FORMATO NRO. 4
CONDICIONES OFERTA TÉCNICA

Yo, *Mayra Alejandra Castro Torres* identificado con cedula de ciudadanía No *1.014.181.910*, obrando en nombre y representación de *AndeanTrade Group Latam SAS* , me comprometo de manera clara e inequívoca al cumplimiento de los siguientes requisitos técnicos mínimos establecidos en la presente invitación.

a) OBLIGACIONES GENERALES DEL CONTRATISTA:

1) Cumplir cabalmente con el desarrollo del objeto presente contrato de acuerdo con las condiciones técnicas y económicas estipuladas en el requerimiento, la Invitación y la propuesta presentada.
2) Informar de manera inmediata al supervisor del contrato cualquier anomalía que se presente durante la ejecución del mismo.
3) Atender las observaciones que durante el desarrollo del contrato imparta el supervisor designado.
4) Presentar los informes correspondientes para la formalización y legalización de los pagos, así como los que el supervisor del contrato le solicite.
5) Dar cumplimiento a las obligaciones del sistema de seguridad social (salud, pensión y riesgos laborales) así como al SG-SST y demás normas aplicables, presentando los documentos respectivos que acrediten tal situación.
6) Cargar en la plataforma SECOP II la factura generada para cada uno de los cobros de bienes y/o servicios prestados, junto con el soporte de pago de los aportes al Sistema de Seguridad Social y demás declaraciones del contratista para el efecto, y enviar electrónicamente a la entidad contratante, para el inicio del trámite de pago respectivo.
7) Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y retrasos injustificados.
8) Mantener el precio relacionado y propuesto en su oferta, sin variación durante el término de la duración del contrato.
9) Dar cumplimiento a todas aquellas obligaciones inherentes al contrato y necesarias para la correcta ejecución del objeto del mismo.

b) OBLIGACIONES ESPECIFICAS DEL CONTRATISTA:

- 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

- **REQUISITOS EVALUABLES DE ORDEN TECNICO:**

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.

- **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.

c) PLAZOS:

1. Plazo de entrega: será de cinco (5) días hábiles.
2. Plazo de garantía: será de doce (12) meses, contados a partir de la prestación del servicio.
3. Plazo de ejecución: será de doce (12) meses, contados a partir del cumplimiento de los requisitos de ejecución del contrato.

d) EXPERIENCIA EXIGIDA

Cumplimos con la experiencia exigida en la invitación para lo cual adjuntamos las certificaciones que la acreditan, en los términos solicitados.

e) PLAZO DE EJECUCIÓN DEL CONTRATO

El plazo de ejecución del contrato será de doce (12) meses, contados a partir del cumplimiento de los requisitos para dar inicio a la ejecución del contrato.

f) ACUERDOS DE NIVELES DE SERVICIO:

Aceptamos realizar en caso de incumplimiento de las obligaciones contractuales generará un descuento comercial automático sobre la facturación presentada por el contratista a la Imprenta, de conformidad con el porcentaje establecido en la presente invitación, el cual será del **2%** del valor del contrato suscrito.

Para constancia se firma el *26 de diciembre de 2023*

(Firma)_____

HOJA NRO. 35 - INVITACIÓN DIRECTA SIN OFERTAS NRO. IMPRENTA NACIONAL DE COLOMBIA IDIRSIN-INC-193-2023

Nombre y apellidos del Representante Legal: *Mayra Alejandra Castro Torres*
C.C. No. *1.014.181.910* De *Bogotá D.C.*