N/A
Garantía:	12 Meses		

Nota. Se deberán indicar la calidad de los días (hábiles o calendario) en los plazos anteriormente indicados. Cuando no se indiquen en el requerimiento o en las cotizaciones presentadas por los oferentes, se entenderán que los días son calendario.

4.1.2 Experiencia adicional exigida:

El proponente deberá presentar por lo menos tres (2) certificaciones expedidas por entidad estatal y/o empresa privada en la que conste:

- Que la sumatoria de los contratos sea igual o superior al que se pretende contratar por parte de la INC
- Que dentro del objeto incluya la Implementación, actualización o Renovación de Plataforma de Seguridad informática perimetral firewall Palo Alto o EndPoint.(Antivirus) de Palo Alto

- Que la certificación venga en papelería de la respectiva entidad y/o empresa con sus logos, direcciones y teléfonos si a ello hubiere lugar.
- La certificación debe estar suscrita por un funcionario de la empresa o entidad, incluyendo los datos de contacto para verificar la información.
- Que indique cualquier otro aspecto que se considere relevante

En caso de que se aplique la subsanabilidad las certificaciones deberán haberse expedido con anterioridad al cierre del proceso

4.1.3 Obligaciones específicas del contratista:

El Oferente debe cumplir con las siguientes especificaciones:

- Ofrecer al menos 20 horas de capacitación y asesoría, para el uso eficiente de las diferentes herramientas y componentes que hacen parte de la solución contratada (Firewall, EndPoint y NAC)
- Configuración de la solución contratada (Firewall, EndPoint y NAC) de todos sus componentes de acuerdo a las necesidades de la Imprenta Nacional de Colombia, utilizando las mejores prácticas de optimización y configuración

4.1.4 Otros requisitos técnicos

SOLUCIÓN NAC – NETWORK ACCESS CONTROL

La entidad requiere una solución que proporcione control de acceso a la red basado en roles y dispositivos para empleados, contratistas e invitados en infraestructuras VPN, inalámbricas y cableadas de múltiples proveedores. La cual debe soportar un motor de políticas integrado basado en contexto, RADIUS, compatibilidad con el protocolo TACACS+, creación de perfiles de dispositivos y evaluación integral de la postura, opciones de incorporación y acceso de invitados.

Especificaciones técnicas mínimas requeridas:
- Licenciamiento de máquina virtual de propósito específico para habilitar Solución de Control de Acceso a la red cableada, inalámbrica y VPN.

La entidad proveerá las siguientes capacidades de cómputo y almacenamiento:
- 8 CPU virtuales reservadas
- 8 GB de RAM
- 1000 GB de espacio en disco
- 2 puertos conmutados virtuales Gigabit

- Solución debe soportar acceso diferenciado para dispositivos corporativos, contratistas, invitados, IoT y BYOD.
- Soporte para ambientes de red multi-vendor
- Soporte integrado para servicios RADIUS, TACACS+, enforcement SNMP e integraciones con soluciones de seguridad de terceros mediante APIs

- Capacidad de adicionar servicios de: BYOD y Postura de Seguridad agregando licenciamiento adicional

Descripción	Características Generales
Capacidad	La solución deberá manejar 500 sesiones RADIUS activas concurrentes. El licenciamiento debe cubrir 500 puntos terminales.
Hipervisor	El dispositivo virtual debe ser soportado en VMware ESX/i y/o en Microsoft Hyper-V
Servicios incluidos en licenciamiento base	Deberá incluir en el licenciamiento base los siguientes servicios: – 802.1X – Autenticación por MAC Address – TACACS+ – Enforcement a través de SNMP – Integraciones con terceros mediante REST APIs
Seguridad contextual	La política de seguridad deberá permitir tomar en consideración elementos contextuales como: horario, ubicación, tipo de dispositivo, versión de SO y nombre del dispositivo, entre otros
Soporte Multivendor	- Soporte para Assessment de postura, perfilamiento y autenticación web en ambientes de red multi-vendor y basado en protocolos estándar RADIUS y RADIUS CoA
Control de acceso unificado	- Deberá controlar el acceso de usuarios y dispositivos a través de la red cableada (switches), inalámbrica (access points y controladores WiFi) y VPN (firewalls y concentradores VPN) de manera unificada. Debe integrarse con los Firewall Palo Alto de la entidad.
Servicios AAA	- Deberá soportar la aplicación de políticas contextuales mediante servicios AAA: RADIUS, RADIUS CoA, TACACS+ y SNMP
Reportería	- Deberá incluir sin costo adicional un componente de monitoreo y reportería con información en tiempo casi real e histórica sobre usuarios y dispositivos conectados, alertas, autenticación, perfiles de dispositivos, estado del cliente. Las alertas se pueden enviar mediante SMS o notificación por correo electrónico a varios destinatarios
Métodos de Perfilamiento	Deberá soportar los siguientes métodos de perfilamiento: - Activo: Nmap, WMI, SSH, SNMP - Pasivo: MAC OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFLOW, Puerto 'SPAN', HTTP User-Agent, IF-MAP - Integrados y de terceros: Desde la solución de BYOD y de chequeo de postura, EMM/MDM, Cisco device sensor.
IPv6	Soporte Ipv6
Protocolos y Frameworks soportados	

Protocolos para los servicios AAA	La solución NAS deberá soportar al menos los siguientes protocolos para los servicios AAA: - RADIUS, RADIUS CoA, TACACS+, autenticación web, SAML 2.0, RadSec - 802.1X - EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS) - PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS. EAP-PEAP-Public,EAP-PWD) - TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5,PAP, CHAP) - EAP-TLS - PAP, CHAP, MSCHAPv1 y 2, EAP-MD5 - OAuth2 - Autenticación de Máquina en dominio Windows - SMB v2/v3 - Online Certificate Status Protocol (OCSP) - SNMP generic MIB, SNMP private MIB - Common Event Format (CEF), Log Event Extended Format (LEEF) y RFC5424
Fuentes de Autenticación	La solución deberá soportar las siguientes fuentes de autenticación sin licenciamiento o plugins adicionales: - Microsoft Active Directory - RADIUS - Cualquier directorio basado en protocolo LDAP - MySQL, Microsoft SQL, PostGRES, Oracle 11g y cualquier servidor SQL ODBC-compliant - Servidores de Token - Base de datos interna - Kerberos - Microsoft Azure Active Directory (viaSAML y OAuth2.0) - Google G Suite

Estándares RFC	El sistema deberá soportar los siguientes estándares RFC: - RFC 2246 The TLS Protocol Version 1.0 - RFC 2248 Network Services Monitoring MIB - RFC 2407 Internet IP Security Domain of Interpretation for ISAKMP - RFC 2408 ISAKMP - RFC 2409 The Internet Key Exchange (IKE) - RFC 2548 Microsoft Vendor-specific RADIUS Attributes - RFC 2759 Microsoft PPP CHAP Extensions, Version 2 - RFC 2865 Remote Authentication Dial In User Service (RADIUS) - RFC 2866 RADIUS Accounting - RFC 2869 RADIUS Extensions - RFC 2882 Network Access Servers Requirements: Extended RADIUS Practices - RFC 3079 Microsoft Point to Point Encryption - RFC 3576 Dynamic Authorization Extensions to RADIUS - RFC 3579 RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP) - RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines - RFC 3748 Extensible Authentication Protocol (EAP) - RFC 3779 X.509 Extensions for IP Addresses and AS Identifiers - RFC 4017 Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs - RFC 4137 State Machines for Extensible Authentication Protocol (EAP) Peer and Authenticator - RFC 4301 Security Architecture for IP - RFC 4302 IP Authentication Header - RFC 4303 IP Encapsulating Security Payload (ESP) - RFC 4308 Cryptographic Suites for IPsec - RFC 4346 TLS Protocol - RFC 4514 Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names - RFC 4518 Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation - RFC 4809 Reqs for IPsec Certificate Mgmt Profile - RFC 4849 RADIUS Filter Rule Attribute - RFC 4851 EAP-FAST - RFC 4945 PKI Profile for IKE/ISAKMP/PKIX - RFC 5216 The EAP-TLS Authentication Protocol - RFC 5246 The Transport Layer Security (TLS) Protocol - RFC 5280 Internet X.509 Public Key Infrastructure - RFC 5281 EAP-TTLSv0 - RFC 7296 Internet Key Exchange Protocol Version 2 - RFC 7321 ESP y AH - RFC 7468 Textual Encodings of PKIX, PKCS, and CMS Structures - RFC 7815 Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation - RFC 8032 Edwards-Curve Digital Signature Algorithm (EdDSA) - RFC 8247 The Internet Key Exchange v2 (IKEv2)



Servicios adicionales	- Deberá tener la capacidad de adicionar de manera modular servicios de: Enrolamiento de dispositivos personales en entornos corporativos (BYOD), Postura de Seguridad sobre PCs corporativos y portal para acceso de visitantes.
Licenciamiento	- El licenciamiento deberá ser perpetuo e incluir soporte directo de fábrica 7/24 con vigencia hasta el 30 de noviembre de 2024.
Fabricante	La solución debe ser del mismo fabricante de la solución de Switches y Access Point que tiene la entidad actualmente (Marca Aruba)
Implementación	Se debe incluir servicio de instalación, configuración y puesta en marcha, por un Ingeniero de sistemas, electrónico, telecomunicaciones o afín, con dos (2) años de experiencia certificada en ciberseguridad y certificaciones de fábrica PCNSA y PCNSA. Además debe cumplir al menos con dos (2) certificaciones en el fabricante ofertado, tales como ACDA, ACMA, ACSA y/o ACA–Network Security. El personal debe de estar contratado por el proponente para la ejecución del contrato y el proponente debe entregar carta de compromiso de ejecución del proyecto firmada por el Ingeniero que cumple el perfil solicitado por el proceso.
Certificado de fábrica	El proponente debe acreditar que es un canal habilitado para Colombia en distribución y venta de la marca ofertada, como mínimo en nivel Register.

5. Sistema de calificación:

La forma de calificación y asignación de puntajes será la siguiente:

CALIFICACIÓN Y ASIGNACIÓN DE PUNTAJES
Solo serán objeto de calificación y puntaje las propuestas que cumplan estrictamente todos los requisitos de carácter jurídico, técnico, económico y financiero. La falta de alguno de ellos inhabilitará la oferta.
Previo cumplimiento de los requisitos anteriores la Imprenta Nacional de Colombia asignará el puntaje a las propuestas de la siguiente manera:

ASPECTO ECONÓMICO **1000 PUNTOS**

Para la evaluación de este aspecto, recibirá el mayor puntaje quien ofrezca el menor precio total y las demás ofertas obtendrán un puntaje aplicando regla de tres inversa.

TOTAL PUNTOS **1.000 PUNTOS**

.

5.1 Descripción de calificación (si se requiere)**:**

No Aplica

6. Obligaciones y/o Requisitos Ambientales y/o Seguridad y salud en el trabajo:

Cumplir con el SGA y SST vigente de la IMPRENTA NACIONAL DE COLOMBIA para procesos de instalación y montaje requeridos.

7. Plazo de ejecución

12 meses

8. Valor estimado de la contratación. Este valor debe estar basado en el estudio de mercado previo a la elaboración del requerimiento.

Se tomó como valor del presupuesto asignado para este proceso, el menor valor ofertado entre las cotizaciones recibidas.

La forma de pago para este proceso debe ser: La Entidad pagará el valor del contrato (bienes y/o servicios suministrados), previo cumplimiento de los requisitos de ley y el cumplido a satisfacción firmado por el supervisor del contrato.

Valor en letras	**Valor en cifras**
CIENTO QUINCE MILLONES OCHOCIENTOS CINCUENTA Y SEIS MIL CIENTO OCHENTA Y CUATRO PESOS M/CTE	$ 115.856.184

9. Acuerdo de niveles de servicio ANS El cumplimiento tardío de las obligaciones contractuales generará un descuento comercial automático sobre la facturación. Se podrá pactar no menos del 0,5% y no más del 5% del valor del contrato.

En el caso de que el supervisor del contrato detalle y pruebe el cumplimiento tardío, el descuento aplicado será por: 2%

10. Evaluador técnico

Jose Vicente Galindo

11. Supervisor o interventor del contrato

La supervisión del contrato será ejercida por:

César Augusto Escobar Prada

Requiere Interventor: ☐ SI ☑ NO

12. Observaciones especiales del requerimiento:

El presente proceso se adelanta bajo la modalidad de Contratación Directa, de acuerdo a lo establecido en el artículos 29 y 30 literal a) "*Cuando la cuantía del contrato a celebrar sea igual o inferior a cien (100) SMLMV*" de la Resolución 002 "Manual de Contratación de la Imprenta Nacional de Colombia", en consideración a que el valor a contratar es por $ 115.856.184, valor inferior a 100 SMLMV). El presupuesto está basado en el estudio de mercado previo a la elaboración del requerimiento (se tomó el menor valor de las cotizaciones recibidas) y los precios históricos de contratación de la entidad para estos servicios. El presupuesto asignado para este proceso, es del rubro de PAQUETES DE SOFTWARE - LICENCIAMIENTO PLATAFORMA DE SEGURIDAD INFORMÁTICA (FIREWALL, ANTIVIRUS Y CORREO ELECTRONICO SEGURO) Y PRUEBAS DE VULNERABILIDAD - ETHICAL HACKING. **Se recomienda la adjudicación de este proceso, al proveedor que cotizó el menor precio por los servicios solicitados**.

Firma Coordinador de grupo
(Grupo solicitante del bien o servicio)

Nombre y firma
(Subgerente, Jefe de Oficina solicitante)

Firma Ordenador del Gasto

Elaborado por: Maria Liliana Navarro M.