PLIEGO DE CONDICIONES PARTICULARES Y ESPECIFICACIONES TÉCNICAS

LICITACIÓN PÚBLICA Nº 425

APERTURA: 15 de agosto de 2018 **HORA: 10:00**

OBJETO:

El presente llamado a Licitación Pública tiene por objeto la adquisición y puesta en marcha de una solución integrada de conectividad inalámbrica y de protección de redes para la seguridad de la información perimetral

1. ESPECIFICACIONES TÉCNICAS

Estas especificaciones técnicas establecen las condiciones mínimas que debe satisfacer el equipamiento objeto de la presente licitación, que consiste en la adquisición y puesta en marcha de una solución integrada de conectividad inalámbrica basada en controladores centrales y puntos de acceso o Access Points y de protección de redes para la seguridad de información perimetral. Esta solución deberá contemplar al menos siete (7) Access Points de interior, dos (2) Access Points de Exterior, un (1) Controlador wireless y una (1) plataforma de seguridad de protección de redes.

Se deberá incluir además todo el software necesario para el normal funcionamiento de los elementos cotizados, el mantenimiento preventivo

y correctivo de los mismos. La propuesta deberá incluir la capacitación al personal técnico del Ente.

1.1 ÍTEM ÚNICO

1.1.1. Renglón 1:

Access Points de interior
Cantidad: 7 (siete)

Se solicitan equipos compactos que ofrezcan mínimamente una velocidad máxima de datos simultáneos de 867 Mbps en la banda de 5Ghz y 400 Mbps en la banda de 12,4Ghz (para una velocidad máxima de datos total de 1,3 Gbps)

Especificaciones técnicas mínimas:

- Número de radios: 2
- Bandas soportadas: dual concurrentes
- Estándares Wi - Fi: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac
- Tipo de Radios MIMO: 2x2: 2SS SU – MIMO
- Máximo número de BSSIDs (por radio): 16
- Máximo número de clientes asociados por radio: 255
- Máxima potencia de transmisión (por cadena de radio, MCS0): para 2.4 Ghz y 5Ghz: 18dBm (conducted) per chain
- Antenas integradas: 2x omni – direccional
- Interface de redes: 1x GE
- Potencia PoE PD: 802.3af/3at
- PoE PSE: No
- Garantía de por vida: Sí
- Montaje: kit de montaje para techo y pared
- Modo de funcionamiento: el mismo equipo debe permitir funcionar en modo controlado o en modo de cluster con un controlador virtual, rol que toma el primer Access Point que se configura
- Soporte de análisis de Espectro: No

- Máximo consumo de potencia (excluyendo USB, PoE PSE) 12.3W (PoE), 10.1W (DC). Debe incluir power inyector para su alimentación
- Máximo desempeño en Ipsec encriptado cableado (modo RAP): 20

1.1.2. **Renglón 2**: Access Points de Exterior
Cantidad: 2 (dos)

Se solicitan equipos que ofrezcan desempeño wi-fi 802.11a/b/g/n/ac rápido y confiable bajo cualquier condición climática, con diseño estético y discreto, que ofrezcan mínimamente una velocidad máxima de datos simultáneos de 867 Mbps en la banda de 5Ghz y 400 Mbps en la banda de 12,4Ghz (para una velocidad máxima de datos total de 1,3 Gbps)

Especificaciones técnicas mínimas:

- Número de radios: 2
- Bandas soportadas: Dual concurrentes
- Estandares de wi-fi: IEEE 802.11a, IEEE 802.11b, 802.11g, IEEE 802.11n, IEEE 802.11 ac, IP66 & IP67
- Tipo de radios MIMO: 3x3: 3
- Máximo número de BSSIDSs (por radio): 16
- Máximo número de clientes asociados por radio: 255
- Máxima potencia de transmisión (por cadena de radio, MCS0): banda de 2.4Ghz; +28dBm; Banda 5 Ghz: +28dBm
- Antenas integradas: con ganancia de 5dBi en 2.4Ghz y en 5 Ghz
- Interfaces de Redes: 1 puerto PoE+ 10/100/1000Base-T Ethernet. 1 puerto 10/100/1000Base-T Ethernet
- Interface USB
- Puerto de consola: Micro USB

- Potencia PoE PD: 802.3at
- TAA/FIPS: No
- Garantía de por vida: si
- Montaje: kit de montaje para techo y pared
- Modo de funcionamiento: el mismo equipo debe permitir funcionar en modo controlado o en modo de cluster con un controlador virtual, rol que toma el primer Access Point que se configura
- Modo de supervivencia: Deberá tener la posibilidad de que en caso de que se pierda la conexión con el controlador siga funcionando en forma autónoma con los usuarios ya conectados dando un servicio mínimo
- Soporte de análisis de Espectro: Si
- Máximo consumo de potencia (excluyendo USB, PoE PSE) 23w (PoE), 802.3at. Debe incluir power inyector de exteriores para su alimentación

Se deberá incluir la totalidad de licencias que permitan gestionar todos los Access Points de la presente solución, tanto Indoor como Outdoor.

1.1.3. **Renglón 3:** Controlador
Cantidad: 1 (uno)

Se solicita controlador de acceso inalámbrico autónomo (no debe ser un módulo que requiera ser instalado en un chasis)

Especificaciones técnicas mínimas:

- Mínimo 1 APs con crecimiento al menos hasta 16 APs
- Máximo número de usuarios inalámbricos concurrentes: 1024
- Puertos para datos: 4 puertos 10/100/1000 BASE-T, Auto -MDIX, al menos 4 de ellos de tipo dual 10/100/1000Base-T
- Puertos para administración: 1 interfaz serial RJ45

- Capacidad de administración: los APs soportados deben ser tanto para interiores como para exteriores. El crecimiento debe darse únicamente a través de licenciamiento, no debe requerir cambios en el hardware del equipo
- Tráfico de datos: debe incluir todo cuanto requiera para poder conmutar al menos 2Gbps de tráfico inalámbrico centralizado
- Portal local: El controlador ofertado debe incluir el servicio de portal local para al menos 1000 usuarios
- Autenticación: Debe incluir el servicio de autenticación "triple A" (AAA) para 1024 usuarios
- SSIDs: Debe soportar 64 SSIDSs configurados
- Listas de Acceso: Debe soportar 2000 listas de Control de Acceso (ACLs)
- Estándares de movilidad: Debe cumplir los siguientes estándares: IEEE 802.11a, IEEE 802.11b, IEEE 802.11d, IEEE 802.11e, IEEE 802.11g, IEEE 802.11h, IEEE 802.11i, IEEE 802.11k, IEEE 802.11n, IEEE 802.11s D1.06 draft, IEEE 802.11w, IEEE 802.11ac
- Con respecto a la movilidad debe ofrecer los siguientes servicios:
  - Ajuste automático de potencia de los radios
  - Detección en tiempo real de interferencias
  - Conmutación inteligente y en tiempo real del canal
  - Balanceo inteligente de clientes entre múltiples APS
  - Mecanismos para ofrecer tiempos iguales de transmisión a los clientes
  - Identificación de fuentes de interferencia RF que permita detectar y clasificar señal inalámbrica.
  - Evaluación de calidad de canal
  - Redirección de usuarios que puedan trabajar en 50 Ghz a esta banda
  - Asignación dinámica de clientes a diferentes VLANs

- Visibilidad unificada de red alámbrica e inalámbrica utilizando al menos LLDP
- Configuración automática de APs.
- Aplicación de políticas basadas en el SSID o perfil de usuario
- Capacidad para agrupar APs
- Capacidad para actualizar el sistema operativo de los APs
- Capacidad para seleccionar la ganancia de la antena.
- Roaming rápido, en capa 3

- Manejo de tráfico: Debe soportar los siguientes tipos de manejo para el tráfico inalámbrico:
  - Tráfico centralizado: debe pasar primero por el controlador antes de pasar a la red inalámbrica
  - Tráfico distribuido: el tráfico inalámbrico puede ir directo del Access Point hacia la red inalámbrica
- Calidad de servicio (QoS): Debe ofrecer:
  - QoS de extremo a extremo al menos a través de DiffServ e IPv6 QoS.
  - Priorización IEEE 802.1p.
  - CoS basado dirección IP, ToS, protocolos de L3, número de puertos TCP o UDP, puerto origen y DiffServ.
  - Perfiles de QoS.
- Autenticación: Debe ofrecer:
  - AAA
  - Login vía 802.1x y RADIUS
  - Autenticación basada en web para clientes que no soportan 802.1x
  - Autenticación por dirección MAC
  - WEP, WPA, WPA2
  - Control de acceso de usuarios definidos por el administrador en APs específicos

- Firewall: El controlador inalámbrico debe contar con servicios integrados de Firewall, basado en:
  - Filtrado de paquetes basado en Listas de Control de Acceso
  - Filtrado de paquetes específicos por aplicación
- Detección de intrusión: Debe integrar un Wireless IDS (Intrusion Detection System) que permita detectar:
  - Inundaciones
  - Spoofing
  - Ataques por debilidad
  - Identificar en forma automática APs y estaciones
  - Base heurística de conocimiento
  - Protección contra ataques de tipo honeypot
  - Seguridad reforzada STA
  - Detección de ataques DoS
  - Distribución de políticas a dominios virtuales de seguridad
- Seguridad adicional: Debe ofrecer:
  - Validación de la relación dirección IP y MAC de usuarios para evitar ataques de suplantación
  - Aislamiento de usuarios para provisión de servicios diferenciados por grupos
  - Integración con servicios de control de admisión a la red
  - PKI
  - Guest VLAN
  - SSL
  - SSHv2
  - RFC 1851 ESP
  - RFC 2246 TLS
  - RFC 2401 Security Architecture
  - RFC 2408 ISAKMP
  - RFC 2409 IKE
  - RFC 2548 Microsoft RADIUS Attributes
  - RFC 2716 PPP EAP TLS Auth

- RFC 2865RADIUS Authentication
- RFC 2867 RADIUS for Tunnel Protocol
- RFC 3394 AES
- RFC 3576 Dynamic Authorization
- RFC 3579 RADIUS Support for EAP
- RFC 3580
- IEEE 802.1x RADIUS

• Alta Disponibilidad: debe soportar al menos los siguientes esquemas de redundancia y respaldo:

- 1+1
- N+1
- N+N

En cualquiera de los esquemas, la validación de los APS debe ser automática, ofreciendo un servicio continuo ante la falla de uno de los Controladores

- Funcionalidades de Capa de Enlace (L2): Debe cumplir al menos los siguientes estándares de la industria:
  - IEEE 802.3ad Link Agregation, con hasta 12 grupos troncales, pudiendo manejar cada uno hasta 8 puertos activos del mismo tipo
  - IEEE 802.1x
  - IEEE 802.1Q, con al menos 4094 VLAN ID simultáneos
  - IEEE 802.1D STP
  - IEEE 802.1w RSTP
  - IEEE 802.1s MSTP
- Servicios adicionales para Capa de enlace (L2): Debe ofrecer los siguientes servicios:
  - Puertos espejo para análisis de tráfico
  - Soporte de paquetes jumbo hasta 9kbytes para el switch y 4kbytes para el controlador

- Enrutamiento IP: Debe ofrecer enrutamiento estático IPv4, IPv6, RIPv1 Y RIPv2
- Protocolos Generales IP: Debe cumplir los siguientes estándares de la industria:
    - RFC 768 UPD
    - RFC 791 IP
    - RFC 792 ICMP
    - RFC 793 TCP
    - RPC 826 ARP
    - RFC854 TELNET
    - RFC 894 IP over Ethernet
    - RFC 950 Standard Subnetting
    - RFC 959 FTP
    - RFC 1122 Host Requirements
    - RFC 1141 Internet Checksum
    - RFC 1144 Compressing TCP/IP headers
    - RFC 1256 ICMP Router Discovery
    - RFC 1305 NTPv3
    - RFC 1321 MD5
    - RFC 1334 PPP PAP
    - RFC 1350 TFTP Protocol revisión 2
    - RFC 1812 IPv4 Routing
    - RFC 1944
    - RFC 1994 PPP CHAP
    - RFC 2104 HMAC
    - RFC 2246 The TLS Protocol v1.0

- RFC 2474 DS Field in IPv4 & IPv6
- RFC 2475 DiffServ
- RFC 2284 EAP over LAN
- RFC 2644 Directed Broadcast Control
- RFC 2864
- RFC 2866 RADIUS Accounting
- RFC 2869 RADIUS Extensions
- RFC 3164 Syslog
- RFC 3164 ECNTo IP
- RFC 3268 AES for TLS
- RFC 3619 EAPS
- RFC 3636 Medium Attchament Units

- Multicast: Debe cumplir los siguientes estándares de la industria:
  - RFC 1112 IGMP
  - RFC 2236 IGMPv2
  - RFC 2934 PIM MIB para IPv4
  - RFC 4541 IGMP and MLD Snooping

- IPv6: Debe cumplir los siguientes estándares de la industria:
  - IPv6 Host
  - Dual stack IPv4 – Ipv6
  - MLD snooping
  - Listas de Control de Acceso para IPv6
  - Calidad de servicio (QoS) para IPv6
  - RFC 1981 IPv6 MTU Discovery
  - RFC 2375 IPv6 Multicast Assignements
  - RFC 2460 IPv6 Specification

- RFC 2463 ICMPv6
- RFC 2464 MIB for IPv6 – ICMPv6
- RFC 2526 Reserved IPv6 Anycast
- RFC 2553 Socket Interface
- RFC 3315 DHCPv6 (client and relay)
- RFC 3484 Default Address Selection
- RFC 3513 IPv6 Addressing Architecture
- RFC 3542 Advanced Sockets API
- RFC 3587 IPv6 Global Unicast Address
- RFC 3596 DNS Extension for IPv6
- RFC 4193 IPv6 Unicast Addresses
- RFC 4443 ICMPv6
- RFC 4541 IGMP & MLD Snooping Switch
- RFC 4861 IPv6 Neighbor Discovery
- RFC 4862 IPv6 Add Autoconfiguration
- RFC 5095 Depprecation of Type 0

- Traslación de direcciones: Debe cumplir:
  - NAT muchos a uno
  - NAT uno a uno
  - Conexión con APs en oficinas remotas donde se haya realizado traslación de direcciones
- Cifrado de datos y VPNs: Debe cumplir los siguientes estándares de la industria:
  - Certificate and Certificate Revocation List (CRL) Profile
  - RFC 1829 The ESP DES-CBC Transform
  - RFC 2403 HMAC - DM5 within ESP and AH
  - RFC 2404 HMAC SHA within ESP and AH
  - RFC 2405 ESP DES – CBC

- RFC 2407 Interpretation for ISAKMP
- RFC 2451 ESP CBC – Mode Cipher
- RFC 3280 Internet X.509 Public Key
- RFC 3602 the AES – CBC Cipher Algorithm
- RFC 3748 EAP

- Administración de red: debe soportar:
  - SNMP v1
  - SNMP v2c
  - SNMP v3
- Montaje: Debe incluir todos los accesorios para montaje y operación en rack estándar de 19"
- Alimentación eléctrica: el equipo debe soportar una alimentación en AC de 100 VAC a 240 VAC con 50Hz a 60Hz. El consumo máximo no debe ser superior a 90w
- Normativas: Debe cumplir con:
  - UL 60950-1
  - CAN/CSA 22.2 No. 60950-1
  - IEC 60950-1
  - EN 60950-1
  - FDA 21 CFR Subchapter J
  - EN 55022 Class A
  - ICES – 003 Class A
  - CISPR 22 Class A
  - AS/NZS CISPR 22 Class A
  - EN 61000 – 3 – 2
  - EN 61000 – 3 -3
  - VCCI – 3 Class A
  - VCCI – 4 Class A
  - ETSI EN 300 386
  - FCC part 15 (CFR 47) Class A

1.1.4. **Renglón 4:** Plataforma de seguridad de protección de redes
Cantidad: 1 (una)

Se solicita una solución de protección de redes para la seguridad de la información perimetral. Debe consistir en un appliance virtual de seguridad de red con funcionalidades de Next Generation Firewall (NGFW), y consola de administración y monitoreo. Por funcionalidades de NGFW se entienden: reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.

La plataforma debe ser optimizada para análisis de contenido de aplicaciones en Capa 7.

Debe brindar prevención contra amenazas de virus, spyware y malware "Zero Day", proveyendo controles de transmisión de datos y acceso a internet, componiendo una plataforma de seguridad integrada y robusta

El software que ejecuten las funcionalidades de seguridad de red y de administración y monitoreo deben ser de tipo appliance virtual. No serán aceptados equipamientos servidores y sistema operativo de uso genérico; no se aceptarán soluciones UTM

Todos los equipamientos ofrecidos deben ser adecuados para montaje en rack 19"

El software deberá ser ofrecido en su versión más estable y/o más avanzada;

Especificaciones técnicas mínimas:

- Fabricante: Debe estar certificado para IPv6 en Firewall
- Throughput: 4 Gbps con la funcionalidad de control de aplicaciones habilitada para todas las firmas que el fabricante posea; 2 Gbps con las siguientes funcionalidades habilitadas simultáneamente para todas las firmas que la plataforma de seguridad posea debidamente activadas y actuando: control de aplicaciones, IPS, Antivirus y Antispyware, en el mayor nivel de

seguridad posible, con log y NAT habilitados medidos por lo menos con 100 reglas de seguridad habilitadas;

- Conexiones simultáneas: debe soportar 800.000, con todos los módulos de seguridad de capa 7 habilitados simultáneamente, en el mayor nivel de seguridad posible;
- Nuevas conexiones: debe soportar 30.000 por segundo;
- Ruteadores virtuales: debe soportar 10 (diez)
- Zonas de seguridad: debe soportar 40 (cuarenta)
- La solución no tiene que tener limitante por licencia del espacio posible de disco rígido a asignarle para el almacenamiento de logs y reportes, o bien de tener una limitante se debe licenciar en la capacidad máxima posible.
- Estar licenciada para soportar sin uso de licenciamiento, 2.000 (dos mil) clientes de VPN SSL simultáneos;
- Estar licenciada para soportar sin uso de licenciamiento, 2.000 (dos mil) túneles de VPN IPSEC simultáneos;
- Hipervisores: debe soportar VMWare ESXi, VMWare NSX y Microsoft Azure. Deberá ser capaz de integrarse a provisionamiento de sistemas basados VMWare ESXi o Vcenter para leer servidores activos; como se esta buscando un NGFW para interactuar con VMWare, debe existir algun documento escrito por el fabricante del hipervisor (VMWare) que recomienda la utilización del fabricante de seguridad con el hipervisor dado, para garantizar el correcto funcionamiento e integración de la solución de seguridad con el hipervisor
- La consola de administración y monitoreo puede residir en el mismo NGFW de seguridad de red, siempre y cuando posea recurso de CPU, memoria, interfaz de red y sistema operacional dedicados para esta función separados a los procesadores, memoria e interface de red dedicados al procesamiento de seguridad del tráfico de red;
- A efectos de la propuesta, ninguno de los modelos ofertados podrá estar listados en el site del fabricante como listas de end-of-life y end-of-sale.
- Los dispositivos de seguridad de red deben poseer por lo menos las siguientes funcionalidades:
    - Soporte a 4000 VLAN Tags 802.1q;
    - Agregación de links 802.3ad;
    - Policy based routing o policy based forwarding;

- Ruteo multicast (PIM-SM);
- DHCP Relay;
- DHCP Server;
- Jumbo Frames;
- Soporte a creación de objetos de red que puedan ser utilizados como dirección IP de interfaces L3;

- Debe soportar sub-interfaces ethernet lógicas.
- Debe soportar los siguientes tipos de NAT:
  - Nat dinamico (Many-to-1);
  - Nat dinámico (Many-to-Many);
  - Nat estático (1-to-1);
  - NAT estático (Many-to-Many);
  - Nat estático bidireccional 1-to-1;
  - Traducción de porta (PAT);
  - NAT de Origen;
  - NAT de Destino;
  - Soportar NAT de Origen y NAT de Destino simultáneamente;
- Debe enviar log para sistemas de monitoreo externos, simultáneamente;
- Debe tener la opción de enviar logs para los sistemas de monitoreo externos vía protocolo TCP y SSL;
- Debe permitir configurar certificado caso necesario para autenticación del sistema de monitoreo externo de logs;
- Seguridad contra anti-spoofing;
- Para IPv4, debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2);
- Debe soportar MP-BGP
- Para IPv6, debe soportar enrutamiento estático y dinámico (OSPFv3);
- Soportar OSPF graceful restart;
- Debe ser capaz de balancear varios enlaces de internet sin el uso de políticas específicas, permitiendo aplicar una variedad de algoritmos distintos (round Robin, weighted...)
- Soportar BFD (bidirectional forward detection)
- Soportar LACP/LLDP Pre-negotiation

- Soportar como mínimo las siguientes funcionalidades en IPv6: SLAAC (address auto configuration), NAT64, Identificación de usuarios a partir de LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Reglas de seguridad contra DoS (Denial of Service), Desencripción SSL y SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Activo/Activo, Activo/Pasivo, SNMP, NTP, NTP autenticado, SYSLOG, DNS y control de aplicaciones;
- Los dispositivos de seguridad deben tener la capacidad de operar de forma simultanea mediante el uso de sus interfaces físicas en los siguientes modos: Modo sniffer (monitoreo y análisis del tráfico de red), Capa 2 (l2) y Capa 3 (l3);
    - Modo Sniffer, para inspección vía puerto espejo del tráfico de datos de la red;
    - Modo Capa – 2 (L2), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación;
    - Modo Capa – 3 (L3), para inspección de datos en línea y tener visibilidad del control del tráfico en nivel de aplicación operando como default Gateway de las redes protegidas;
    - Modo mixto de trabajo Sniffer, L2 e L3 en diferentes interfaces de red;
- Debe soportar configuración de alta disponibilidad Activo/Pasivo e Activo/Activo: en modo transparente, en layer 3;
- La configuración en alta disponibilidad debe sincronizar:
    - Sesiones;
    - Configuraciones, incluyendo, más no limitado a políticas de Firewall, NAT, QOS y objetos de red;
    - Certificados de descripción;
    - Asociaciones de Seguridad de las VPNs;
    - Tablas FIB;
    - El HA (modo de Alta-Disponibilidad) debe posibilitar monitoreo de fallo de link.
- Las funcionalidades de control de aplicaciones, VPN IPSec y SSL, QOS, SSL y SSH Decryption y protocolos de enrutamiento dinámico deben operar en carácter permanente, pudiendo ser utilizadas por tiempo

indeterminado, incluso si no existe derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.

- Debe poder inspeccionar protocolos como:
  - GRE
  - IPSEC no encriptado (NULL o AH)
  - GPRS para GTP-U
- Control de Política de Firewall: Deba cumplir las siguientes funciones:
  - Deberá soportar controles por zona de seguridad
  - Controles de políticas por puerto y protocolo.
  - Control de políticas por aplicaciones grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (basados en características y comportamiento de las aplicaciones) y categorías de aplicaciones.
  - Control de políticas por usuarios, grupos de usuarios, IPs, redes y zonas de seguridad.
  - Control de políticas por código de País (Por ejemplo: BR, USA, UK, RUS).
  - Control, inspección y desencripción de SSL por política para tráfico de entrada (Inbound) y Salida (Outbound).
  - Offload de certificado en inspección de conexiones SSL de entrada (Inbound);
  - Capacidad de Desencripción de SSL de al menos 15.000 sesiones simultáneas.
  - Desencriptar tráfico Inbound y Outbound en conexiones negociadas con TLS 1.2;
  - Debe desencriptar tráfico que use certificados ECC (como ECDSA)
  - Control de inspección y desencripción de SSH por política;
  - La plataforma de seguridad debe implementar copia del tráfico desencriptado (SSL y TLS) para soluciones externas de análisis (Forense de red, DLP, Análisis de Amenazas, entre otras);
  - Bloqueos de los siguientes tipos de archivos: bat, cab, dll, exe, pif, y reg
  - Traffic shaping QoS basado en políticas (Prioridad, Garantía y Máximo)

- QoS basado en políticas para marcación de paquetes (diffserv marking), inclusive por aplicaciones.
- Soporte a objetos y Reglas IPV6.
- Soporte a objetos y Reglas multicast.
- Soportar los atributos de agendamiento de las políticas con el objetivo de habilitar y deshabilitar políticas en horarios predefinidos automáticamente.

- Control de Aplicaciones: Los dispositivos de seguridad de red deberán poseer la capacidad de reconocer aplicaciones, independiente del puerto y protocolo, con las siguientes funcionalidades:
  - Debe ser posible la liberación y bloqueo solamente de aplicaciones sin la necesidad de liberación de puertos y protocolos.
  - Reconocer por lo menos 2.000 aplicaciones diferentes, incluyendo, mas no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, voip, audio, vídeo, proxy, mensajería instantánea, compartición de archivos, e-mail;
  - Reconocer por lo menos las siguientes aplicaciones: Bittorrent, Gnutella, Skype, Facebook, Linked-in, Twitter, Citrix, Logmein, Teamviewer, Ms-rdp, Vnc, Gmail, Youtube, Http-proxy, Http-tunnel, Facebook chat, Gmail chat, Whatsapp, 4shared, Dropbox, Google drive, Skydrive, Db2, Mysql, racle, Active Directory, Kerberos, Ldap, Radius, Itunes, Dhcp, Ftp, Dns, Wins, Msrpc, Ntp, Snmp, Rpc over http, Gotomeeting, Webex, Evernote, Google-docs, etc;
  - Debe inspeccionar el payload del paquete de datos con el objetivo de detectar a través de expresiones regulares firmas de aplicaciones conocidas por los fabricantes independiente del puerto y protocolo. El chequeo de firmas también debe determinar si una aplicación está utilizando su puerto default o no, incluyendo, más no limitando a RDP en el puerto 80 en vez del 389;
  - Debe aplicar análisis heurístico a fin de detectar aplicaciones a través de análisis comportamental del tráfico observado, incluyendo, más no limitado a Encrypted Bittorrent y aplicaciones VOIP que utilizan criptografía propietaria;

- Identificar el uso de tácticas evasivas, o sea, debe tener la capacidad de visualizar y controlar las aplicaciones y los ataques que utilizan tácticas evasivas vía comunicaciones criptografiadas, tales como Skype y ataques mediante el puerto 443.
- Para tráfico criptografiado (SSL y SSH), debe soportar desencripción paquetes con el fin de posibilitar la lectura del payload para chequeo de firmas de aplicaciones conocidas por el fabricante;
- Debe realizar decodificación de protocolos con el objetivo de detectar aplicaciones encapsuladas dentro del protocolo y validar si el tráfico corresponde con la especificación del protocolo, incluyendo, mas no limitado a Yahoo! Instant Messenger usando HTTP. La decodificación de protocolo también debe identificar funcionalidades específicas dentro de una aplicación, incluyendo, más no limitado a la compartición de archivos dentro de Webex. También debe detectar el archivo y otros contenidos que deben ser inspeccionados de acuerdo a las Reglas de seguridad implementadas;
- Debe Identificar el uso de tácticas evasivas vía comunicaciones criptografiadas;
- Debe actualizar la base de firmas de aplicaciones automáticamente;
- Deberá incluir la capacidad de creación de políticas basadas en el control por aplicación, por categoría de aplicación, subcategoría de aplicación, tecnología y factor de riesgo;
- La tecnología de identificación de aplicaciones deberá estar habilitada por default (motor de inspección base) sin necesidad de habilitar funcionalidades adicionales;
- Debe Reconocer aplicaciones en IPv6;
- Limitar el ancho de banda (download/upload) usado por aplicaciones (traffic shaping), basado en IP de origen, usuarios y grupos del LDAP/AD;
- Los dispositivos de seguridad de red deben poseer la capacidad de identificar al usuario de red con integración al Microsoft Active

Directory, sin la necesidad de instalación de agente en el Domain Controller, ni en las estaciones de los usuarios;

- Debe ser posible adicionar control de aplicaciones en todas las Reglas de seguridad del dispositivo, o sea, no limitándose solamente a la posibilidad de habilitar control de aplicaciones en algunas Reglas;
- Debe soportar múltiples métodos de identificación y clasificación de las aplicaciones, por lo menos chequeo de firmas, decodificación de protocolos y análisis heurístico;
- Para mantener la seguridad de la red eficiente, debe soportar el control sobre aplicaciones desconocidas y no solamente sobre aplicaciones conocidas;
- Permitir nativamente la creación de firmas personalizadas para reconocimiento de aplicaciones propietarias en la propia interface gráfica de la solución, sin la necesidad de acción por parte del fabricante, manteniendo la confidencialidad de las aplicaciones del órgano;
- La creación de firmas personalizadas debe permitir el uso de expresiones regulares, contexto (sesiones o transacciones), usando la posición en el payload de los paquetes TCP y UDP y usando decoders de por lo menos los siguientes protocolos:
- HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP y File body.
- El fabricante debe permitir la solicitud de inclusión de aplicaciones en la base de firmas de aplicaciones;
- Debe alertar al usuario cuando una aplicación sea bloqueada
- Debe posibilitar que el control de puertos sea aplicado para todas las aplicaciones;
- Debe posibilitar la diferenciación de tráficos Peer2Peer (Bittorrent, Emule, Neonet, etc.) proveyendo granularidad de control/políticas para los mismos;
- Debe posibilitar la diferenciación de tráficos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) proveyendo granularidad de control/políticas para los mismos;

- Debe posibilitar la diferenciación y control de partes de las aplicaciones como por ejemplo permitir Gtalk chat;
- Debe posibilitar a diferenciación de aplicaciones Proxies (ghostsurf, freegate, etc.) proveyendo granularidad de control/políticas para los mismos;
- Debe ser posible la creación de grupos estáticos de aplicaciones y grupos dinámicos de aplicaciones basados en características de las aplicaciones como:
- Tecnología utilizada en las aplicaciones (Client-Server, Browse Based, Network Protocol, etc).
- Nivel de riesgo de las aplicaciones.
- Categoría y sub-categoría de aplicaciones.
- Aplicaciones que usen técnicas evasivas, utilizadas por malware, como transferencia de archivos y/o uso excesivo de ancho de banda, etc.
- Debe poder monitorear aplicaciones SaaS (Software as a service) tanto vía GUI como en reporte predefinido

- Prevención de amenazas: Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS, Antivirus y Anti-Spyware integrados en el propio appliance virtual de NG-Firewall
  - Debe incluir firmas de prevención de intrusos (IPS) y bloqueo de archivos maliciosos (Antivirus y Anti-Spyware);
  - Las funcionalidades de IPS, Antivirus y Anti-Spyware deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones o que no haya contrato de garantía de software con el fabricante.
  - Debe sincronizar las firmas de IPS, Antivirus, Anti-Spyware cuando esté implementado en alta disponibilidad Activo/Activo e Activo/pasivo;
  - Cuando se utilicen las funciones de IPS, Antivirus y Anti-spyware, el equipamiento debe entregar el mismo performance (no degradar) entre tener una única firma de IPS habilitada o tener

todas las firmas de IPS, Anti-Vírus y Antispyware habilitadas simultáneamente.

- Las firmas deben poder ser activadas o desactivadas, o incluso habilitadas apenas en modo de monitoreo;
- Excenciones por IP de origen o de destino deben ser posibles en las Reglas, de forma general y firma a firma;
- Debe soportar granularidad en las políticas de IPS Antivirus y Anti-Spyware, permitiendo la creación de diferentes políticas por zona de seguridad, dirección de origen, dirección de destino, servicio y la combinación de todos esos ítems.
- Debe permitir el bloqueo de vulnerabilidades y de exploits conocidos.
- Debe incluir seguridad contra ataques de negación de servicios.
- Deberá poseer los siguientes mecanismos de inspección de IPS:
- Análisis de patrones de estado de conexiones;
- Análisis de decodificación de protocolo;
- Análisis para detección de anomalías de protocolo;
- Análisis heurístico;
- IP Defragmentation;
- Re ensamblado de paquetes de TCP;
- Bloqueo de paquetes malformados.
- Ser inmune y capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
- Detectar y bloquear el origen de portscans;
- Bloquear ataques efectuados por worms conocidos, permitiendo al administrador adicionar nuevos patrones;
- Soportar los siguientes mecanismos de inspección contra amenazas de red: análisis de patrones de estado de conexiones, análisis de decodificación de protocolo, análisis para detección de anomalías de protocolo, análisis heurístico, IP Defragmentation, re ensamblado de paquetes de TCP y bloqueo de paquetes malformados;
- Debe poseer firmas específicas para la mitigación de ataques DoS;

- Debe poseer firmas para bloqueo de ataques de buffer overflow;
- Debe poseer firmas de C2 (Comando y control) generadas de forma automática.
- Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- Permitir el bloqueo de virus y spyware en, por lo menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- Soportar bloqueo de archivos por tipo;
- Identificar y bloquear comunicaciones como botnets;
- Debe soportar varias técnicas de prevención, incluyendo Drop y tcp-rst (Cliente, Servidor y ambos);
- Debe soportar referencia cruzada como CVE;
- Debe registrar en la consola de monitoreo las siguientes informaciones sobre amenazas identificadas:
- Debe soportar la captura de paquetes (PCAP), por firma de IPS y Antispyware;
- Debe permitir que en la captura de paquetes por firmas de IPS y Antispyware sea definido el número de paquetes a ser capturados. Esta captura debe permitir seleccionar, como mínimo, 50 paquetes;
- Debe poseer la función resolución de direcciones vía DNS, para que conexiones como destino a dominios maliciosos sean resueltas por el Firewall como direcciones (IPv4 e IPv6), previamente definidos;
- Permitir el bloqueo de virus, por al menos, los siguientes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- Los eventos deben identificar el país de donde partió la amenaza;
- Debe incluir seguridad contra virus en contenido HTML y JavaScript, software espía (spyware) y worms.
- Seguridad contra downloads involuntarios usando HTTP de archivos ejecutables. maliciosos.
- Debe permitir el rastreo de virus en pdf.

- Debe permitir la inspección en archivos comprimidos que utilizan algoritmo deflate (zip, gzip, etc.)
- Debe ser posible la configuración de diferentes políticas de control de amenazas y ataques basados en políticas del firewall considerando usuarios, grupos de usuarios, origen, destino, zonas de seguridad, etc, es decir que, cada política de firewall podrá tener una configuración diferente de IPS, siendo esas políticas por Usuarios, Grupos de usuario, origen, destino, zonas de seguridad.
- Debe soportar controles automatizados y grupos dinámicos de IP de origen o destino.
- Se tiene que poder asignar de manera automática etiquetas a una IP de origen (o destino) cuando se genera un log en el firewall (ejemplo log de amenazas, reglas de firewall, URL, etc o bien una combinación de las mismas) para luego poder utilizar esas etiquetas en grupos dinámicos para otras políticas para lograr de esta manera asignar controles dinámicos. Ejemplo: Si la correlación de eventos indica que un equipo ha sido comprometido y es parte de una botnet, se le aplicaría una etiqueta asociada a la IP del equipo y ese grupo dinámico se aplicara a una política para evitar que ese equipo pueda acceder a redes protegidas y de esta manera mitigar el incidente.

- Análisis de Malware Moderno: Debe poseer la capacidad de análisis de amenazas y malware no conocidas. Debe ser capaz de enviar archivos transferidos de forma automática para análisis "In Cloud" o local, donde el archivo será ejecutado y simulado en un ambiente controlado;
  - Seleccionar a través de la política de Firewall que tipos de archivos sufrirán este análisis;
  - Debe soportar el análisis como por lo menos 60 (sesenta) tipos de comportamientos maliciosos para el análisis de la amenaza no conocida;
  - Debe soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, con sistema operativo Windows XP y Windows 7;

- Debe soportar el monitoreo de archivos transferidos por internet (HTTP, FTP, HTTP, SMTP) como también archivos transferidos internamente en los servidores de archivos usando SMB;
- El sistema de análisis "In Cloud" o local debe proveer informaciones sobre las acciones del Malware en la máquina infectada, informaciones sobre cuáles aplicaciones son utilizadas para causar/propagar la infección, detectar aplicaciones no confiables utilizadas por el Malware, generar firmas de Antivirus y Anti-spyware automáticamente, definir URLs no confiables utilizadas por el nuevo Malware y proveer informaciones sobre el usuario infectado (su dirección IP y su login de red); debe emitir relación para identificar cuáles soluciones de antivirus existentes en el mercado poseen firmas para bloquear el malware;
- Debe permitir exportar el resultado de los análisis de malware de día Zero en PDF y CSV a partir de la propia interfaz de administración;
- Debe permitir la descarga de los malware identificados a partir de la propia interfaz de administración; permitir visualizar los resultados de los análisis de malware de día Zero en los diferentes sistemas operacionales soportados; permitir informar al fabricante cuando haya una sospecha de falso-positivo y falso-negativo en el análisis de malware de día Zero a partir de la propia interfaz de administración.
- Debe soportar el análisis de archivos ejecutables, DLLs, ZIP y encriptados en SSL en el ambiente controlado;
- Soportar el análisis de archivos del paquete office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), archivos java (.jar e class), email link, flash, archivos de MacOSX (mach-o, dmg, pkg) y Android APKs en el ambiente controlado;
- Debe poseer SLA de, como máximo, 5 minutos para actualización de la base de vacunas contra malware desconocidos identificados en el ambiente controlado;
- Debe permitir el envío de archivos para análisis en el ambiente controlado vía web y de forma automática vía API.

- Debe poder dar veredictos distintos: Malicioso, Grayware, Benigno, Phising
- En caso de detectar una forma de evasión de máquina virtual, debe poder enviar de forma automática a revisión en modo Bare Metal (máquinas físicas)

- Filtro de URL: La plataforma de seguridad debe poseer las siguientes funcionalidades de filtro de URL:
  - Especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
  - Crear políticas por usuario, grupo de usuario, IPs, redes y zonas de seguridad
  - Incluir la capacidad de creación de políticas basadas en la visibilidad y contra de quien está utilizando cuál URLs a través de la integración con servicios de directorio, autenticación vía LDAP, Active Directory, E-Directory y base de datos local
  - Permitir poder publicar los logs de URL con la información de los usuarios conforme a lo descrito en la integración con servicios de directorio
  - Soportar la capacidad de crear políticas basadas en control por URL y categoría URL
  - Bloquear el acceso a sitios de búsqueda (Google, Bing y Yahoo!) en el caso de que la opción de Safe Search este deshabilitada. Debe en ese caso exhibir una página de bloqueo dando instrucciones al usuario de como habilitar dicha función
  - Soportar una caché local de URL en el appliance virtual, evitando el delay de comunicación/validación de las URLs
  - Poseer al menos 60 categorías de URLs
  - Soportar la creación de categorías URL custom
  - Soportar la exclusión de URLs del bloqueo por categoría
  - Permitir la customización de la página de bloqueo
  - Permitir o bloquear y continuar (habilitando que el usuario acceso a un sitio potencialmente bloqueado informándole del bloqueo y habilitando el botón de "continuar" para permitirle seguir a ese site)

- Soportar la inclusión de los logs del producto de las informaciones de las actividades de los usuarios
- La solución debe evitar la fuga de credenciales internas (usuarios y passwords) desde o hacia diferentes categorías de sitios (ejemplo: phising, malware, otros , etc) pudiendo seleccionar el administrador a qué categorías de páginas se le permite a los usuarios pasar credenciales internas y cuál no. Incluso se debe poder gestionar el uso indebido de los mismos dentro de la red del cliente.
- Actualizar de forma automática en 5 minutos o menos las categorías de malware y phising.

- Identificación de Usuarios: Debe incluir las siguientes funcionalidades:
  - Capacidad de creación de políticas basadas en la visibilidad y control de quién está utilizando qué aplicaciones a través de la integración como servicios de directorio, autenticación vía ldap, Active Directory, E-directory y base de datos local.
  - Integración con Microsoft Active Directory para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
  - Integración con Radius para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en usuarios y grupos de usuarios.
  - Integración con TACACS+
  - Integración con Ldap para identificación de usuarios y grupos permitiendo la granularidad de control/políticas basadas en Usuarios y Grupos de usuarios.
  - Debe soportar la recepción de eventos de autenticación de controladoras Wireless, dispositivos 802.1x y soluciones NAC vía syslog, para la identificación de direcciones IP y usuarios
  - Debe permitir el control, sin instalación de cliente de software, en equipamientos que soliciten salida a internet para que antes de iniciar la navegación, se muestre un portal de autenticación residente en el firewall (Captive Portal).
  - Soporte a autenticación Kerberos.
  - Soporte SAML 2.0

- Debe soportar múltiples factores de autenticación (como por ejemplo usuario y password + 2FA hard token + 2FA soft token + portal cautivo)
- Debe soportar políticas para multiples factores de autentificación, para poder lograr que a determinadas aplicaciones criticas o dependiendo desde donde se acceden a la misma (ejempo red, host, rango o zona de origen) se le solicite al usuario multiples factores de autentificación.
- Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en ambientes Citrix y Microsoft Terminal Server, permitiendo visibilidad y control granular por usuario sobre el uso de las aplicaciones que tiene estos servicios
- Debe poseer Soporte a identificación de múltiples usuarios conectados en una misma dirección IP en servidores accedidos remotamente, incluso que no sean servidores Windows.

- QoS: Como la finalidad es controlar aplicaciones y tráfico cuyo consumo pueda ser excesivo, y tener un alto consumo de ancho de banda, se requiere que la solución, a la vez de poder permitir o negar ejecutar aplicaciones que consuman alto ancho de bandad; debe tener la capacidad de controlarlas por políticas de máximo de ancho de banda cuando fuesen solicitadas por diferentes usuarios o aplicaciones, tanto de audio como de vídeo streaming.
- Debe soportar la creación de políticas de QoS por:
  - ✓ Dirección de origen
  - ✓ Dirección de destino
  - ✓ Por usuario y grupo de LDAP/AD.
  - ✓ Por aplicaciones, incluyendo, más no limitando a Skype, Bittorrent, YouTube y Azureus;
  - ✓ Por puerto;
- El QoS debe permitir la definición de clases por:
  - ✓ Ancho de Banda garantizado
  - ✓ Ancho de Banda Máximo
  - ✓ Cola de prioridad.

- Soportar priorización Real Time de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP y aplicaciones como Skype.
- Soportar marcación de paquetes Diffserv, inclusive por aplicaciones;
- Disponer de estadísticas Real Time para clases de QoS.
- Permitir el monitoreo del uso que las aplicaciones hacen por bytes, sesiones y por usuario.

- Filtro de Datos: Debe cumplir con las siguientes funcionalidades:
- Creación de filtros para archivos y datos predefinidos;
- Los archivos deben ser identificados por extensión y firmas;
- Identificar y opcionalmente prevenir la transferencia de varios tipos de archivos (MS Office, PDF, etc) identificados sobre aplicaciones (P2P, InstantMessaging, SMB, etc);
- Soportar la identificación de archivos compactados y las aplicaciones de políticas sobre el contenido de esos tipos de archivos;
- Identificar y, opcionalmente, prevenir la transferencia de informaciones sensibles, permitiendo la creación de nuevos tipos de datos vía expresión regular;
- Listar el número de aplicaciones soportadas para control de datos;
- Listar el número de tipos de archivos soportados para el control de datos;
- Poder integrarse son soluciones de punto final de terceros para mejorar la política de DLP.
- Traer por defecto al menos dos perfiles de bloqueo predefinidos.

- Geolocalización: Debe cumplir con las siguientes funcionalidades:
- Soportar la creación de políticas por Geo localización, permitiendo que el tráfico de determinado País/Países sean bloqueados.
- Posibilitar la visualización de los países de origen y destino en los logs de acceso.
- Posibilitar la creación de regiones geográficas desde la interfaz gráfica y crear políticas utilizando las mismas.

- VPN:
- Soportar VPN Site-to-Site y Cliente-To-Site;
- Soportar IPSec VPN;
- Soportar SSL VPN;
- La VPN IPSEc debe soportar:
    - ✓ DES y 3DES;
    - ✓ Autenticación MD5 e SHA-1;
    - ✓ Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
    - ✓ Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
    - ✓ AES 128, 192 e 256 (Advanced Encryption Standard)
    - ✓ Debe permitir SSO via Kerberos
    - ✓ Autenticación vía certificado IKE PKI.
    - ✓ Debe ser compatible con la Suite B de protocolos de NSA
- Debe poseer interoperabilidad como los siguientes fabricantes:
    - ✓ Cisco;
    - ✓ Checkpoint;
    - ✓ Juniper;
    - ✓ Palo Alto Networks;
    - ✓ Fortinet;
    - ✓ Sonic Wall
- Las VPN SSL deben soportar las siguientes funcionalidades:
    - ✓ Permitir que el usuario realice la conexión por medio de cliente instalado en el sistema operativo del equipamiento o por medio de interfaz web;
    - ✓ Las funcionalidades de VPN SSL deben ser atendidas con o sin el uso de agente;
    - ✓ La asignación de dirección IP en los clientes remotos de VPN;
    - ✓ La asignación de DNS en los clientes remotos de VPN;
    - ✓ Debe tener la opción de ocultar el agente de VPN instalado en el cliente remoto, tornando el mismo invisible para el usuario;
    - ✓ Deber permitir crear políticas de control de aplicaciones, IPS, Antivirus, Antispyware para tráfico de los clientes remotos conectados en la VPN SSL;

- ✓ Las VPN SSL deben soportar proxy arp y el uso de interfaces PPPOE;
- ✓ Soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local;
- ✓ Permite establecer un túnel VPN client-to-site del cliente a la plataforma de seguridad, proveyendo una solución de single-sign-on a los usuarios, integrándose como las herramientas de Windows-logon;
- ✓ Soporte de lectura y verificación de CRL (certificate revocation list);
- ✓ Permite la aplicación de políticas de seguridad y visibilidades para las aplicaciones que circulan dentro de los túneles SSL;
- ✓ El agente de VPN a ser instalado en los equipamientos desktop y laptops, debe ser capaz de ser distribuido de manera automática vía Microsoft SMS, Active Directory y ser descargado directamente desde su propio portal, en el cual residirá el centralizador de VPN;
- ✓ El agente deberá comunicarse con el portal para determinar las políticas de seguridad del usuario,
- ✓ Debe permitir que las conexiones como VPN SSL sean establecidas de las siguientes formas:
  - Antes del usuario autenticarse en la estación;
  - Después de la autenticación del usuario en la estación;
  - Bajo demanda del usuario;
- ✓ Deberá mantener una conexión segura con el portal durante la sesión.
- ✓ El agente de VPN SSL client-to-site debe ser compatible al menos con: Windows XP, Vista, Windows 7, Windows 8, Windows 10, MacOS X;
- ✓ El portal de VPN debe enviar al cliente remoto la lista de gateways VPN activos para el establecimiento de la conexión, los cuales deben poder ser administrados de manera centralizada

- ✓ Debe haber una opción en el cliente remoto de escoger manualmente el Gateway de VPN y de forma automática a través de la mejor respuesta entre los gateways disponibles con base al más rápido.
- ✓ Debe poseer la capacidad de identificar el origen de conexión de VPN si es interna o externa

- Consola de Administración y Monitoreo:
  - La administración de la solución debe soportar acceso vía SSH, cliente WEB (HTTPS) y API abierta;
  - En el caso de que sea necesaria la instalación de cliente para administración de la solución, el mismo debe ser compatible con los sistemas operativos Windows y Linux;
  - La administración debe permitir/hacer:
    - ✓ Creación y administración de políticas de firewall y control de aplicaciones;
    - ✓ Creación y administración de políticas de IPS y Anti-Spyware;
    - ✓ Creación y administración de políticas de filtro de URL
    - ✓ Monitoreo de logs;
    - ✓ Herramientas de investigación de logs;
    - ✓ Debugging;
    - ✓ Captura de paquetes.
    - ✓ El acceso concurrente de administradores;
    - ✓ Tener un mecanismo de búsqueda de comandos de administración vía SSH, facilitando la localización de los comandos;
    - ✓ Utilizar palabras clave y distintos tags de colores para facilitar la identificación de Reglas;
    - ✓ Monitorear vía SNMP fallas en el hardware, inserción o remoción de fuentes, discos y ventiladores, uso de recursos por número elevado de sesiones, número de túneles establecidos de VPN cliente-to-site, porcentaje de utilización en referencia al número total soportado/licenciado y número de sesiones establecidas;

- ✓ El bloqueo de alteraciones, en el caso de acceso simultáneo de dos o más administradores;
- ✓ La definición de perfiles de acceso a la consola con permisos granulares como: acceso de escritura, acceso de lectura, creación de usuarios, alteración de configuraciones;
- ✓ La autenticación integrada con Microsoft Active Directory y servidor Radius;
- ✓ La localización de dónde están siendo utilizados objetos en: Reglas, dirección IP, Rango de IPs, subredes u objetos
- ✓ Atribuir secuencialmente un número a cada regla de firewall, NAT, QOS y Reglas de DOS;
- ✓ La creación de Reglas que estén activas en un horario definido;
- ✓ La creación de Reglas con fecha de expiración;
- ✓ Realizar un backup de las configuraciones y rollback de configuración para la última configuración salvada;
- ✓ Soportar el Rollback de Sistema operativo para la última versión local;
- ✓ Poseer la habilidad del upgrade vía SCP, TFTP e interfaz de administración;
- ✓ Validar las Reglas antes de las aplicaciones;
- ✓ Validación de las políticas, avisando cuando haya Reglas que ofusquen o tengan conflicto con otras (shadowing);
- ✓ La visualización y comparación de configuraciones actuales, la configuración anterior y configuraciones más antiguas.
- ✓ La integración con otras soluciones de SIEM del mercado (third-party SIEM vendors)
- ✓ La generación de logs de auditoría detallados, informando de la configuración realizada, el administrador que la realizo y el horario de la alteración;
- ✓ Tener la capacidad de generar un gráfico que permita visualizar los cambios en la utilización de aplicaciones en la red en lo que se refiere a un período de tiempo anterior, para

permitir comparar los diferentes consumos realizados por las aplicaciones en el tiempo presente con relación al pasado;

- ✓ La generación de mapas geográficos en tiempo real para la visualización de orígenes y destinos del tráfico generado en la institución;
- ✓ Proveer resúmenes con la vista correlacionada de aplicaciones, amenazas (IPS, Antispyware) URLs y filtro de archivos, para un mejor diagnóstico y respuesta a incidentes;
- ✓ La administración de la solución debe posibilitar la recolección de estadísticas de todo el tráfico que pasa por los dispositivos de seguridad;
- ✓ Proveer resúmenes de utilización de los recursos por aplicaciones, amenazas (IPS, Anti-Spyware y antivirus de la solución), etc;
- ✓ Proveer una visualización sumarizada de todas las aplicaciones, amenazas (IPS, Antivirus e Anti-Spyware) y URLs que pasan por la solución;
- ✓ Poseer un mecanismo "Drill-Down" para navegación por los resúmenes en tiempo real;
- ✓ En las listas de "Drill-Down", debe ser posible identificar el usuario que ha determinado el acceso;
- ✓ Exportar los logs en CSV;
- ✓ Acceder al equipamiento a aplicar configuraciones durante momentos donde el tráfico sea muy alto y la CPU y memoria del equipamiento este siendo totalmente utilizada.
- ✓ Tener rotación de logs;
- ✓ Tener presentaciones de las siguientes informaciones, de forma histórica y en tiempo real (actualizado de forma automática y continua cada 1 minuto):
- ✓ Mostrar la situación del dispositivo y del cluster;
- ✓ Mostrar las principales aplicaciones;
- ✓ Mostrar las principales aplicaciones por riesgo;
- ✓ Mostrar los administradores autenticados en la plataforma de seguridad;

- ✓ Mostrar el número de sesiones simultáneas;
- ✓ Mostrar el estado de las interfaces;
- ✓ Mostrar el uso de CPU;

- Generación de reportes. Deben poder ser generados los siguientes reportes:
  - ✓ Resumen gráfico de las aplicaciones utilizadas;
  - ✓ Principales aplicaciones por utilización de ancho de banda de entrada y salida;
  - ✓ Principales aplicaciones por tasa de transferencia en bytes;
  - ✓ Principales hosts por número de amenazas identificadas;
  - ✓ Actividades de un usuario específico y grupo de usuarios del AD/LDAP, incluyendo aplicaciones accedidas y amenazas (IPS, y Anti-Spyware), de red vinculadas a este tráfico;
  - ✓ Debe permitir la creación de reportes personalizados;
- Definición de criterios y complejidad mínima para contraseña. Soportar las siguientes capacidades de administración y reportes de los siguientes criterios:
  - ✓ Longitud mínima de contraseña
  - ✓ Número mínimo de mayúsculas
  - ✓ Número mínimo de minúsculas
  - ✓ Número mínimo de caracteres numéricos
  - ✓ Número mínimo de caracteres no alfanuméricos
  - ✓ Prevenir el uso de contraseñas previas
  - ✓ Prevenir el uso de nombre de usuario como contraseña
  - ✓ Advertencia de expiración de contraseña
  - ✓ Forzar el cambio de contraseña en un periodo específico
- En cada criterio de búsqueda del log debe ser posible incluir múltiples entradas (ej. 10 redes e IP's distintas; servicios HTTP, HTTPS y SMTP), excepto en el campo horario, donde debe ser posible definir un rango de tiempo como criterio de búsqueda;
- Generar alertas automáticas vía:
  - ✓ Email;
  - ✓ SNMP;
  - ✓ Syslog;

- La plataforma de seguridad debe permitir a través de API-XML (Application Program Interface) la integración con sistemas existentes en el ambiente de contratación de forma que posibilite que aplicaciones desarrolladas por el cliente puedan interactuar en tiempo real con la solución permitiendo así que Reglas y políticas de seguridad puedan ser modificadas por estas aplicaciones con la utilización de scripts en lenguajes de programación como Perl o PHP.

1.1.5. **Renglón 5:** Instalación y Capacitación

El oferente deberá realizar las tareas de instalación y puesta en marcha coordinando con el Ente las políticas a implementar.

Se deberá realizar una capacitación y transferencia de conocimiento no menor a 12 (doce) horas en nuestras oficinas en la cual se abordarán temas como:

- Configuración inicial
- Políticas básicas
- Configuración avanzada de políticas de firewall de próxima generación
- Otros temas que especifique nuestro organismo.
- Para la capacitación el oferente deberá entregar Manual de Usuario y Manual de Configuración, en formato digital o impreso

2- CONDICIONES PARTICULARES

2.1 VISITA DE RECONOCIMIENTO

El área de cobertura de la solución incluirá la zona de estacionamiento de usuarios, cabinas de peaje y oficinas administrativas del lado Santa Fe y Paraná. Todos los oferentes deberán visitar las instalaciones del Ente Tunel Subfluvial, a efectos de conocer el estado de las mismas, sus servicios y todo otro elemento o información que el Oferente considere prudente tomar conocimiento. Esta visita es OBLIGATORIA y apunta a que el oferente dimensione el alcance del proyecto, cotice todos los elementos y servicios necesarios para una adecuada instalación y puesta en marcha del equipamiento licitado como así también, para el cumplimiento de las tareas de ingeniería solicitadas. Se extenderá un CERTIFICADO DE VISITA que será firmado por el Jefe del Depto de Informática, que deberá ser presentado conjuntamente con la Oferta. La visita podrá realizarse una vez que el Oferente haya adquirido los Pliegos correspondientes y deberá ser coordinada con el Jefe del Departamento Informática.-

2.2 PLAN DE TRABAJO GENERAL:

Deberá contener:

- Cronograma de entrega e instalación del equipamiento
- Cronograma de actividades requeridas para la instalación y configuración del equipamiento y del software.
- Esquema y metodología de soporte post puesta en funcionamiento.

2.3. ANTECEDENTES DEL OFERENTE:

El oferente deberá acreditar al menos 3 (tres) antecedentes demostrables de implementaciones exitosas de tecnología idéntica a la cotizada en la ciudad de Paraná o de Santa Fe.

Presentar carta emitida por la fabricante firmada por su representante en Argentina donde reconocen al participante como un canal autorizado para la venta y soporte de sus productos

2.4. TÉCNICOS Y CAPACITADORES:

El Oferente deberá presentar un listado con el equipo técnico que colaborará en las tareas de instalación, configuración, consultoría y capacitación, con indicación clara de su rol y responsabilidad. Dicho personal debe ser propio y debe estar certificado en la marca que cotizan.-

2.5. DOCUMENTACIÓN:

Adjuntar con la oferta.-

- Catálogos y/o folletos con las especificaciones técnicas, marcas y modelos ofrecidos.-
- Certificado de visita de reconocimiento.-
- Plan de trabajo general.-
- Antecedentes del oferente.-

Adjuntar con la recepción.-

- Manuales en español de los equipos y sus componentes.-
- Licencias de Software.-

2.6. CALIDAD:

Los equipos ofrecidos deberán ser nuevos, de calidad reconocida, tecnología actual y última serie de fabricación.-

Las marcas a cotizar deberán ser las indicadas en el Pliego de Especificaciones Técnicas o de calidad superior.-

El fabricante debe ser reconocido en el mercado; no se aceptarán soluciones opensource o sin el respaldo de un fabricante con presencia mundial.

El fabricante debe estar en el cuadrante de líderes de Gartner para "Enterprise Firewall" o firewalls empresariales en los últimos 3 años. Debe estar certificado para IPv6 en Firewall e IPS por USGv6.

2.7. GARANTIA Y MANTENIMIENTO CORRECTIVO Y PREVENTIVO:

GARANTÍA:

Los equipos deberán garantizarse de fábrica por un período de al menos doce (12) meses, contados a partir de la fecha de instalación de los mismos. El fabricante deberá tener personal técnico oficial o propio, con certificación en todos los productos ofrecidos, residente disponible en ciudad de Paraná o Santa Fe.

La garantía cubrirá íntegramente el servicio técnico de mantenimiento, repuestos, mano de obra, y personal técnico y de ingeniería, y se brindará en el lugar en que se encuentren instalados los equipos. Se debe especificar claramente elementos y daños no cubiertos por la garantía, si los hubiera.

Deberá atender el servicio de mantenimiento preventivo y correctivo durante el período de garantía "on site" en el Ente.

El oferente deberá disponer del personal, las herramientas, equipos de diagnóstico y medición, así como de todos los repuestos nuevos y servicios de ingeniería requeridos para atender el servicio de garantía indicado.

Comenzar a trabajar en la resolución del problema reportado como máximo dentro de las cuatro (4) horas después de efectuado el reclamo.

Resolver los problemas en un período de cuarenta y ocho (48) horas contadas a partir de que se realiza el reclamo.

En caso de ser necesario sustituir algún suministro defectuoso por uno nuevo, la sustitución deberá realizarse en cuarenta y ocho (48) horas como máximo.

MANTENIMIENTO PREVENTIVO Y CORRECTIVO:

El mantenimiento de los equipos debe ser integral (repuestos y mano de obra), debiendo incluir la totalidad de los componentes físicos y drivers, firmware y documentación necesarios para operar el equipo dentro de cualquiera de los sistemas operativos descritos. En caso de sustitución de un componente, el

sustituto debe ser idéntico al retirado o si es distinto (más moderno o de mayores prestaciones) el instalado no debe degradar los niveles de certificación originales ni afectar el desempeño de ninguna de las aplicaciones existentes.

El mantenimiento correctivo se efectuará dentro de los plazos previstos, contados desde el reporte del personal del Depto Informática sobre mal funcionamiento o falla total de alguno de los equipos. El servicio deberá realizarse "on site".

En caso de que por razones de operación de los sistemas, sea necesario realizar tareas fuera del horario de 7:00 a 13:00, las mismas serán coordinadas con anterioridad entre el personal del Depto Informática y la empresa proveedora del servicio, sin generar gastos para el Ente.

En caso de ser necesaria una modificación en la instalación, que la modificación involucre cualquier tipo de cambio para el usuario, aunque esta se entienda por parte del adjudicatario beneficioso, debe ser expresamente autorizada y aceptada por el Ente en forma escrita. Se debe especificar claramente los elementos o daños no cubiertos por el mantenimiento, si los hubiera.

2.8. OFERTA:

Se deberá cotizar con IVA INCLUIDO, condición del Ente ante AFIP, sujeto EXENTO.-

El oferente deberá proponer forma de pago.-

En ningún caso se podrá ofrecer descuentos por pago contra entrega de los equipos en un tiempo menor al de mantenimiento de oferta.-

2.9. FORMA DE COTIZACIÓN:

Se deberá cotizar por renglón y se adjudicará por ítem.-

NOTA: No se considerarán las ofertas que coticen "Según Stock".-

2.10. PLAZO ENTREGA:

Indicar, de lo contrario el mismo será de 45 (cuarenta y cinco) días corridos a partir de la fecha de recepción de la Orden de Compra por parte del adjudicatario.-

2.11. TRANSPORTE:

El transporte, carga y descarga de los equipos, estará a cargo del adjudicatario.-

2.12. PAGO:

El pago se gestionará mediante la presentación de la Factura, emitida por duplicado y confeccionada conforme lo establece la Resolución General N° 1415- de la A.F.I.P, acompañada del acta de recepción que corresponda.-

El plazo para el pago comenzará a contarse a partir de la fecha de recepción de la documentación citada, en Mesa de Entradas del Ente.

El pago se efectivizará en el término de 5(cinco) días hábiles administrativos, posteriores a la gestión de la cumplimentación citada y se efectuará en la tesorería del Ente, sita en Av. Raúl Uranga S/N°, peaje lado Paraná.-

2.13. PRESENTACIÓN DE LAS PROPUESTAS:

Las propuestas deberán ser presentadas en Mesa de Entradas del Ente (Peaje lado Paraná), con anterioridad a la hora de apertura de la Licitación.-

No se considerarán las ofertas presentadas en el acto de apertura.-

El sobre previsto en el Art. 5° del Pliego de Condiciones Generales, no deberá tener signos identificatorios del oferente.-

2.14- GARANTIA DE OFERTA:

En caso de optar el oferente por ofrecer garantía de oferta, según lo normado por el Art. 26°, inciso b) del Pliego de Condiciones Generales, se deberá cumplimentar según el modelo adjunto.-

En caso de existir algún error (no esencial) en la confección del documento, se obliga a subsanarlo dentro del término de cinco (5) días corridos de serle requerido por el Ente.-

<u>Nota:</u> Se adjunta modelo de documentación de garantía, de acuerdo a lo requerido por el Art. 26°, Inciso b).-

2.15. GARANTIA DE ADJUDICACIÓN:

Reformulando el Art. 26°, Inciso b) del Pliego de Condiciones Generales, la Garantía de Adjudicación no podrá constituirse con pagaré a la vista.-

2.16. EVALUACIÓN TÉCNICA DE LAS OFERTAS:

La evaluación técnica se realizará en función de la documentación técnica incluida en la oferta. El Ente se reserva el derecho de solicitar aclaraciones y, la consideración de éstas, **únicamente cuando no contengan agregados que signifiquen modificación de la oferta.-**

2.17. RECEPCIÓN PROVISORIA PARCIAL O TOTAL:

El acta de recepción provisoria se firmará luego de haberse efectuado las verificaciones y controles por parte del personal del Ente, a partir de lo cual entrará en vigencia la obligación de pago por parte del Túnel y luego de ello la Garantía Funcional.-

2.18. RECEPCIÓN DEFINITIVA:

La recepción definitiva tendrá lugar luego de operar el vencimiento de la garantía funcional.-

2.19. VARIABLE DE ADJUDICACIÓN:

El Ente se reserva el derecho de aumentar o disminuir la adjudicación hasta en un 30% del monto total adjudicado a los mismos precios y condiciones.-

2.20. CONSTITUCIÓN DE DOMICILIO:

Domicilio del Ente:

El Ente tiene domicilio legal en: Av. Raúl Uranga S/N° (3.100) Paraná, Provincia de Entre Ríos, República Argentina. Dirección Postal: Casilla de Correo N° 189 (3.100) Paraná.-

Sólo se considerarán válidas durante la licitación las comunicaciones y notificaciones hechas en dicho domicilio.-

Domicilio del oferente:

Al efectuar la oferta, el proponente deberá constituir un domicilio especial en la ciudad de Paraná, para los efectos judiciales y extrajudiciales.-

Cambio de domicilio:

El cambio de los domicilios de ambas partes surtirá efectos a partir de su notificación fehaciente, pero siempre deberán estar constituidos según lo indicado en este artículo.-

2.21. INFORMACIONES SUPLEMENTARIAS:

Durante el período de Licitación y hasta tres (3) días antes de la fecha de apertura de las ofertas, el Ente podrá emitir circulares para aclarar cualquier duda o dificultad de interpretación. Las circulares emitidas por el Ente formarán parte de los documentos de Licitación. Cada circular será publicada en la página web del Ente.-

Las dudas que pudieran originarse, deberán plantearse por escrito al Ente, solicitando concretamente las aclaraciones que se estimen necesarias, hasta cinco (5) días antes de la fecha de apertura de las ofertas.-

Tanto las consultas como las respuestas serán dadas a conocer a todos los interesados que hayan adquirido el Pliego.-

La no recepción de las informaciones suplementarias, y en la forma indicada por parte de los adquirientes, no les da derecho a reclamo alguno, debiendo inexcusablemente notificarse en el domicilio del Ente hasta el tercer día hábil anterior al de la apertura de Ofertas. La no concurrencia en esa fecha, hará suponer el conocimiento y la aceptación de las aclaraciones expedidas.-

2.22. TRIBUNALES COMPETENTES:

Queda establecido que agotado el procedimiento administrativo previsto en las cláusulas 16°, 17°, 18° y 19° del Tratado Interprovincial vigente, los proponentes hacen renuncia a todo fuero judicial que no sean los Tribunales de la ciudad de Paraná y/o Santa Fe, a los que en consecuencia, se someten.-

2.23. GESTION DE LAS OBSERVACIONES E IMPUGNACIONES:

Los oferentes podrán examinar toda la documentación a partir del primer día hábil posterior al de la apertura de la Licitación y por un término de dos (2) días hábiles, en el lugar que indique el Ente y en horario administrativo de 7,00 a 13,00 hs., pudiendo interponer las **observaciones** que estimen convenientes en dicho lapso y hasta las dos (2) primeras horas del tercer día.-

Todas las **impugnaciones** contra los actos administrativos de admisibilidad y adjudicación, deberán afianzarse mediante depósito en efectivo en la Tesorería del Ente por un monto equivalente a uno por ciento (1%) del Presupuesto Oficial.-

En caso de resultar aceptada, en todo o en parte, la impugnación presentada, se devolverá el importe de la fianza al impugnante.-

El plazo para presentar **impugnaciones**, será de tres (3) días hábiles administrativos improrrogables, con dos (2) horas de gracia, a partir de la fecha de la notificación fehaciente del acto impugnado.-

2.24. DE LAS IMPUGNACIONES:

Complementando lo estipulado anteriormente, la existencia de observaciones o impugnaciones a lo actuado durante la Apertura de la Licitación, o a las ofertas presentadas, por ninguna circunstancia inhibirá o producirá efectos suspensivos al trámite de Adjudicación, éstas deberán ser tramitadas por separado y el dictamen final recaerá simultáneamente con el acto administrativo que apruebe la Licitación o cada etapa de análisis de las Propuestas.-

2.25. LUGAR DE ENTREGA:

Los materiales se entregarán en el Dpto. Almacenes del Ente, en días hábiles y horario administrativo de 7,00 a 13,00 hs.-

2.26. CONSULTAS:

Los interesados podrán imprimir el Pliego desde la página web del Ente, www.tunelsubfluvial.gov.ar. Además, podrán recabar información en el Departamento Informática del Ente, los días hábiles de 07:00 a 13:00 hs.-

Tel.: (0343) 4-200415.-

FAX (Compras): (0343) 4-200406/409.-

www.tunelsubfluvial.gov.ar

webtunel@tunelsubfluvial.gov.ar

informatica@tunelsubfluvial.gov.ar

NOTA: Se adjunta modelo de carta de presentación y datos del proponente.-

PRESUPUESTO OFICIAL: $ 500.000 (pesos quinientos mil)

DATOS DEL PROPONENTE.

- Denominación de la firma o Consorcio de Firmas.....
- Domicilio:.....
- Tipo de Sociedad:.....
- Antigüedad de la sociedad con su denominación actual:.....
- Caracterización del mandato otorgado a favor del firmante de la propuesta y demás representantes del Proponente.

NOTA: El Ente se reserva el Derecho de solicitar la ratificación de los datos con certificación Notarial

CARTA DE PRESENTACIÓN

Señores del Ente Interp.Túnel Subfluvial
RAUL URANGA – C.SYLVESTRE BEGNIS

La firma.....(Nombre de la firma o Consorcio de Firmas) representada legalmente por el/los Señor/es.....abajo firmantes, con domicilio legal en calle.....Nº:.....de la ciudad de Paraná, provincia de Entre Ríos de la República Argentina, presenta su propuesta para la *Licitación Pública Nº 425/18 "ADQUISICION Y PUESTA EN MARCHA DE UNA SOLUCIÓN INTEGRADA DE CONECTIVIDAD INALÁMBRICA Y DE PROTECCIÓN DE REDES PARA LA SEGURIDAD DE LA INFORMACIÓN PERIMETRAL."* y declara expresamente que:

a) Conoce plenamente y acepta el contenido de la documentación de la Licitación y de la totalidad de las aclaraciones y comunicaciones emitidas en legal forma.
b) Ha recorrido el lugar donde se realizarán los trabajos, requerido las informaciones necesarias para la concreción de los trabajos, aceptando que no podrá reclamar concepto basado en el desconocimiento del lugar y/o las instalaciones.
c) Garantiza la autenticidad y exactitud de todas sus declaraciones y autoriza al Organismo Licitante a solicitar las informaciones pertinentes a organismos oficiales, compañías de seguro, bancos, fabricantes de equipos o cualquier otra persona física o jurídica.
d) Renuncia a cualquier reclamación o indemnización originada en error propio en la interpretación de la documentación del llamado a Licitación.
e) Conoce la normativa legal y especificaciones que se aplican a la presente Licitación.
f) Se comprometen al estricto cumplimiento de las obligaciones asumidas en su presentación a esta Licitación.

Se acompaña constancia de la garantía de oferta consistente en: (depósito en efectivo, fianza bancaria o póliza de seguro de caución, indicando Banco o Compañía) por la suma de Pesos.....($.....). También se adjuntan los datos del Proponente y la declaración jurada de nacionalidad.

Lugar y Fecha

.....
Firma del Proponente

MODELO DE PAGARE A PRESENTAR COMO GARANTIA DE OFERTA EN LICITACIONES PRIVADAS.

Cuando la garantía supere la suma de $ 325,65 debe estar ***sellado.-***

Nº..... Por $.....
.....de 2018 .....
A la vista pagaré/mos sin protesto (Art. 50 D.Ley 5965-63 a Señor COMISION ADMINISTRADORA ENTE INTERPROVINCIAL TUNEL SUBFLUVIAL
o a su orden la cantidad Pesos.....
.....
por igual valor recibido en Garantía Lic.Pública Nº 425/18…fecha……
a entera satisfacción pagadero en Paraná/Santa Fe.

Firmante.....
Calle.....
Localidad.....
Teléfono.....

ADVERTENCIA: Si el documento no cumple con estos requisitos o el mismo posee algún error (no esencial) en la confección del documento (Art.23 inc.a- y 49 del Pliego de Condiciones Generales) el oferente deberá cumplimentarlos dentro de los cinco días (5) corridos de serle requerido por el Ente.

PLIEGO DE CONDICIONES

GENERALES LICITACIONES PÚBLICAS Y PRIVADAS

OBJETO DE LLAMADO

ARTÍCULO 1º - Este llamado a licitación tiene por objeto contratar el suministro de los materiales y elementos mencionados en el detalle y especificaciones del pliego de condiciones particulares parte integrante de este pliego, debiendo la mercadería satisfacer en su calidad y características, a juicio de la COMISIÓN ADMINISTRADO-RA DEL ENTE INTERPROVINCIAL TÚNEL SUBFLUVIAL "RAÚL URANGA – CARLOS SYLVESTRE BEGNIS", a los fines a que se destinan.

CONCURRENCIA A LA LICITACIÓN

ARTÍCULO 2º - Podrán intervenir:

1°) Las firmas inscriptas en el Registro de Proveedores de la Comisión Administradora
2°) Las firmas que formalicen su pedido de Inscripción dentro de los ocho (8) días de realizado el acto, cumplimentando los requisitos pertinentes de los diez (10) días siguientes.
3°) Las inscriptas en el Registro de Proveedores de otras Provincias Argentinas o del Estado Nacional que así lo demuestren al solo efecto de considerar la propuesta, debiendo tramitar su Inscripción dentro del plazo establecido en el punto 2º.
4°) Los proponentes extranjeros, además de cumplir con los requisitos determinados en el punto 2º, deberán hacer legalizar la documentación por la autoridad consular
5°) El cumplimiento de los prescripto en los puntos anteriores motivará que se desestime la propuesta respectiva.

ARTÍCULO 3º - La sola presentación de ofertas significa la aceptación lisa y llana de todas las estipulaciones que rigen la contratación, aún cuando el pliego de condiciones particulares no se acompañe a la oferta o no esté firmado por el proponente.

ARTÍCULO 4º - Por cualquier cuestión que se plantee los proponentes hacen renuncia a todo fuero judicial que no sean los Tribunales de la Ciudad de Paraná y/o Santa Fe, a los que en consecuencia se someten.

FORMA DE PRESENTAR LAS PROPUESTAS

ARTÍCULO 5º - Se presentarán por duplicado, en el lugar establecido en el pliego de condiciones particulares, en sobre cerrado, consignándose en la cubierta el número de la licitación, día y hora de apertura de la misma, dirigido a la Comisión Administradora que hace el llamado.

ARTÍCULO 6º - Todo proponente deberá indicar en la propuesta su número de inscripción en el Registro de Proveedores de la Comisión Administradora salvo los casos previstos en el artículo 2º y rubricará sus fojas cuando sean más de una.

ARTÍCULO 7º - Las enmiendas y raspaduras en partes esenciales de la propuesta tendrán que estar debidamente salvadas por el oferente.

ARTÍCULO 8º - Para el depósito de los sobres que se entreguen antes de la hora de apertura, se habilitarán urnas con el número de la licitación correspondiente y una vez en las mismas, los interesados no podrán solicitar su devolución. Se entregará recibo numerado a quienes entreguen ofertas personalmente con anticipación al acto. Para las ofertas recibidas por vía postal, valdrá como única constancia para el interesado, la fecha de entrega obrante en el aviso de retorno.

ARTÍCULO 9º - Las cotizaciones en cada renglón serán por la cantidad total especificada en el mismo. También se podrá ofrecer parte de alguno o de todos los renglones licitados, siempre que se hubiese previsto esta posibilidad en el pliego de condiciones particulares.

APERTURA DE PROPUESTAS

ARTÍCULO 10º - Las propuestas serán abiertas en la fecha y hora indicados en el pliego de condiciones particulares o el día hábil siguiente a la misma hora si resultara feriado o se decretase asueto, y sólo se tomarán en consideración las que sean presentadas hasta el instante de la apertura. Una vez abierto el primer sobre no se admitirá ninguna propuesta más, ni modificaciones a las recibida. Tampoco se considerarán las que llegaren por correo fuera de hora, aún cuando se justifique con el matasellos u otro elemento, haberse despachado oportunamente.

REQUISITO DE LAS OFERTAS

ARTÍCULO 11º - Los proponentes quedan obligados a mantener sus ofertas por el termino de treinta (30) días hábiles a contar de la fecha del acto de apertura, salvo que el pliego de condiciones particulares indicare expresamente otro plazo

ARTÍCULO 12º - Las ofertas especificarán:

1°) El precio unitario y total con referencia a la unidad solicitada, determinando además el total general de la propuesta en letras y números. Salvo indicación expresa en el pliego de condiciones particulares, el precio de los materiales o prestaciones deservicio, no estará sujeto a reajuste de variaciones de costo.
2°) Serán presentadas en moneda argentina, salvo cuando el pliego de condiciones particulares permita la cotización en moneda extranjera autorizada, en cuyo caso, a efectos de la comparación, deberá indicarse con precisión el tipo de cambio vendedor vigente al cierre del día anterior.
3°) Se presentarán en el lugar, día y hora que indique el respectivo pliego de condiciones particulares
4°) Cuando el total parcial de alguno o todos los renglones cotizados se observaran errores de cálculo, se tomarán como válidos los valores que figuren como precio unitario.

ARTÍULO 13º - Cuando en las ofertas se observaren defectos de forma que a juicio de la COMISIÓN DE COMPRAS no se refieran a la esencia de la propuesta y que no impida la comparación con las demás, se podrá requerir su cumplimiento o perfeccionamiento dentro de un plazo perentorio de ocho (8) días, siempre que no signifique una modificación a las cláusulas que expresamente determinen las condiciones estipuladas en el pliego.

MUESTRAS

ARTÍCULO 14º - Los proponentes deberán acompañar muestras de los artículos licitados cuando en las cláusulas particulares del pliego de condiciones se establezca expresamente y no será considerada la propuesta en el renglón respectivo que no cumpla tal requisito. Se entregarán bajo recibo que se agregará a la propuesta antes o en el momento de la apertura de la licitación.

ARTÍCULO 15º - Se presentarán en tamaño adecuado para los análisis o experiencias a que se las someta, cuyas medidas se indicarán en el pliego de condiciones particulares.

ARTÍCULO 16º - Se exceptuará de la presentación de muestras que menciona el artículo 15º cuando el elemento ofrecido responde a una reconocida marca y calidad, o bien que las características del mismo no lo permitan.

ARTÍCULO 17º - Se podrán presentar hasta la hora de apertura de la licitación en el lugar que indique la solicitud de cotización.

ARTÍCULO 18º - Las muestras deberán presentarse con un rótulo en lugar visible, asegurado mediante precinto o lacre sellado y llevará el número de la misma, el del renglón correspondiente y el de la licitación, datos éstos que deben figurar en la propuesta respectiva.

ARTÍCULO 19º - Tratándose de especialidades medicinales u otros casos que se justifiquen debidamente y siempre que así se establezca en el pliego de condiciones particulares, se prescindirá de su presentación.

ARTÍCULO 20º - Las que correspondan a ofertas rechazadas, quedarán a disposición de los proponentes para su retiro hasta treinta (30) días después de resuelta la adjudicación. Vencido este plazo, las mismas pasarán a ser propiedad de la Comisión Administradora.

ARTÍCULO 21º - Las correspondientes a ofertas aceptadas, podrán ser retiradas una vez cumplido el contrato, hasta treinta (30) días a contar de la última conformidad de recepción de la mercadería adjudicada. De no procederse a su retiro dentro de dicho plazo, se observará el mismo procedimiento señalado en el artículo 20º.

ARTÍCULO 22º - Los oferentes no tendrán derecho a reclamo por deterioro proveniente de los análisis y ensayos a que se las someta.

GARANTÍAS

ARTÍCULO 23º - Para afianzar el cumplimiento de todas las obligaciones, los proponentes y adjudicatarios deberán presentar las siguientes garantías:
a) De Ofertas: El UNO POR CIENTO (1%) del total del valor de la oferta. En el caso de cotizar con alternativas, la garantía se calculará sobre el mayor valor propuesto.

b) De Adjudicación: La garantía señalada en a) será aumentada al CINCO POR CIENTO (5%) del monto adjudicado.

En ningún caso dichas garantías devengan intereses.

ARTÍCULO 24º - El requisito anotado en b) deberá cumplimentarse dentro de los veinte (20) días a contar de la fecha de notificación de la adjudicación, salvo el caso de que antes de vencer el plazo establecido, el adjudicatario dé cumplimiento a todas las obligaciones contraídas.

ARTÍCULO 25º - Cuando el depósito se haga en moneda extranjera, el importe de la garantía se calculará al tipo de cambio vendedor vigente al cierre del día anterior de la constitución de la garantía.

ARTÍCULO 26º - Las garantías a que se refiere el Artículo23 deberán constituirse en algunas de estas formas a opción del proponente o adjudicatario.

a) Giro o remesa postal o bancario, depósito bancario, cheque certificado a la orden de la Comisión Administradora del Ente Túnel Subfluvial "Raúl Uranga – Carlos Sylvestre Begnis"

b) Con pagaré a la vista sobre plaza Paraná o Santa Fe suscriptos por quienes tengan el uso de la razón social o actuaren con poderes suficientes a favor de la Comisión Administradora del Ente Túnel Subfluvial "Raúl Uranga – Carlos Sylvestre Begnis".

Cuando se optare por esta forma de garantía de adjudicación y ésta sea superior a los $325,65 el documento deberá presentarse con sellado y aval bancario

c) Mediante carta fianza suscripta por una institución bancaria garantizando a favor de la Comisión Administradora el cumplimiento de las obligaciones contraídas por el oferente.

d) Póliza de Seguro que garantice el cumplimiento de las obligaciones tomadas por el proponente o adjudicatario

ARTÍCULO 27º - Los documentos presentados en garantía de las propuestas o de las adjudicaciones deberán llevar el sellado de ley correspondiente.

ARTÍCULO 28º - El incumplimiento a los requerimientos de la Comisión Administradora podrá ser pasible de sanciones de suspensión o cancelación de la inscripción en el Registro de Proveedores, según los casos.

ARTÍCULO 29º - La Comisión Administradora, dispondrá inmediatamente de resuelta la adjudicación la devolución de los depósitos de garantías a todas las firmas cuyas propuestas no fueran aceptadas y a la o las adjudicatarias una vez cumplimentadas todas las obligaciones contraídas.

ADJUDICACIONES

ARTÍCULO 30º - La adjudicación se hará por renglón o por el total licitado, según convenga como consecuencia de la comparación de las ofertas presentadas al acto respectivo y excepcionalmente ella puede tener lugar aunque se hubiere presentado una sola oferta siempre que la misma sea válida, es decir que se ajuste al pliego de condiciones generales y especificaciones particulares y ser además su precio conveniente a los Intereses del Estado.

ARTÍCULO 31º - También se podrá adjudicar parte de alguno o de todos los renglones licitados siempre que se hubiese establecido esta condición en el llamado a licitación.

ARTÍCULO 32º - La adjudicación recaerá siempre en la propuesta más conveniente, entendiéndose por tal aquella cuyos precios sean los más bajos, en igualdad de condiciones y calidad, de acuerdo a las siguientes normas:

1°) Cuando los efectos ofrecidos reúnan las especificaciones exigidas por los pliegos de bases y condiciones y cláusulas o especificaciones especiales, la adjudicación se resolverá
2°) Por vía de excepción podrá adjudicarse por razones de calidad previo dictamen fundado de la Comisión de Compras, que en forma descripta y comparada con la oferta de menor precio, justifique en detalle la mejor calidad de material, funcionamiento a otras características que demuestren las ventajas de la adjudicación que a precios superiores al menor cotizado se proyecte efectuar.
3°) En igualdad de condiciones se dará preferencia a las propuestas en que figuren los menores plazos de entrega. Cuando así se hubiere establecido en el pliego de condiciones particulares podrá adjudicarse a propuestas que ofrezcan menor plazo de entrega, aunque su precio no sea el más bajo, si la oportunidad del abastecimiento lo requiere. En este caso la diferencia de precio deberá justificar los beneficios que se obtengan por el menor plazo de entrega.
4°) En igualdad de precios y condiciones se dará preferencia en la adjudicación a los artículos de procedencia nacional, de acuerdo a la Ley Nacional Nº 18.875 decreto reglamentario Nº 2930/70.
5°) En caso de empate (igualdad de precio y condiciones) y superar el monto del renglón la cantidad se llamará a los respectivos proponentes a una mejora de precios dentro del término de tres (3) días, cuando se trate de firmas de la localidad de Paraná y/o Santa Fe, y hasta diez (10) días cuando ello ocurra con oferentes de otras ciudades. De subsistir el empate por no modificarse los precios o por resultar estos nuevamente iguales o por no superar el monto del renglón la cantidad mínima prevista para mejora de precios, se dilucidará por sorteo.

ARTÍCULO 33º - La autoridad de adjudicación, está facultada aceptar la oferta que a su juicio resulte más conveniente a los intereses del Estado o de rechazarlas a todos in que ello otorgue derecho a los oferentes a reclamo de indemnización alguna.

ARTÍCULO 34º - Dos (2) días antes de vencer el mantenimiento de ofertas, la Comisión de Compras a cargo de quien estuviere el estudio de las ofertas requerirá telegráficamente ampliación del plazo, si estimara que la adjudicación no estará aprobada a su vencimiento.

ORDEN DE COMPRA

ARTÍCULO 35º - Producida la aprobación del acto licitatorio, la Comisión Administradora procederá a:

Emitir la orden de compra.
Comunicar a la o las firmas adjudicatarias la obligación de integra%) r el depósito de garantía ejecutado, hasta cubrir el CINCO POR CIENTO (5del monto adjudicado, dentro del término de veinte (20) días de la fecha de notificación de la adjudicación, salvo el caso de que antes de vencer el plazo establecido, el adjudicatario de cumplimiento a todas las obligaciones contraídas.
Comunicar a la o las adjudicatarias la obligación de abonar dentro del plazo de quince (15) días a partir de la fecha de la orden de compra el impuesto de sello sobre el total adjudicado, conforme lo establece la Ley Impositiva vigente, en la Pcia. E.R. por contratos de suministros, licitaciones y concurso de precios.

ARTÍCULO 36º - Comunicar a las firmas oferentes que no resultaron adjudicatarias en el acto respectivo y devolver a las mismas los depósitos de garantía.

ENTREGA DE MERCADERÍA

ARTÍCULO 37º - Recibida por el adjudicatario la orden de compra éste procederá a entregar la mercadería con remito por duplicado, el que deberá ser conformado y devuelto al proveedor con la anotación de "Mercadería a Revisar" por el empleado interviniente.

ARTICULO 38º - La recepción definitiva se efectuará en el sitio establecido en el pliego de condiciones particulares con intervención de los funcionarios previstos en el Reglamento de compras, quienes extenderán el certificado de recepción que se entregará al proveedor, labrándose el "Acta de Aprobación de Materiales" con la constancia de la cantidad, calidad y demás características de la orden de compra a que corresponden.

ARTÍCULO 39º - Los receptores de mercadería podrán requerir directamente la entrega a las firmas adjudicatarias de las cantidades en menos que hubieren remitido, pero el rechazo por diferencia de calidad, característica, etc., no podrá ser encarado directamente por los mismos, quienes deberán formular por escrito a las autoridades de adjudicación las observaciones que estimen oportunas, quedando a cargo de la misma la decisión final sobre la recepción. No se admitirá la entrega parcial de los elementos piezas o partes que no constituyan una unidad funcional apta para cumplir el fin indicado en las especificaciones técnicas salvo expresa indicación en contrario.

ARTÍCULO 40º - Vencido el plazo de cumplimiento pactado sin que la mercadería o servicio fuesen entregados o prestados o en el caso de rechazo sin perjuicio de la multa por mora señalada en las bases de licitación y demás sanciones que pudiera corresponder, la Comisión Administradora intimará su entrega o prestación en un plazo perentorio bajo apercibimiento de rescisión del contrato con pérdida del depósito de garantía.

ARTÍCULO 41º – Con la copia del "Acta de Aprobación de Materiales" firmada por los receptores de la mercadería, el Proveedor presentará a la Comisión Administradora, las facturas correspondientes, las que debidamente conformadas, se enviarán a Contaduría para que proceda a tramitar la orden de pago.

ARTÍCULO 42º - Serán a cargo del adjudicatario todos los gastos que se originen por flete, acarreo y entrega de la mercadería en el lugar establecido

PENALIDADES

ARTÍCULO 43º - En caso de incumplimiento de sus obligaciones, los proponentes y adjudicatarios se harán pasibles de las siguientes penalidades:
1°)Pérdida del depósito de garantía que hubieran constituido en beneficio de la Comisión Administradora si el proponente desistiera de su oferta dentro del plazo de mantenimiento establecido y no mediare adjudicación anterior.
2°)Igual penalidad será aplicada al adjudicatario que no ampliara la garantía hasta el CINCO POR CIENTO (5%) del valor adjudicado, dentro del término fijado, sin perjuicio de las demás sanciones que correspondan.
3°)Vencido el plazo contractual sin que la mercadería o servicio fuere entregado o hubieses sido rechazado sin perjuicio de las multas señaladas en el Art. 44 la Comisión Administradora

intimará su entrega en un plazo perentorio que no podrá exceder de treinta (30) días a partir del vencimiento, bajo apercibimiento de rescisión del contrato. De no cumplirse la obligación en el plazo acordado, se rescindirá el contrato, haciéndose pasible el adjudicatario de la pérdida de la garantía presentada.
4°)En los casos que la provisión no esté respaldad por ningún depósito en razón de su monto, el incumplimiento será sancionado con una multa equivalente al CINCO POR CIENTO (5%) del importe total cotizado o adjudicado según el caso

ARTÍCULO 44º - Si el proveedor entregara el material o parte de él después de vencido el plazo contractual, se le aplicará una multa equivalente al TRES POR MIL (3‰) diario del valor de los efectos no entregados en término, durante los diez (10) primeros días; CINCO POR MIL (5‰) diario del mismo valor durante los diez (10) días siguientes y DIEZ POR MIL (10‰) durante los diez (10) días posteriores.

ARTÍCULO 45º - Vencido el último término acordado en el Artículo 47º, Inc. 3, la Comisión Administradora dispondrá la rescisión del contrato y efectivización de las penalidades que corresponda, sin perjuicio de las penalidades establecidas anteriormente, la Comisión Administradora, previo dictamen de la Comisión de Compras que intervino, podrá suspender o eliminar del Registro de Proveedores las casas o firmas inscriptas que no den cumplimiento de sus obligaciones.

ARTÍCULO 46º - Se entenderá por "Mercadería no entregada" también aquella que fuera entregada y rechazada por no ajustarse a las condiciones de la orden de compra

ARTÍCULO 47º - Se considera producida la mora por el simple vencimiento del plazo contractual, sin necesidad de interpelación judicial o extrajudicial.

PAGO DE LAS ADQUISICIONES

ARTÍCULO 48º - El pago se efectuará de conformidad con la forma estipulada por el oferente en su propuesta, pudiendo la Comisión Administradora, si lo estimare conveniente a los intereses del Ente, hacer anticipos a cuenta del precio, cuando y en la forma que fije el pliego de condiciones particulares.

RECHAZO DE OFERTAS

ARTÍCULO 49º - No se considerarán las ofertas:

1°)Cuando no vengan acompañadas de la garantía prevista en el Art. 26 inc. a), b), c), d)
2°)Presentadas por firmas que hayan sido eliminadas o se encuentren suspendidas del Registro de Proveedores de la Comisión Administradora y/o Provincias de Entre Ríos y Santa Fe.
3°)El o los renglones que tengan enmiendas o raspaduras en su texto, que no estén debidamente salvadas o aclaradas al pie de la oferta y firmada por el proponente.
4°)Que no se ajusten al Pliego de condiciones Generales y Particulares en lo que respecta al término de mantenimiento de la oferta, plazo, condiciones de pago, lugar y forma de entrega de la mercadería

5°)Será también motivo de rechazo cuando no se presenten las muestras respectivas, catálogos, prospectos ilustrativos, etc., si así se indicara expresamente en el Pliego de Condiciones Particulares.
6°)No se considerará tampoco la oferta en el renglón que se cotice precio unitario por talles o numeración.
7°)Cuando no se consigne el precio unitario, el total parcial por renglón y el total general de la propuesta.

PLIEGO DE CONDICIONES GENERALES LICITACIONES PUBLICAS Y PRIVADAS

ANEXO:

CUMPLIMIENTO DE OBLIGACIONES PREVISIONALES Y FISCALES

Los proveedores deberán tener vigente en el Ente la declaración jurada a que se refiere la Ley Nacional Nº: 17.250/67 (Art.4º) respecto a la no existencia de deuda exigible en concepto de aportes, contribuciones y de toda otra obligación previsional.

Justificarán estar al día en el pago del impuesto a los INGRESOS BRUTOS (para Santa Fe/Entre Ríos), según corresponda, y Ley 4035 (para Entre Ríos).

Consignarán en sus ofertas los números de CODIGO UNICO DE IDENTIFICACION TRIBUTARIA (C.U.I.T.), INGRESOS BRUTOS (Santa Fe) o a los INGRESOS BRUTOS - Ley 4035 (Entre Ríos) y Cajas Nacionales de Previsión Social.

La omisión de estos requisitos no invalidará la propuesta ni obstará a su consideración, pero el Ente no conformará ni dará curso a factura alguna, hasta tanto no se de cumplimiento a lo establecido en el presente.