

AVISO CONSULTA PRELIMINAR

1. OBJETO DE CONTRATACIÓN:

ADQUISICIÓN E IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL Y EQUIPAMIENTO ACTIVO DE RED PARA LA MATRIZ DE ARCOM

TIPO DE COMPRA	SELECCIÓN
Servicios	
Bienes	X
Obras	
Consultoría	

2. CÓDIGO CPC:

CPC NIVEL 9 DÍGITOS	DESCRIPCIÓN
452400017	EQUIPOS DE SEGURIDAD INFORMATICA
871300011	SERVICIOS DE MANTENIMIENTO, REPARACION Y ATENCION DEL EQUIPO DE COMPUTACION (INFORMATICA)

3. PRODUCTOS O SERVICIOS ESPERADOS:

Los servicios que requiere la ARCOM son los que se detallan a continuación:

ÍTEM	DESCRIPCIÓN	CANTIDAD	UNIDAD DE MEDIDA
1	Switches Core de fibra óptica, capa 3, en alta disponibilidad	2	Unidad
2	Switch de acceso capa 2+, 48 puertos PoE+ (full PoE)	3	Unidad
3	Equipos seguridad perimetral (firewall de nueva generación) en alta disponibilidad; incluye plataforma virtual de gestión de registros y reportería, suscripciones de seguridad y accesorios	2	Unidad
4	Servicio de implementación, configuración, integración, pruebas y puesta en operación de la solución	1	Servicio

COMPONENTE 1: SWITCHES CORE DE FIBRA ÓPTICA

SWITCHES CORE DE FIBRA ÓPTICA	
Característica	Especificación técnica
Cantidad	2 (dos)
Equipo	Nuevo, de primer uso, no remanufacturado ni reacondicionado, en su empaque original del fabricante
Marca/Modelo	A declarar por el oferente; deberá ser compatible y soportado por el fabricante de los equipos ofertados; sin anuncio de fin de venta o soporte a la fecha de la oferta; el fabricante debe ser reconocido y debe estar dentro del cuadrante mágico de Gartner
Administración	
Administración centralizada	Administrable desde una consola centralizada
Administración local	Configuración independiente mediante puerto de consola, CLI por SSH e interfaz web HTTPS.
Capacidad	
Arquitectura de conmutación	No bloqueante (wire-speed) en todos los puertos.

SWITCHES CORE DE FIBRA ÓPTICA	
Característica	Especificación técnica
Capacidad de conmutación	Al menos 880 Gbps
Tasa de reenvío	Al menos 1.300 Mpps
Tabla de direcciones MAC	Al menos 32.000 entradas
Tabla de rutas	Al menos 8.000 rutas IPv4 y 4.000 rutas IPv6
Hardware	
Puertos 10GE SFP+ (compatibles con 1GE SFP)	Al menos 24
Puertos 40/100GE QSFP+/QSFP28	Al menos 2
Puerto de consola	Al menos 1 (RJ-45 o USB)
Formato	Montaje en rack de 19", incluye kit de montaje
Fuentes de poder	Redundantes, intercambiables en caliente
Alta disponibilidad	
Operación en par	Los dos switches Core operarán en alta disponibilidad activo-activo, con agregación de enlaces multichassis (MC-LAG, stacking virtual o tecnología equivalente del fabricante), permitiendo que los switches de acceso y los firewalls se conecten a ambos Core como un único enlace lógico.
Funcionalidades de capa 2	
VLAN	IEEE 802.1Q; Private VLAN; VLAN mapping/translation; IEEE 802.1ad (QinQ)
Agregación de enlaces	IEEE 802.1AX / 802.3ad (LACP)
Spanning Tree	IEEE 802.1D (STP), 802.1w (RSTP), 802.1s (MSTP)
Otros	Jumbo frames; LLDP (IEEE 802.1AB); IEEE 802.1Qbb (PFC)
Funcionalidades de capa 3	
Enrutamiento	Estático; dinámico OSPFv2 y OSPFv3; BGP-4 y MP-BGP (IPv4/IPv6); Policy-Based Routing; ECMP
Redundancia de gateway	VRRP (v2/v3)
Virtualización de red	VRF (VRF-lite); VXLAN; BGP EVPN
Servicios	DHCP server y DHCP relay
Multicast	IGMP snooping; IGMP proxy; PIM-SM/PIM-SSM
IPv6	Doble pila IPv4/IPv6
Estándares mínimos (IETF)	RFC 4271 (BGP-4), RFC 4760 (MP-BGP), RFC 6793 (ASN de 4 bytes), RFC 2328 (OSPFv2), RFC 5340 (OSPFv3), RFC 5798 (VRRPv3), RFC 8200 (IPv6), RFC 4861 (ND), RFC 4862 (SLAAC), RFC 4443 (ICMPv6), RFC 2474 (DSCP)
Seguridad, visibilidad y QoS	
Seguridad	ACL L2/L3/L4 para IPv4 e IPv6; IEEE 802.1X; RADIUS y TACACS+; DHCP snooping; IP Source Guard; Dynamic ARP Inspection; seguridad de puerto (límite de direcciones MAC)
Visibilidad	sFlow, NetFlow o IPFIX; port mirroring; SNMPv2c/v3; syslog
QoS	Clasificación y priorización por IEEE 802.1p y DSCP; colas de prioridad
Soporte y licenciamiento	
Licencias	Incluidas todas las licencias para las funcionalidades requeridas en esta tabla (incluidas las de capa 3 avanzadas), por el período de soporte.
Soporte	Soporte técnico del fabricante 24x7 por al menos 2 años

COMPONENTE 2: SWITCHES DE ACCESO FULL POE

SWITCHES DE ACCESO FULL POE	
Característica	Especificación técnica
Cantidad	3 (tres)
Equipo	Nuevo, de primer uso, no remanufacturado ni reacondicionado, en su empaque original del fabricante
Marca/Modelo	A declarar por el oferente; deberá ser compatible y soportado por el fabricante de los equipos ofertados; sin anuncio de fin de venta o soporte a la fecha de la oferta; el fabricante debe ser reconocido y debe estar dentro del cuadrante mágico de Gartner
Administración	
Administración centralizada	Administrable desde una consola centralizada
Administración local	Configuración independiente mediante puerto de consola, CLI por SSH e interfaz web HTTPS.
Capacidad	
Arquitectura de conmutación	No bloqueante (wire-speed) en todos los puertos
Capacidad de conmutación	Al menos 176 Gbps
Tasa de reenvío	Al menos 130 Mpps
Tabla de direcciones MAC	Al menos 16.000 entradas
Hardware	
Puertos de acceso	48 puertos 10/100/1000BASE-T RJ-45, todos con PoE+ (IEEE 802.3at)
Puertos de uplink	Al menos 4 puertos 10GE SFP+
Presupuesto PoE	Al menos 740 W
Puerto de consola	Al menos 1 (RJ-45 o USB)
Formato	Montaje en rack de 19", incluye kit de montaje
Funcionalidades de capa 2	
VLAN	IEEE 802.1Q; Private VLAN
Spanning Tree	IEEE 802.1D, 802.1w (RSTP), 802.1s (MSTP); Root Guard; BPDU Guard; Edge Port / PortFast
Agregación de enlaces	IEEE 802.3ad (LACP), compatible con la agregación multichasis de los switches Core
Otros	Jumbo frames; autonegociación de velocidad y dúplex; Auto MDI/MDIX; enrutamiento estático IPv4/IPv6
Multicast	
IPv4 / IPv6	IGMP snooping, IGMP querier/proxy; MLD snooping, MLD querier/proxy
Seguridad y visibilidad	
Control de acceso	IEEE 802.1X; MAC Authentication Bypass; RADIUS con Change of Authorization (CoA)
Listas de control de acceso	ACL L2/L3/L4 para IPv4 e IPv6, con posibilidad de aplicación por horario
Protección de puerto	Seguridad de puerto (límite y aprendizaje persistente de direcciones MAC); DHCP snooping; Dynamic ARP Inspection; IP Source Guard (vinculación IP-MAC); IPv6 RA Guard
Cifrado de enlace	IEEE 802.1AE (MACsec)
Visibilidad	Port mirroring; sFlow, NetFlow o IPFIX; LLDP y LLDP-MED (IEEE 802.1AB); SNMPv2c/v3; syslog
QoS	
Priorización	Colas de prioridad basadas en IEEE 802.1p y en IP ToS/DSCP

SWITCHES DE ACCESO FULL POE	
Característica	Especificación técnica
Soporte y licenciamiento	
Soporte y licencias	Soporte técnico del fabricante 24x7 por al menos 2 años y licencias necesarias para las funcionalidades requeridas

COMPONENTE 3: EQUIPOS SEGURIDAD PERIMETRAL, INCLUYE REPORTARÍA DE LA SOLUCIÓN DE FIREWALL

Equipos de Seguridad Perimetral

EQUIPOS SEGURIDAD PERIMETRAL	
Característica	Especificación técnica
Cantidad	2 (dos), en clúster de alta disponibilidad
Equipo	Firewall de nueva generación (NGFW), tipo appliance físico, nuevo, de primer uso, no remanufacturado ni reacondicionado, en su empaque original del fabricante
Marca/Modelo	A declarar por el oferente; deberá ser compatible y soportado por el fabricante de los equipos ofertados; sin anuncio de fin de venta o soporte a la fecha de la oferta; el fabricante debe ser reconocido y debe estar dentro del cuadrante mágico de Gartner
Capacidad	
Throughput de firewall (IPv4/IPv6)	Al menos 25 Gbps
Throughput de prevención de amenazas (firewall, IPS, control de aplicaciones y antimalware habilitados, tráfico empresarial mixto)	Al menos 6 Gbps
Throughput VPN IPsec	Al menos 10 Gbps
Sesiones concurrentes (TCP)	Al menos 3.000.000
Nuevas sesiones por segundo (TCP)	Al menos 300.000
Túneles VPN IPsec sitio a sitio	Al menos 500
Usuarios concurrentes de VPN de acceso remoto	Al menos 500, con licencias incluidas
Contextos o instancias virtuales de firewall	Al menos 5, con licencias incluidas
Hardware	
Puertos 10GE SFP+	Al menos 8
Puertos 1GE SFP (o puertos SFP+ adicionales compatibles con 1GE)	Al menos 4
Puertos 1GE RJ-45	Al menos 8
Puertos de gestión y alta disponibilidad	Al menos 1 puerto de gestión dedicado y 1 puerto para HA (dedicado o configurable)
Puertos de consola y USB	Al menos 1 de cada uno
Funcionalidades básicas	
Modos de operación	Capa 3 (enrutamiento y NAT); capa 2 (transparente/bridge); monitoreo pasivo (TAP/SPAN)
Alta disponibilidad	Activo-Pasivo y Activo-Activo entre equipos idénticos, con sincronización de configuración y sesiones y conmutación automática; licencias incluidas
Políticas	Administración de políticas unificadas basadas en objetos: dirección IP, subred, rango, FQDN, geolocalización (país), usuarios y grupos, dispositivos,

EQUIPOS SEGURIDAD PERIMETRAL	
Característica	Especificación técnica
	aplicaciones y servicios
Programación de políticas	Horarios recurrentes y de ejecución única
Objetos dinámicos de nube	Objetos de servicios de Internet y nube (p. ej., suites de ofimática en la nube, proveedores de infraestructura en la nube) actualizados por el fabricante, utilizables como origen o destino en políticas, enrutamiento y SD-WAN
Registros	Visualización del país de origen y destino en los registros de tráfico
Inspección cifrada	Inspección SSL/TLS (incluido TLS 1.3), con excepciones por reputación y por categoría web
Servicios de red	Servidor DHCP, DNS (servidor/proxy) y NTP
IPv6	Administración, enrutamiento, políticas de firewall y seguridad, NAT64 (o NAT46/DNS64) y VPN IPsec sobre IPv6
Cuarentena	Cuarentena de usuarios o direcciones IP por tiempo definido, manual y automática ante eventos de IPS
Automatización	Respuesta automática a eventos (al menos: cambios de configuración, reinicio del sistema, expiración de licencias, conmutación de alta disponibilidad, actualización de firmas) mediante acciones (al menos: notificación por correo electrónico, bloqueo o cuarentena de la dirección IP o del dispositivo, llamada a API/webhook). Puede ser nativa o mediante la plataforma de gestión ofertada
Networking	
Enrutamiento	Estático, Policy-Based Routing y dinámico: RIPv2, OSPFv2, OSPFv3, BGP-4 / MP-BGP
NAT	NAT estático, NAT dinámico y PAT
Interfaces	VLAN IEEE 802.1Q (troncales), agregación de enlaces IEEE 802.3ad (LACP) e interfaces redundantes; VXLAN
Redirección de contenido	ICAP
Balanceo de enlaces WAN / SD-WAN	Al menos 2 enlaces de Internet; algoritmos por volumen, por sesiones, por IP de origen y por origen-destino; verificación de disponibilidad (ping y HTTP); selección dinámica de ruta por aplicación según SLA (latencia, jitter y pérdida de paquetes); conmutación automática ante falla. Licencias incluidas
QoS y traffic shaping	Políticas por dirección de origen, destino, puerto y aplicación; ancho de banda garantizado y máximo; colas de prioridad; marcación y priorización DSCP/ToS; aplicable en interfaces agregadas o redundantes; estadísticas en tiempo real
Control de consumo	Denegación o limitación de ancho de banda para aplicaciones de alto consumo (audio y video streaming)
Prevención de amenazas	
IPS	Al menos 7.000 firmas; detección de anomalías de protocolo; firmas personalizadas; acciones: bloquear, monitorear, reiniciar la conexión y poner en cuarentena el origen; filtros por severidad, sistema operativo objetivo y aplicación/protocolo; operación en modo IDS
Denegación de servicio	Umbrales configurables para ataques de inundación (flood), escaneo de puertos, barrido ICMP e inundación de sesiones
Antimalware	Antivirus en modo flujo y/o proxy; detección basada en firmas y en aprendizaje automático; análisis de archivos

EQUIPOS SEGURIDAD PERIMETRAL	
Característica	Especificación técnica
	en sandbox (en sitio o en la nube) con envío automático y actualización dinámica de firmas ante amenazas de día cero
Desarme de contenido	Desarme y reconstrucción de archivos PDF y de ofimática para retirar contenido activo (CDR)
Botnets e inteligencia	Bloqueo de comunicaciones con servidores de comando y control por reputación global; uso de listas externas de dominios, direcciones IP, URL y hashes de malware
Archivos	Identificación y aplicación de políticas sobre archivos comprimidos y cifrados
Control de aplicaciones y filtrado web	
Control de aplicaciones	Base de aplicaciones del fabricante con al menos 18 categorías (p. ej., P2P, proxy, acceso remoto); firmas personalizadas; detección de HTTP/2 y bloqueo de QUIC; acciones: permitir, bloquear, reiniciar sesión y monitorear
Aplicaciones SaaS	Control granular de aplicaciones en la nube (p. ej., almacenamiento y colaboración en línea) y visibilidad/control de uso de SaaS (CASB en línea)
Modos de filtrado web	Proxy, flujo y filtrado DNS
Categorías	Al menos 60 categorías web del fabricante; creación de categorías locales y reclasificación de las del fabricante
Excepciones y perfiles	Exclusión de URL individual y por categoría; perfiles de navegación por usuario o grupo; cuotas de navegación por categoría
Evasión	Prevención del uso de proxies y anonimizadores por categoría, por aplicación y por comportamiento (IPS)
Restricción de cuentas	Restringir el acceso a servicios en la nube únicamente con cuentas corporativas (p. ej., servicios de correo y colaboración en la nube)
Experiencia de usuario	Página de bloqueo personalizable; modo de advertencia con opción de continuar; notificaciones personalizadas al bloquear sitios o adjuntos
Listas y rendimiento	Integración con múltiples listas negras externas; caché de clasificación de URL local o en la nube del fabricante
Proxy	Proxy web explícito y transparente
Protección de datos, correo y aplicaciones publicadas	
DLP	Identificación y, opcionalmente, bloqueo de información sensible (p. ej., números de tarjeta) con patrones predefinidos y expresiones regulares; filtrado por tipo de archivo, extensión, contenido o huella digital
Correo	Inspección de SMTP(S), POP3(S) e IMAP(S); antispam
Aplicaciones web	Firewall de aplicaciones web (WAF) basado en firmas
Balanceo de servidores	Balanceo de carga hacia granjas de servidores (HTTP, HTTPS, SSL/TLS, TCP, UDP) por round robin, ponderado y por tiempo de respuesta
Políticas avanzadas	Por tiempo (día, mes, año, día de la semana y hora); por usuario, IP, red o zona; integradas con el directorio institucional; por URL y categoría de URL
VPN	
VPN IPsec sitio a sitio	IKEv2 (e IKEv1 por compatibilidad); cifrado AES-128/256 (CBC y GCM); integridad SHA-256/384/512; Diffie-Hellman grupos 14, 19, 20, 21 o superiores; PFS; autenticación con clave precompartida y certificados X.509 (PKI)

EQUIPOS SEGURIDAD PERIMETRAL	
Característica	Especificación técnica
Interoperabilidad	Con equipos de terceros, basada en estándares (RFC 7296 y RFC 4301)
VPN de acceso remoto	Mediante cliente IPsec (IKEv2) y/o SSL/TLS para Windows, macOS, iOS y Android; licencias incluidas para al menos 500 usuarios concurrentes
Configuración de acceso remoto	Múltiples perfiles o portales asociados a grupos de usuarios; límite de usuarios concurrentes y de sesiones simultáneas por usuario; asignación de DNS; túnel completo (redirigir todo el tráfico del usuario al túnel) y túnel dividido
Seguridad del tráfico VPN	Aplicación de control de aplicaciones, IPS, antimalware y filtrado URL al tráfico de usuarios remotos
Gestión	Activación y desactivación de túneles IPsec desde la interfaz gráfica
Autenticación	
Fuentes de identidad	Base de datos local; LDAP/LDAPS; RADIUS; TACACS+ (acceso administrativo); SAML 2.0
Doble factor (MFA)	Para acceso administrativo y VPN de acceso remoto, nativo o mediante integración con el proveedor de identidad institucional (SAML 2.0, RADIUS o TOTP)
Single Sign-On	Identificación transparente de usuarios integrada con el Directorio Activo; RADIUS accounting
Portal cautivo	Autenticación sin software cliente antes de permitir la navegación
Certificados	Autenticación con certificados digitales
Administración y monitoreo	
Acceso	Interfaz gráfica web HTTPS y CLI por SSH y puerto de consola; posibilidad de deshabilitar protocolos no seguros
Idioma de la consola	Español o inglés
Perfiles	Perfiles de administración por roles con permisos granulares; registro de auditoría de cambios (usuario, fecha y hora, cambio realizado)
Visibilidad	Visualización en tiempo real e histórica de usuarios, dispositivos, aplicaciones y amenazas
Monitoreo e integración	SNMPv2c y SNMPv3; syslog; NetFlow/IPFIX o sFlow; integración con SIEM; API REST para integración con plataformas de virtualización, nube y SDN
Diagnóstico	Captura de paquetes, rastreo de sesiones y herramientas de depuración
Suscripciones, soporte y licenciamiento	
Suscripciones de seguridad	• IPS • Antimalware y antivirus, incluidos sandbox y detección basada en aprendizaje automático • Bloqueo de botnets y comando y control • Filtrado URL, filtrado DNS y detección de certificados maliciosos • Control de aplicaciones y control de SaaS / CASB en línea • Antispam • Prevención de pérdida de datos (DLP) • Identificación de dispositivos IoT • Desarme y reconstrucción de contenido

EQUIPOS SEGURIDAD PERIMETRAL	
Característica	Especificación técnica
Soporte del fabricante	Al menos 2 años, 24x7; reemplazo de partes y piezas; actualizaciones de software y firmas
Funciones incluidas	Todas las funcionalidades de esta tabla (alta disponibilidad, SD-WAN, contextos virtuales, VPN de acceso remoto y demás) deberán estar licenciadas en la oferta, sin costos adicionales para la ARCOM durante el período de soporte
Accesorios	
Transceivers 10GE SR	20 unidades, multimodo, compatibles y soportados por el fabricante de los equipos ofertados
Patch cords de fibra óptica	24 unidades, dúplex LC/LC, multimodo OM3 o superior (compatibles), 7 m
Cables de interconexión Core	Al menos 1 cable Direct Attach (DAC) QSFP+ o QSFP28 de 40 Gbps o más, compatibles con los switches Core ofertados
Otros	Cables de poder, kits de montaje y demás accesorios necesarios para la instalación

Plataforma de gestión de registros y reportería

PLATAFORMA DE GESTIÓN DE REGISTROS Y REPORTERÍA	
Característica	Especificación técnica
Cantidad	1 instancia virtual
Formato	Appliance virtual desplegado en la infraestructura de virtualización de la ARCOM
Marca/Modelo	A declarar por el oferente; compatible con los equipos de seguridad perimetral ofertados. Versión de software vigente, soportada por el fabricante y sin anuncio de fin de venta o de soporte a la fecha de la oferta.
Plataforma	
Virtualización	Compatible con VMware ESXi, que es la plataforma disponible en la ARCOM
Recursos	Recursos de procesamiento, almacenamiento y memoria RAM que serán provistos por la ARCOM
Capacidad	
Volumen de registros	Al menos 5 GB por día
Tasa de recepción sostenida	Al menos 1.000 registros por segundo
Retención para análisis	Al menos 15 días en línea; archivo del excedente según el almacenamiento asignado
Depuración	Depuración automática de logs antiguos según una política configurable
Monitoreo, Control y Auditoría	
Recolección y visualización	- Recolección y consolidación de logs de tráfico, seguridad y auditoría de los equipos de seguridad perimetral. - Recepción de logs de los switches Core y de acceso. - Visor de logs con filtros por objetos (hosts, redes, grupos, usuarios), búsqueda por texto libre y navegación desde vistas generales hasta el detalle. - Panel unificado de eventos de firewall, VPN, IPS, control de aplicaciones, filtrado URL, antimalware y anti-botnet. - Estadísticas históricas y en tiempo real sobre el desempeño de CPU y memoria de los equipos administrados. - Vistas históricas por hora, día, semana, mes o rango personalizado. - Incluirá mecanismos de navegación en tiempo real desde

PLATAFORMA DE GESTIÓN DE REGISTROS Y REPORTERÍA	
Característica	Especificación técnica
	vistas de alto nivel hasta registros granulares de aplicaciones, usuarios o eventos específicos.
Auditoría	• Historial de cambios de configuración y de políticas de los equipos, con administrador responsable, fecha y hora. • Los logs de auditoría se presentarán separados de los logs de tráfico. • Protección de la integridad de los logs almacenados frente a modificaciones.
Reportes y notificaciones	• Al menos 10 plantillas de reportes predefinidas, personalizables, por ejemplo: Top de aplicaciones más usadas, Amenazas bloqueadas por día, Usuarios con más tráfico, etc. • Programación automática diaria, semanal o mensual, con hora de generación definida. • Exportación como mínimo en PDF y CSV. • Alertas por consola y correo electrónico; envío automático de reportes por correo.
Integración	• Reenvío de logs a un servidor syslog externo o a un SIEM.
Seguridad y administración	
Seguridad de la plataforma	• Acceso por HTTPS y SSH (sin protocolos no cifrados). • Perfiles por rol con permisos granulares (al menos administración y monitoreo). • Autenticación integrada con el Directorio Activo. • Respaldo y restauración de la configuración de la plataforma y de los logs.
Soporte y licenciamiento	
Licencias y soporte	Licencias para la capacidad requerida y soporte técnico del fabricante 24x7 por al menos 2 años.
Implementación	Se entregarán configurados al menos 3 reportes, definidos con la DTIC para necesidades concretas de la ARCOM, así por ejemplo: reporte semanal de seguridad, reporte mensual de consumo de Internet, etc.

Administración Centralizada de la Solución

Característica	Especificación técnica
Consola única de switches	Los switches Core y de acceso se administrarán desde una única consola centralizada, que podrá estar integrada en los equipos de seguridad perimetral o ser una plataforma de gestión (en sitio o en la nube del fabricante) incluida en la oferta con su licenciamiento por el período de soporte.
Funciones de la consola	Inventario; configuración de VLAN y puertos; plantillas; monitoreo de estado, PoE y alarmas; actualización de firmware.
Compatibilidad	Las versiones de firmware o software de todos los componentes ofertados (firewalls, switches, consola de gestión y reportería) deberán ser compatibles entre sí. El oferente presentará un documento o matriz de compatibilidad.
Actualizaciones	Si para la integración se requiere actualizar el firmware de algún componente, el contratista lo ejecutará sin costo adicional y será responsable del correcto funcionamiento de la solución.
Administración local	Sin perjuicio de la consola centralizada, cada equipo deberá poder administrarse de forma local (consola, SSH y HTTPS).

Condiciones generales aplicables a todos los bienes

- **Estado de los bienes:** nuevos, de primer uso, no remanufacturados ni reacondicionados, en su empaque original del fabricante.
- **Marca y modelo:** Todos los componentes de cada ítem (equipos, módulos, transceivers y licencias)

deberán ser compatibles y soportados por el fabricante de los equipos ofertados.

- **Respaldo del fabricante:** el oferente presentará carta de autorización del fabricante o de su distribuidor autorizado en el Ecuador, específica para este proceso, que certifique la procedencia legítima de los bienes, la garantía y el soporte técnico ofertados.
- **Vigencia del producto:** a la fecha de presentación de la oferta, los modelos ofertados no deberán tener anuncio de fin de venta (End of Sale) ni de fin de soporte (End of Support). El sistema operativo o firmware deberá corresponder a una versión vigente y soportada por el fabricante.
- **Verificación:** el cumplimiento se verificará con documentación técnica oficial y pública del fabricante (hojas de datos, guías de administración o de configuración). Los valores de desempeño se tomarán de la hoja de datos oficial del modelo ofertado. El oferente presentará una matriz de cumplimiento punto por punto con la referencia de cada respaldo (documento, página o URL).
- **Garantía técnica:** no inferior a la otorgada por el fabricante y, en ningún caso, menor a dos (2) años contados desde la suscripción del acta de entrega-recepción. Incluye reemplazo de partes y piezas o del equipo completo en caso de falla de fabricación.
- **Soporte, actualizaciones y licencias:** soporte técnico del fabricante en modalidad 24x7, actualizaciones de software o firmware y suscripciones por un período mínimo de dos (2) años, registrados a nombre de la ARCOM. [DTIC validar] (período unificado)
- **Mantenimiento:** el oferente presentará un plan de mantenimiento preventivo con cronograma durante el período de garantía y garantizará el mantenimiento correctivo, sin costo adicional para la ARCOM.
- **Reposición:** en caso de falla que no pueda solucionarse en sitio, el contratista proveerá un equipo de respaldo de iguales o superiores características en el plazo que se establezca en los pliegos, mientras se repara o reemplaza el equipo averiado.
- **Manuales:** se entregarán los manuales técnicos de uso, operación y mantenimiento, conforme a la Normativa Secundaria del SNCP, en formato digital.

COMPONENTE 4: SERVICIO DE IMPLEMENTACIÓN, CONFIGURACIÓN, INTEGRACIÓN, PRUEBAS Y PUESTA EN OPERACIÓN DE LA SOLUCIÓN.

1. Configuración mínima por componente

Switches de Core

- Revisión, configuración, optimización o rediseño de las VLAN existentes y creación de nuevas VLAN, conforme al nuevo diseño de red de la Oficina Matriz, aplicando mejores prácticas de TI, segmentación y seguridad.
- Integración con la solución de seguridad perimetral y con la plataforma de administración centralizada.
- Configuración de alta disponibilidad y agregación de enlaces hacia los switches de acceso y los equipos de seguridad perimetral.
- Configuración de enrutamiento, redundancia de gateway y demás servicios requeridos según el diseño.
- Incorporación a la consola de administración centralizada.
- Ejecución de pruebas de conectividad, redundancia, conmutación por falla y operación de los servicios configurados.
- Documentación de la configuración implementada y entrega de respaldos de configuración.

Switch de Acceso

- Configuración, optimización o rediseño de VLAN, conforme al diseño de red y mejores prácticas de TI.
- Configuración de puertos de acceso/troncales y enlaces hacia los switches de Core.
- Configuración de PoE y mecanismos de seguridad de puertos, según corresponda.

- Integración con los Switches Core y la plataforma de administración centralizada.
- Pruebas de conectividad y operación.
- Documentación y respaldo de la configuración implementada.

Equipos de seguridad perimetral

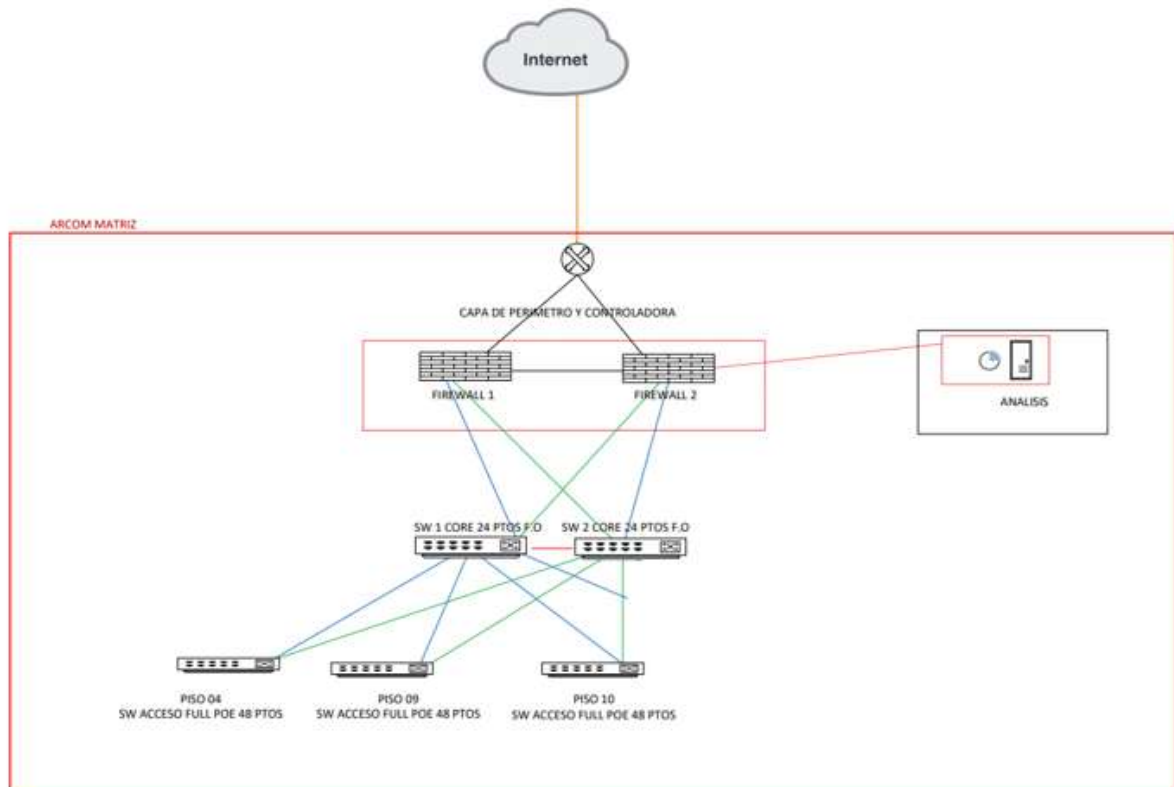
Los equipos de seguridad perimetral serán configurados para garantizar la seguridad, continuidad y disponibilidad de las comunicaciones institucionales, permitiendo el acceso controlado y seguro a los servicios internos y externos requeridos por la ARCOM, incluidos, entre otros, la conectividad con el Centro de Datos Virtual (VDC) de CNT EP, los servicios institucionales, Internet y demás recursos autorizados.

El oferente deberá considerar, como parte integral de la solución, todas las actividades, configuraciones, accesorios, materiales y servicios necesarios para su correcta implementación y funcionamiento. El proveedor deberá:

- Diseñar e implementar la solución de seguridad perimetral de acuerdo con los requerimientos técnicos establecidos por la ARCOM y las condiciones de la infraestructura tecnológica existente.
- Realizar el montaje físico, instalación, interconexión y cableado de los equipos, incluyendo todos los accesorios, componentes y materiales necesarios para su correcta instalación, operación y funcionamiento en Alta Disponibilidad (HA).
- Configurar e implementar el clúster de firewalls en modalidad Activo-Pasivo, incluyendo los mecanismos de sincronización y conmutación automática (*failover*) requeridos por la solución.
- Configurar las políticas, reglas y controles de seguridad necesarios para permitir y restringir el tráfico de acuerdo con los requerimientos institucionales, aplicando criterios de seguridad y mínimo privilegio.
- Configurar las comunicaciones y reglas de acceso necesarias para garantizar la conectividad segura con los servicios institucionales, el VDC de CNT EP, Internet y demás destinos autorizados por la ARCOM.
- Configurar e implementar las funcionalidades de seguridad requeridas y aquellas adicionales que se encuentren disponibles y soportadas por los equipos ofertados, de acuerdo con las características y licenciamiento de la solución.
- Realizar las configuraciones necesarias para la correcta integración de los firewalls con la infraestructura de red y demás componentes tecnológicos institucionales involucrados.
- Ejecutar las pruebas funcionales, de conectividad, seguridad y Alta Disponibilidad, incluyendo pruebas de conmutación (*failover*) entre los equipos, a fin de verificar la continuidad de los servicios ante la indisponibilidad de uno de los firewalls.
- Elaborar y entregar la documentación técnica de la solución implementada, incluyendo, como mínimo, diagramas de conexión, direccionamiento, configuración de alta disponibilidad, políticas de seguridad implementadas y parámetros relevantes de operación.
- Realizar la puesta en producción de la solución dentro de la ventana de mantenimiento previamente coordinada y autorizada por la ARCOM, procurando minimizar cualquier afectación a los servicios institucionales.
- Verificar, posterior a la puesta en producción, el correcto funcionamiento de los servicios y comunicaciones institucionales que atraviesan la solución de seguridad perimetral.
- Realizar el monitoreo de la solución durante un período mínimo de quince (15) días calendario posteriores a su puesta en producción, con la finalidad de verificar su estabilidad y correcto funcionamiento.
- En caso de presentarse incidentes que ocasionen una afectación parcial o total de los servicios durante el período de monitoreo, el proveedor deberá brindar la atención y soporte técnico correspondiente, incluyendo soporte en sitio cuando sea técnicamente necesario, en el menor tiempo posible, conforme a los niveles de servicio establecidos en la contratación.
- Realizar las configuraciones y ajustes necesarios que permitan optimizar el funcionamiento de la solución durante el período de implementación y estabilización.

2. Diseño de Arquitectura de Red Esperada

El proveedor se registrará al siguiente diseño de arquitectura de red proporcionado por la ARCOM, garantizando la compatibilidad, escalabilidad y seguridad de la infraestructura tecnológica de la Oficina Matriz.



3. Conectividad y Configuración de los Equipos

Componente 1: Switches CORE

a) Conectividad entre switches Core

- Los switches Core estarán en un diseño de core colapsado en alta disponibilidad Activo - Activo para lo cual entre los switches Core se deberán interconectar al menos a 40 Gbps a través de Direct Attach Cables (DAC).
- Los switches Core deberán contar con fuente redundante de poder.
- Los switches Core soportarán las conexiones con los Switches de data center a 40 Gbps y a 10 Gbps.

b) Conectividad entre switches Core – Switches de Acceso

- Los Switches Core soportará todos los switches de acceso de la oficina matriz. La ARCOM dispone de enlaces redundantes.
- Cada switch de acceso se conectará a través de los enlaces redundantes que dispone la ARCOM en cada piso, a través de al menos dos enlaces de 10 Gbps a cada uno de los switches Core en la oficina Matriz.

c) Conectividad entre Switches Core – Equipos de Seguridad Perimetral

- Los switches Core deberán conectarse a la capa de Seguridad Perimetral a través de enlaces de al menos 10 Gbps a cada uno de los equipos que formarán parte de la Seguridad Perimetral en Alta Disponibilidad

Componente 2: Switches de Acceso

a) **Conectividad entre Switches de Acceso y Switches Core (Matriz)**

- Los switches de Acceso en el edificio matriz de la ARCOM estarán conectados a los Switches Core a través enlaces de 10 Gbps a cada uno de los switches Core.

Componente 3: Equipos de Seguridad Perimetral

a) **Conectividad** entre Firewalls de Seguridad Perimetral y Switches Core

- Los Equipos Firewall de seguridad Perimetral deben estar conectados hacia cada uno de los equipos de los Switches Core a través de dos interfaces 10Gbps (SFP+).

b) **Conectividad** Firewalls de Perímetro y Proveedor de Internet

- Los Equipos Firewalls de Perímetro deberán conectarse hacia el switch o router del proveedor de servicio de Internet contratado por la ARCOM.

Componente 4: Reportaría Centralizada

a) **Conectividad de la Gestión Centralizada de Equipos de seguridad perimetral**

- La solución de gestión centralizada estará hosteado en servidores virtuales provistos por la ARCOM.

4. Arquitectura Core Colapsado

Se implementará una arquitectura de red y seguridad optimizada con equipos de seguridad perimetral para la ARCOM, migrando desde la actual topología de Core colapsado hacia una solución con equipamiento que permita crecimiento escalable (colapsada en alta disponibilidad). La implementación de la solución de ADQUISICIÓN E IMPLEMENTACIÓN DE SEGURIDAD PERIMETRAL Y EQUIPAMIENTO ACTIVO DE RED PARA LA MATRIZ DE ARCOM contará con la información provista por la ARCOM y deberá ser aplicada.

5. Soporte técnico post-instalación

El proveedor deberá brindar soporte técnico post-instalación por un mínimo de treinta (30) horas, contadas a partir de la puesta en producción de la solución, para atender requerimientos relacionados con la solución implementada.

El soporte podrá comprender, entre otras, las siguientes actividades:

- Diagnóstico y resolución de incidentes.
- Análisis de eventos y alertas de seguridad.
- Cambios y ajustes de configuración.
- Creación, modificación o revisión de políticas de seguridad.
- Optimización de la configuración de los firewalls.
- Revisión de la configuración de Alta Disponibilidad.
- Análisis de eventos de conmutación (failover).
- Asesoramiento técnico para la administración y operación de la solución.
- Apoyo en la identificación y solución de problemas de conectividad asociados a la solución implementada.

Cuando la naturaleza del incidente lo requiera, el proveedor deberá brindar **soporte en sitio**, sin que esto genere costos adicionales para la ARCOM, dentro de las condiciones y tiempos establecidos en la contratación.

6. Transferencia de conocimientos

El proveedor deberá realizar la transferencia de conocimientos por un mínimo de veinte (20) horas,

dirigida a mínimo cuatro (4) funcionarios de la DTC designados para la administración y operación de la solución.

La transferencia deberá abordar, como mínimo:

- Administración y operación de los firewalls.
- Gestión y modificación de políticas de seguridad.
- Administración y monitoreo del clúster de Alta Disponibilidad.
- Procedimientos de conmutación y recuperación ante fallas.
- Monitoreo de eventos, alertas y registros.
- Diagnóstico y atención de incidentes.
- Gestión de configuraciones y respaldos.
- Buenas prácticas para la administración y seguridad de la solución.
- El proveedor deberá entregar el material técnico utilizado durante la transferencia de conocimientos, en formato digital, como parte de la documentación de la solución.

ESPECIFICACIONES ADICIONALES:

Evolución futura

La solución deberá, además, permitir su evolución futura, incluyendo la posibilidad de implementar un enlace de Internet de respaldo para la Oficina Matriz y las Direcciones Distritales a nivel nacional, como mecanismo adicional para fortalecer la continuidad de los servicios tecnológicos institucionales.

Traslado de equipos en caso de traslado de oficina Matriz

En caso de que la Oficina Matriz de la ARCOM se traslade a una nueva infraestructura, el proveedor deberá realizar el traslado de los equipos que forman parte del proceso de contratación con todas las configuraciones y requerimientos necesarios para garantizar la normal operación de los servicios institucionales de la ARCOM, en coordinación con la DTIC.

4. DATOS MÍNIMOS QUE DEBE CONTENER LA PROFORMA:

1. Razón Social	
2. Numero de Ruc	
3. Fecha Actual	
4. Numero de Proforma	
5. Cantidad	
6. Detalle de los bienes / servicios/ obras/ consultoría	
7. Valor Unitario	
8. Subtotal	
9. Impuestos	
10.Valor Total	
11. Forma de pago	
12. Vigencia de la Proforma	
13. Plazo de Entrega	
14. Firma	
15. Copia del RUC	
16. Copia de RUP	
17. Tipo de Garantía	
18. Plazo de Garantía	

5. FIRMAS DE RESPONSABILIDAD

Descripción	Servidor	Firma
Revisado y Aprobado por:	Mgs. Carlos Omar Ordóñez Mora Director de Tecnologías de la Información y Comunicación	 Validar únicamente en FirmaEC. Firmado electrónicamente por: CARLOS OMAR ORDOÑEZ MORA
Elaborado por:	Ing. Enma Edith Salazar Orellana Especialista Tecnológico	 Validar únicamente en FirmaEC. Firmado electrónicamente por: ENMA EDITH SALAZAR ORELLANA