República de Colombia Ministerio de Igualdad y Equidad INSOR Instituto Nacional para Sordos	**FICHA DE CONDICIONES TÉCNICAS**	**FECHA:** 17/03/2025

1. CONDICIONES BÁSICAS

A. Objeto

Adquisición, instalación y configuración de solución de seguridad perimetral y WIFI en las instalaciones del INSOR.

B. Plazo de ejecución

El Plazo de ejecución del contrato, será de dos (2) meses contados a partir de la fecha de perfeccionamiento y cumplimiento de los requisitos de ejecución, en todo caso no podrá sobrepasar el 31 de diciembre de 2025.

C. Lugar de ejecución del contrato

El lugar de ejecución del contrato será en la ciudad de Bogotá en la sede del INSOR.

2. CLASIFICACION UNSPSC

A. Clasificación

Código UNSPSC	Segmento	Familia	Clase
81111500	81 - Servicios basados en ingeniería, investigación y tecnología	11 - Servicios informáticos	15 - Ingeniería de Software o hardware
43221700	43 difusión de tecnologías de información y telecomunicaciones	22 – Equipos o plataformas y accesorios de redes multimedia o de voz y datos	17 equipo de red y componentes
43222500	43 difusión de tecnologías de información y telecomunicaciones	22 – Equipos o plataformas y accesorios de redes multimedia o de voz y datos	25 equipo de seguridad de red

3. ESPECIFICACIONES TÉCNICAS DE PRODUCTOS O SERVICIOS REQUERIDOS

Descripción general de los Bienes y/o Servicios a contratar

Actualmente, la entidad cuenta con dos dispositivos de seguridad perimetral configurados en alta disponibilidad y que suministran servicios de seguridad, tales como, filtrado web, filtrado de descargas, inspección de información entrante y saliente, gestión de NATS para la publicación de servicios, conexiones vía VPN y VPN SSL (limitadas), log de eventos de los diferentes servicios, integración con el servicio de directorio activo. Así mismo, la entidad cuenta con el servicio de conectividad WIFI, la cual se gestiona desde los dispositivos de seguridad perimetral y sobre la cual se filtran contenidos de dispositivos conectado inalámbricamente.

En cuanto a dispositivos de seguridad perimetral existe una característica, la cual está dada en la capacidad de filtrado de información y la capacidad de detección de amenazas, las cuales han venido evolucionando con el crecimiento de tecnologías emergentes y de los diferentes métodos de violación y vulnerabilidad que cada vez se hacen más robustas y por lo tanto, para mitigar dichos riesgos que general la exposición de la infraestructura hacia la Web, hay que evolucionar con dispositivos con mecanismos de seguridad acorde con la evolución. Por lo anterior se hace necesario involucrar en la infraestructura de la entidad, en el tema de seguridad dispositivos de nueva general (NGFW) que cuenten con capacidades, herramientas y mecanismos de detección, respuesta y mitigación de vulnerabilidades que puedan acarrear un riesgo a los servicios y la información que maneja la entidad.

Los dispositivos de seguridad perimetral cuentan actualmente con soporte de fábrica y el licenciamiento correspondiente. Por parte de fábrica se ha indicado el fin de vida (EOL) para dichos dispositivos en la presente vigencia (2025-09-30), lo que hace necesario la renovación de equipos por dispositivos de nueva generación.

Por otro lado, en cuanto a la solución de WIFI, actualmente se cuenta con dispositivos que ya se encuentran obsoletos en cuanto a capacidades de gestión, cobertura y niveles de seguridad que limitan la aplicación de políticas, métodos de autenticación y gestión de vulnerabilidades a través de la red inalámbrica.

Así mismo, teniendo en cuenta que los dispositivos inalámbricos son gestionados desde los dispositivos de seguridad perimetral, los cuales se pretenden renovar, se hace necesario el reemplazo de dichos dispositivos (Access Point) por dispositivos de nueva generación con capacidades de cobertura más amplias, mecanismos de seguridad más eficientes y actualizados. Por lo anterior se hace necesario la adquisición de dispositivos que cumplan con los estándares de seguridad y desempeño actualizados.

4. DESCRIPCIÓN ESPECÍFICA DE LOS BIENES Y/O SERVICIOS A CONTRATAR

4.1. CRONOGRAMA

El contratista en los primeros cinco (5) días hábiles una vez iniciada la ejecución del contrato deberá elaborar y presentar un cronograma y plan de trabajo, previa concertación con el supervisor del contrato.

REQUERIMIENTOS TECNICOS MÍNIMOS

El oferente debe cumplir con todos los requerimientos y soportes solicitados en cada uno de los ITEMS objeto de contratación.

1. SOLUCION DE PROTECCION PERIMETRAL	
Denominación técnica:	Dos (2) Next Generación Firewall
ESPECIFICACIONES TÉCNICAS	
1.1 GENERALIDADES	Se requiere el suministro, instalación, configuración y soporte técnico del sistema de Seguridad perimetral tipo Next Generation Firewall. Las actividades de instalación, configuración y puesta en producción de los equipos ofertados deberán ser realizadas por personal certificado por el fabricante Solución en alta disponibilidad, dos equipos de la misma referencia y marca funcionando en modo clúster.
	El equipo debe contar con soporte técnico y retorno por parte del fabricante por un periodo mínimo de **3 años** en un esquema 7 x 24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono.
	Cada equipo debe ocupar una unidad (1) de racks, debe incluir su respectivo kit de montaje para la instalación física donde indique el supervisor designado para el contrato.

	Es responsabilidad del contratista la instalación, configuración y puesta en marcha de la solución conforme las necesidades de la Entidad y la verificación del supervisor designado para el contrato.
	El dispositivo debe ser un equipo de arquitectura integrada de propósito específico para ofrecer un alto rendimiento y baja latencia.
	El equipo debe tener un rendimiento alto de firewall para tráfico IPv4 e IPv6.
	El dispositivo debe soportar prevención de intrusos basada en anomalías, desfragmentación de paquetes y descarga de checksum.
	El equipo debe soportar VPN, CAPWAP, aceleración de túneles IP, traffic shapping y prioridad de colas.
	El dispositivo deberá incluir aceleración de inspección de contenido basada en firmas, tráfico cifrado y texto claro.
	El fabricante de la solución debe estar validado a nivel de rendimiento y seguridad por los siguientes laboratorios de pruebas de terceros, líderes en la industria de protección: NSS Labs, VB100, AV Comparatives e ICSA.
	El dispositivo debe controlar miles de aplicaciones, bloquear los últimos exploits y filtrar tráfico web basado en millones de clasificaciones de URLs en tiempo real.
	El equipo debe estar respaldado por un laboratorio de investigación y desarrollo que ofrezca inteligencia en tiempo real entregando actualizaciones de seguridad completas, investigadores de amenazas de seguridad.
	El dispositivo debe proporcionar información granular para aplicaciones basadas en nube, tales como: YouTube, Dropbox, Baidu, Microsoft Office 365, Amazon, entre otras.

		El dispositivo debe tener una base de datos que contenga una lista de direcciones Botnet C&C que sean actualizadas dinámicamente y almacenadas en el NGFW.
		El nivel de soporte del fabricante debe incluir tiempo de respuesta de 2 horas hábiles para situaciones no criticas y 15 minutos para situaciones críticas.
1.2	**RENDIMIENTO**	Rendimiento de Firewall (paquetes de 1518 Bytes): 35 Gbps Rendimiento de IPS en tráfico de mix empresarial: 5 Gbps Rendimiento de NGFW: 3 Gbps Rendimiento Inspección SSL: 2.8 Gbps Rendimiento VPN IPSec: 35 Gbps Soporte de mínimo 3.000.000 sesiones concurrentes
1.3	**CONECTIVIDAD**	El equipo deberá contar minimo con las siguientes interfaces de conexión. • Un (1) puerto USB • Un (1) puerto Consola • Dos (2) interface de administración/alta disponibilidad • 16 interfaces GE RJ45 • 4 Interfaces 10 GE SFP+ • 8 Interfaces 10 GE SFP
1.4	**NAT/PAT**	**Traducción de direcciones de red** NAT dinámico, NAT estático, PAT, NAT64, NAT46, NAT 66
1.5	**FUNCIONES BÁSICAS DE FIREWALL**	Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs.
		La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios.

		El equipo deberá poder contar con la característica de modo de aprendizaje para políticas de firewall, cuyo objetivo sea monitorear el tráfico para determinar cuáles restricciones y protecciones se deben aplicar.
		Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario).
		La solución tendrá la capacidad de hacer captura de paquetes por política de seguridad implementada para luego ser exportado en formato PCAP.
		Tendrá la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para este análisis.
		Funcionalidad de DHCP: como Cliente DHCP, Servidor o Relay de solicitudes DHCP.
1.6	**CONECTIVIDAD Y ENRUTAMIENTO**	Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.
		Soporte a rutas estáticas para IPv4 o IPv6.
		Soporte de enrutamiento basado en políticas para IPv4 e IPv6, para envió de tráfico de diferentes tipos basado en protocolo de tráfico entrante, dirección o interfaz fuente, dirección destino o número de puerto.
		Soporte a ruteo dinámico RIP, RIPNG, OSPF, OSPFv3, BGP (para IPv4 e IPv6), IS-IS
		Soporte de ECMP (Equal Cost Multi-Path)
		Soporte a ruteo de multicast PIM SM y PIM DM.
		Soporte de reverse path lookup o anti-spoofing.
		Soporte de rutas blackhole

		La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow o Netflow.
		Soporte de SDWAN
		Clasificación de aplicaciones para determinación de camino.
		Monitoreo de salud de enlaces WAN mediante Ping, HTTP, tcp Echo, UDP Echo.
		Monitoreo de métricas de salud por aplicación (al menos latencia, jitter y pérdida de paquetes).
		Asignación de camino basada en identidad (usuario y/o grupo).
		Aplicación de estrategias de SLA basadas en las métricas de verificación.
1.7	**VPN IPSEC**	El equipo deberá soportar las siguientes características: Soporte a certificados RSA X.509 para construcción de VPNs cliente a sitio (client-to site).
		Soporte de VPNs IPSec sitio a sitio y cliente – sitio.
		Soporte para IKEv2 e IKE Configuration Method
		Soporte de VPNs con algoritmos de cifrado: AES256, AES192, AES128, DES, 3DES
		Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
		La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)
		Se deben soportar VPNs basadas en rutas y VPNs basadas en políticas.
1.8	**VPN SSL**	Capacidad de realizar SSL VPNs sin necesidad de licenciamiento por usuarios.
		Soporte para modo de operación basado en web o modo túnel.
		Soporte a certificados RSA X.509 para construcción de VPNs SSL.
		Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado

		digital además de una contraseña para lograr acceso al portal de VPN.
		Soporte de autenticación de dos factores con token, la solución debe estar en la capacidad de suplir o integrarse con tokens físicos o basados en software.
		Validación de equipos de plataformas Windows mediante la comprobación de sistema operativo, firewall de Windows, antivirus para obtener acceso mediante VPN SSL.
		Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet
		Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL
		Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo con el grupo de pertenencia de dichos usuarios.
		La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información.
1.9	**AUTENTICACIÓN**	El dispositivo deberá manejar los siguientes tipos de autenticación:
		Autenticación basada en contraseña y en doble factor de autenticación (certificado, correo, SMS y tokens).
		Capacidad de integrarse con Servidores de Autenticación: RADIUS, LDAP, TACACS+, POP3, SSO y RSA ACE.
		Capacidad incluida, al integrarse con Microsoft Windows Active Directory o Novell eDirectory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto “Single-Sign-On”.

		El equipo debe soportar traffic shaper basado en fuente (dirección IP, usuarios locales y grupos), destino (dirección IP, FQDN, URL o categoría), servicio (General, acceso web, acceso a archivos, servicios de correo y red, autenticación, acceso remoto, tunneling, VoIP, mensajería y otras aplicaciones, web proxy), aplicación, categoría de aplicaciones, categoría de URLs.
1.10	**MANEJO DE TRAFICO**	El equipo debe permitir la configuración de reglas de prioridad de tráfico por dirección fuente, grupo de usuarios, dirección destino, numero de protocolo y aplicaciones basadas en nube.
		Capacidad de poder definir ancho de banda garantizado y máximo.
		Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer antivirus en tiempo real en al menos los siguientes protocolos: HTTP, SMTP, IMAP, POP3, FTP, NNTP, HTTPS, IMAPS, POP3S, SMTPS y FTPS.
1.11	**ANTIMALWARE**	Debe mitigar las siguientes amenazas: Virus, gusanos, troyanos, ransomware, scareware, spyware, adware, botnets, entre otros.
		El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de esta.
		El Antivirus deberá poder configurarse de forma que los archivos que pasan sean totalmente capturados y analizados, permitiendo hacer análisis sobre archivos que tengan varios niveles de compresión.
		El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6
		El antivirus deberá escanear tráfico de compartición de archivos: CIFS, SMB y SAMBA.

		La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C.
1.12	**FILTRADO WEB**	La solución debe permitir filtrado de contenido web, filtrado de URLs y servicio de filtrado web basado en firmas desarrolladas por laboratorio de investigación y desarrollo propio del fabricante. Debe poder categorizar contenido Web requerido mediante IPv6.
		Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
		La solución de Filtrado de Contenido debe soportar la característica de "Safe Search" o "Búsqueda Segura" para prevenir imágenes y sitios web con contenido explícito en los resultados de búsqueda. Esto debe ser soportado para los siguientes sitios: Google, Yahoo, Bing y Yandex.
		Será posible exceptuar la inspección de HTTPS por categoría.
		El filtrado de contenido web debe permitir la definición de palabras, frases, patrones, wildcards y expresiones regulares Perl para prevenir acceso a páginas con material cuestionable.
		El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en categoría, grupo de categoría o clasificación.
		La solución debe poder aplicar distintos perfiles de navegación de acuerdo al usuario que se esté autenticando. Estos perfiles deben poder ser aplicados a usuarios o grupos de usuarios
		El filtrado debe ser sobre tráfico HTTP y HTTPS.
1.13	**PROTECCIÓN CONTRA INTRUSOS (IPS)**	El sistema de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en spam o mirror.

		Deberá ser posible seleccionar el sistema operativo, protocolo, severidad y objetivo para la configuración de perfiles IPS.
		Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6 a través de sensores.
		El IPS debe tener la posibilidad de tomar las siguientes acciones: permitir, monitorear, bloquear, resetear la sesión, guardar copia de los paquetes que coincidan con las firmas, hacer cuarentena con base en dirección IP del atacante y tiempo basado en días, horas o minutos.
		El sistema de protección de intrusos debe utilizar decodificadores de protocolo para identificar patrones de tráfico anormal que no reúnan los requerimientos de protocolo y estándares.
		Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)
		El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo. La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso
		El sistema de detección y prevención de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / Rate base).

1.14	**CONTROL DE APLICACIONES**	Debe basarse en categorías que permitan seleccionar grupos de firmas basados en un tipo de categoría. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
		La solución debe tener un listado de al menos 2300 aplicaciones ya definidas por el fabricante.
		El listado de aplicaciones debe actualizarse periódicamente.
		Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, hacer traffic shapping, registrar en log, ver firmas y bloquear acceso a una aplicación por un periodo de tiempo específico basado en días, horas y minutos.
		Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.
		Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.
		Debe ser posible inspeccionar aplicaciones tipo Cloud como YouTube, Dropbox, Baidu, Amazon entre otras entregando información como login de usuarios, transferencia de archivos y videos visualizados.
1.15	**INSPECCION DE SSL**	La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3. Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de la entidad.
		El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de

		Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS
		Debe ser posible inspeccionar tráfico SSH y funcionalidades como Exec, Port-Fortward o X11.
1.16	**ALTA DISPONIBILIDAD**	El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6
		Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico.
		Posibilidad de definir al menos dos interfaces para sincronía
		El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red
		Posibilidad de definir interfaces de gestión independientes para cada miembro en un clúster
		Debe ser posible definir que Firewall Virtual estará activo sobre que miembro del Cluster para hacer una distribución de carga en caso de necesario.
		El equipo debe soportar hasta 4 equipos en esquema de HA.
1.17	**VISIBILIDAD**	La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. El equipo debe permitir la visualización de la topología física y lógica, con el fin de obtener más información de los dispositivos y conexiones.
		El equipo debe entregar las siguientes consolas para reunir los siguientes objetivos: Políticas Interfaces Países Traffic shaping

		Mapa de amenazas Autenticaciones fallidas
		Menú tipo dropdown para navegar por la información.
		Mostrar los orígenes del tráfico o usuarios que lo generan
		Mostrar las aplicaciones y su categorización según riesgo.
		Visibilidad de aplicaciones Cloud usadas por el usuario.
		Visibilidad de destinos del tráfico.
		Visibilidad de los sitios web más consultados por los usuarios.
		Visibilidad de las amenazas o incidentes que han ocurrido en la red
		En la información de fuentes, aplicaciones, navegación debe ser posible con un doble click filtrar la información para ser más específica la búsqueda.
1.18	**ADMINISTRACIÓN**	Interface gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interface debe soportar SSL sobre HTTP (HTTPS) Interface basada en línea de comando (CLI) para administración de la solución.
		Puerto de consola dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.
		El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales.
		Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.
		Soporte de SNMP versión 2 y SNMPv3

		Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos
		Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
		Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica.
		Contar con facilidades de administración a través de la interfaz gráfica como ayudantes de configuración (setup wizard).
1.19	**VIRTUALIZACIÓN**	El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains" La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS.
		Se debe incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer.
		Cada instancia virtual debe poder tener un administrador independiente
		La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.
		Cada instancia virtual deberá poder estar en modo Gateway o en modo transparente a la red
		Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual
		Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual.
		Se debe poder ver el consumo de CPU y memoria de cada instancia virtual.
1.20	**Logs, Analítica y Reportes**	Se debe incluir capacidad de almacenamiento de Logs históricos, Analítica y Reportes en Nube para el Firewall en HA ofertado.
		Incluir capacidad de retención de Logs en nube.

		Capacidad de recibir y almacenar todos los tipos de logs o registros generados por la plataforma firewall en nube.
		Incluir Indicadores de Compromiso para analizar los logs contra IPs, dominios o URLs conocidas como maliciosas.
		Capacidad de toma de acciones basado en los logs e incidentes recibidos para automatizar acciones por medio de scripts y conectores preestablecidos
		Visualización de amenazas basado en modelo de Purdue y Mitre
		Contar con informes predeterminados de amenazas y cumplimiento.

2. SOLUCIÓN DE CONECTIVIDAD WIFI ACCESS POINT Y SWITCH PoE		
Denominación técnica:		Solución de conectividad red inalámbrica de nueva generación
Cantidad:		Once (11) AP y un (1) switch de conectividad y alimentación
ESPECIFICACIONES TÉCNICAS		
2.1	**GENERALIDADES**	La modernización tecnológica a nivel de conectividad de la entidad plantea la renovación de la solución WIFI compuesta por hardware, software y comunicaciones con herramientas de última generación, que asegure cobertura, disponibilidad, rendimiento y seguridad de los servicios informáticos que consumen los usuarios mediante WIFI. Dentro de las características esperadas de la solución a contratar, tenemos las funcionalidades de alta velocidad de acceso WIFI para mejorar los tiempos de respuesta de los servicios de la entidad y el análisis y protección ante eventos de seguridad informática que puedan colocar en riesgo los activos estratégicos de la entidad. En este sentido se requiere que la solución a contratar posea características robustas de seguridad y capaces de integrarse de forma nativa a la solución de ciberseguridad perimetral ofertada para ser gestionadas desde allí, así mismo aumentar la visibilidad, monitoreo, control y capacidad de respuesta ante cualquier incidente relacionado con el acceso seguro.

2.2	**CARACTERÍSTICAS**	Toda la solución ofertada debe ser mono marca (con los Access Point) incluyendo los accesorios de conectividad Permitir control de acceso basado en roles (RBAC) integrado para delegar roles y permisos a diferentes administradores Administración del dashboard para validar el estado de la red El oferente debe garantizar el suministro de los elementos necesarios para el buen funcionamiento de la red y el cumplimiento del objeto del presente proceso El Instituto Nacional para Sordos posee la infraestructura de datos y los puntos cableados para la instalación y configuración de los Access point La solución ofertada debe ser mono-marca para los Firewalls con capacidades de Analítica y reportes en Nube, Switch para conectividad y alimentación PoE de Puntos de Acceso, y Access points, Las actividades de instalación, configuración y puesta en producción de los equipos ofertados deberán ser realizadas por personal certificado por el fabricante.
2.3	**CARACTERÍSTICAS TÉCNICAS AP**	La solución debe soportar las siguientes características: AP de uso interno WIFI-7 **Características avanzadas 802.11** UL MU-MIMO DL MU-MIMO OFDMA TWT **Hardware** Numero de radios: 4-Radio 2.4GHz + 5.0GHz + 6GHz + Tri-band scan Bandas de frecuencia: banda 2.4GHZ ISM 2.4-2.484GHz, banda 5.0GHZ UNII-1 5.15-5.25GHz, UNII-2A 5.25-5.35GHz, UNII-2C 5.47-5.73GHz, UNII-3 5.725-5.85GHz, UNII-4 5.85-6.895GHz SSID simultáneos: mínimo 24 Tipos de SSID: Local-Bridge, Mesh, and Tunnel Autenticación: WPA, WPA2, and WPA3 with 802.1x or Preshared key, WEP, Web Captive Portal, MAC blacklist and whitelist Tipo de antena y ganancia: PIFA antena Dual band: 4.5dBi for 2.4Ghz and 5.5dBi for 5GHz PIFA BLE antena 5.2 dBi at 2.4GHz band

		Tasa máxima de datos: 2.4GHz band: up to 688 Mbps, 5.0GHz band: up to 4.324 Gbps, 6.0GHz band: up to 5.765 Gbps Soporte para Sniffer Mode Soporte analizador de espectro Clientes por radio: 512 Cantidad: 11 Puntos de Acceso
2.4	**CARACTERÍSTICAS DE CONECTIVIDAD Y ALIMENTACION (SWITCH)**	Interfaces: 16 x GE RJ45 8 x 2.5 GE RJ45 2x 5 GE RJ45 4x 10 GE SFP+ ports PoE Power Budget 420 W Cantidad 1 Switch de conectividad PoE.
2.5	**MODO DE OPERACIÓN**	La solución deberá contar con la capacidad de detección de Access Points intrusos Modos de operación: Local-Bridge, Tunnel, y Mesh La solución debe poder implementar políticas de seguridad tipo WIPS La solución deberá tener la capacidad de detectar un Access Points intruso cuando es puesto en la red cableada La solución de red inalámbrica deberá permitir la implementación de portales cautivos sin necesidad de equipos adicionales Soporte para Kensington Lock
2.6	**CERTIFICADOS**	Los equipos ofertados deben cumplir con la certificación WiFi Alliance Certified Los equipos ofertados deben cumplir por lo menos con una norma de cuidado del medio ambiente y/o manejo eficiente de energía, para lo cual el proponente debe adjuntar la ficha técnica del fabricante donde se pueda corroborar el cumplimiento de este requerimiento.

3. SERVICIOS ASOCIADOS, GARANTIA Y MANTENIMIENTO SOBRE PLATAFORMAS OFERTADAS		
ESPECIFICACIONES TÉCNICAS		

3.1	**SOPORTE Y GARANTÍA**	Debe contar con soporte y mantenimiento directo con fábrica en la modalidad 7X24 con cambio de partes por tres (3) años. Los componentes ofertados deben ser nuevos de fábrica, no remanufacturados, ni reparados, ni reacondicionados en ninguna de sus partes. El soporte debe ser en un esquema 7x24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos. El proponente deberá atender y resolver cualquier problema técnico de la solución, en un esquema de atención 5x8 (telefónico, e-mail, acceso remoto o presencial en caso de que así se requiera), este soporte deberá ser suministrado por personal especializado en la herramienta. El servicio de soporte debe incluir atención de incidentes y consultas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil. Para ello debe contar con un centro de servicio que cumpla con mínimo: • Software de Mesa de Servicio en la Nube, donde se puedan registrar casos o incidentes de forma web, correo o teléfono. • Nivel de soporte 1 para atención remota, 2 para atención en sitio y 3 para soporte de especialista y escalamiento a fábrica. Al finalizar cada visita correctiva el proponente generará un informe de servicio con las evidencias de estas actividades. De igual forma quedará constancia en la misma acta o informe de servicio si hubo cambio de software y/o en alguna configuración.
3.2	**REVISIÓN PREVIA DE SEGURIDAD PERIMETRAL**	El contratista deberá recopilar información general sobre la solución de seguridad perimetral que utiliza la Entidad y presentar un reporte con observaciones de carácter general, tomando como referencia lineamientos comunes de buenas prácticas basadas en normas standard tales como NIST e ISO 27001, con el fin de que el Instituto Nacional para Sordos cuente con insumos que le permitan conocer de manera preliminar el estado actual de su configuración e identificar posibles acciones de mejora en materia de ciberseguridad aplicables a la solución a adquirir.
3.3	**SERVICIOS DE SEGURIDAD**	El contratista deberá realizar un seguimiento mensual del rendimiento y operación de la solución de seguridad perimetral ofertada durante el periodo de soporte el cual debe entregar un informe periódico mensual con las estadísticas de operación de la solución, tendencias y recomendaciones de ciberseguridad.
3.4	**SERVICIOS PROFESIONALES**	Se debe realizar la instalación, configuración, actualización y puesta en marcha de las soluciones ofertadas.

		El contratista deberá realizar y ejecutar un protocolo de pruebas para la entrega a satisfacción de la solución, el cual será aprobado por el Supervisor del contrato. Se deben realizar las respectivas pruebas de funcionalidad y operatividad de todos y cada uno de los elementos, con el propósito de comprobar la calidad y cumplimiento de los requerimientos solicitados. Presentar plan de trabajo y cronograma de trabajo dentro de los cinco (5) días hábiles siguientes a la suscripción del acta de inicio, para aprobación del supervisor y realizar los ajustes a que haya lugar. La implementación deberá comprender los siguientes puntos: • Diseño y planeación de cada una de las actividades minimizando la afectación del servicio. • Configuración y alistamiento de la plataforma a la última versión estable aprobada por el fabricante. • Implementación de la solución de acuerdo con las mejores prácticas del fabricante, teniendo en cuenta una arquitectura de red segura. • Pruebas de Servicio. • Puesta en Producción. • Estabilización de la plataforma.
3.5	**EQUIPO DE TRABAJO**	El oferente debe contar con un equipo mínimo de trabajo para la ejecución del proyecto, el cual debe estar conformado como mínimo por: <u>Coordinador de Proyecto:</u> Uno (1) Profesional Ingeniero Industrial y/o Electrónico, y/o Sistemas y/o Telecomunicaciones con especialización en Gerencia de Proyectos, debe contar con Certificación ITILV3 o superior. Experiencia mínima de cinco (5) años a partir de la tarjeta profesional. Se debe anexar a la propuesta copia de los siguientes documentos: Cédula de Ciudadanía Tarjeta Profesional Certificados de estudio Certificaciones de experiencia Certificado de Especialización en Gerencia de proyectos e ITILV3 o Superior Hoja de Vida.

		Ingeniero de Implementación: Uno (1) Un (1) Ingeniero electrónico de Sistemas y/o Telecomunicaciones, con experiencia mínima de cuatro (4) años a partir de la tarjeta profesional, el cual debe encontrase certificado en el nivel profesional, especialista y arquitecto del fabricante ofertado, se debe anexar a la propuesta copia de los siguientes documentos: Cédula de Ciudadanía Tarjeta Profesional, Certificación del fabricante a nivel profesional, especialista y arquitecto Se solicita para el equipo de trabajo que las certificaciones de fabricante se encuentren vigentes a la fecha de presentación de la oferta Hoja de vida Ingeniero de Soporte: Uno (1) Un (1) Ingeniero electrónico, de Sistemas y/o Telecomunicaciones, con eexperiencia mínima de cuatro (4) años a partir de la tarjeta profesional, el cual debe encontrase certificado en el nivel 3 del fabricante ofertado, se debe anexar a la propuesta copia de los siguientes documentos: Cédula de Ciudadanía Tarjeta Profesional, Certificación del fabricante a nivel 3 Se solicita para el equipo de trabajo que la certificación de fabricante se encuentre vigente a la fecha de presentación de la oferta Hoja de vida

3.6	**CERTIFICADOS**	a. El oferente debe ser canal (Partner) certificado en alguno de los dos niveles más altos establecidos por la marca de membresía del fabricante de los equipos ofertados y estar en capacidad técnica de configurar, mantener y dar soporte técnico a los equipos. En consecuencia, el oferente deberá presentar la certificación del fabricante que lo acredite como Partner en alguno de los dos niveles más altos establecidos por la marca. Este documento debe ser expedido por el fabricante de los equipos ofertados con fecha no mayor a 30 días y dirigido a la entidad haciendo referencia al número de la licitación a la cual está aplicando. b. El oferente deberá entregar cuadro resumen de los elementos entregados y junto con la propuesta una certificación emitida directamente de los fabricantes de las soluciones ofertadas donde se evidencie que los equipos suministrados no se encuentran en fin de venta, estas cartas deben ser dirigidas a la Entidad.
3.7	**Transferencia de conocimiento**	a. El proveedor deberá brindar capacitación en el manejo, administración y gestión de los elementos entregados y el software que hace parte de la solución. b. El proveedor deberá presentar cronograma de capacitaciones mencionadas de mínimo para un mínimo de ocho (8) horas para el personal que designe el INSOR, máximo 4 profesionales.

5. OBLIGACIONES ESPECIFICAS DEL CONTRATISTA

1. Conocer y acatar las políticas de seguridad de la información de la entidad.
2. El oferente debe suministrar toda la infraestructura de tecnología (hardware/software) externa a INSOR y necesaria para garantizar el cumplimiento del objeto contractual.
3. Garantizar la oportuna y eficaz prestación del objeto contratado, respondiendo por la calidad de los bienes suministrados y con las características requeridas.
4. Instalar los bienes en la Carrera 89 A # 64C-30 de la ciudad de Bogotá.
5. Atender los servicios de traslado, instalación, configuración, mantenimiento preventivo, mantenimiento correctivo y capacitación sin intermediarios y con personal calificado.
6. Garantizar la calidad de los bienes entregados asegurando que sean originales, nuevos, no repotenciados ni remanufacturados y cumplan con las características ofrecidas.
7. Presentar informes de las visitas de mantenimiento, estos informes de la visita deberán incluir fecha, serial de los dispositivos revisados, diagnostico, solución y recomendaciones, así mismo las solicitadas por el supervisor del contrato.

8. Realizar las capacitaciones descritas en el anexo técnico las cuales serán programadas por el supervisor del contrato una vez se realice la entrega y puesta en funcionamiento de los bienes ofertados.
9. Responder sin perjuicio de la garantía, por la calidad de los elementos adquiridos.
10. Mantener indemne a la entidad por las reclamaciones que se deriven con ocasión a la ejecución contractual.
11. Acatar y cumplir las instrucciones que el Supervisor le imparta en relación con el objeto contractual.
12. Asistir a las reuniones que sean convocadas por el Supervisor del contrato, para revisar el estado de ejecución de este, el cumplimiento de las obligaciones a cargo del contratista o cualquier aspecto técnico referente al mismo.
13. Mantener fijos los precios de los bienes ofrecidos durante la ejecución del contrato.
14. Aportar en los plazos dispuestos las hojas de vida junto con la documentación de soporte del equipo de trabajo y Mantener durante la ejecución del contrato el personal aprobado por la Supervisión, en caso de cambio de personal se deber acreditar un perfil igual o superior al inicialmente propuesto.
15. Cumplir las demás obligaciones que se deriven de los presentes estudios previos y de la naturaleza del contrato

6. FORMA DE PAGO

El valor del contrato se pagará de la siguiente forma

- Un único pago contra la entrega a satisfacción de la solución de seguridad perimetral y Wifi instalada, configurada y puesta en marcha de acuerdo a los requerimientos de la entidad.

El INSOR pagará el valor del contrato en moneda legal colombiana, en las condiciones establecidas por el Grupo Financiero del INSOR, de acuerdo con los bienes, servicios prestados, facturados y recibidos a satisfacción por el Supervisor designado por EL INSOR, siempre y cuando el CONTRATISTA haya cumplido con la obligación exigida en el artículo 23 de la Ley 1150 de 2007 y los demás requisitos de pago pactados.

Documentos soporte para el pago:

6.1. Factura dando estricto cumplimiento a las exigencias legales que establece el artículo 617 del Estatuto Tributario, y para las facturas electrónicas lo establecido en los artículos 1.6.1.4.13 a 1.6.1.4.23 del Decreto 1625 de 2016 y las normas que lo modifiquen;

6.2. Acreditación conforme a la Ley vigente aplicable, del cumplimiento del CONTRATISTA de sus obligaciones ante el Sistema de Seguridad Social Integral en

Salud, pensiones y riesgos laborales, así como aportes parafiscales: Sena, ICBF y Cajas de Compensación Familiar, cuando corresponda;

6.3. Certificación de cumplimiento del contrato expedida por el Supervisor, en la que conste el valor a pagar al CONTRATISTA.

En el caso de factura electrónica, el contratista deberá tener en cuenta lo establecido en la Circular No. 016 de marzo 9 de 2021 emitida por el Ministerio de Hacienda y Crédito Público, la cual hace referencia al proceso de recepción de facturas electrónicas, notas crédito y notas débito, y a la implementación del "Modelo de Recepción de Facturas de Venta, Notas Débito y/o Notas Crédito", el cual aplica de forma obligatoria para todas las entidades que hacen parte del Presupuesto General de la Nación (PGN), así como lo señalado en la Circular 000003 del 16 de abril de 2021 expedida por de la UAE-DIAN, la cual dispone: "(…) … la forma de envío de la factura electrónica a SIIF, así: el contratista para "Registrar en la sección de la factura Datos del Adquiriente en el campo "Correo", el buzón electrónico siifnacion.facturaelectronica@minhacienda.gov.co.

Si las facturas no han sido correctamente elaboradas, o no se acompañan de los documentos requeridos para el pago, el término para éste sólo efecto empezará a contar desde la fecha en que el CONTRATISTA aporte el último de los documentos, de lo cual se dejará expresa constancia. La demora del CONTRATISTA en la entrega de la totalidad de los documentos que son requisito para el pago será su responsabilidad, y en consecuencia no tendrá por ello derecho al pago de intereses o compensación de ninguna naturaleza.

El CONTRATISTA no podrá librar factura alguna que no corresponda a obras y/o bienes entregados real y materialmente, o a servicios efectivamente prestados, y recibidos a satisfacción por el supervisor o interventor del contrato, según el caso. Corresponderá al supervisor o interventor del contrato, aceptar o rechazar la factura por escrito, dentro de los tres (3) días hábiles siguientes a su recepción, si considera que incluye obras y/o bienes que no han sido entregados real y materialmente, o servicios que no han sido efectivamente prestados (Art.86, L.1676/13).

El Supervisor remitirá mediante Orfeo directamente a la Coordinación del Grupo Financiero del INSOR la factura presentada por el contratista en físico con los demás documentos exigidos para el pago.

Los pagos se efectuarán, mediante consignación en la cuenta bancaria que informe el Contratista, para lo cual el Contratista deberá presentar a través de SECOP II certificación de la entidad bancaria en la que conste quién es el cuentahabiente, su identificación, el número, el tipo de cuenta y si a la fecha está activa.

NOTA: Las facturas que se tramiten para pago y que incluyan pagos por concepto de bienes devolutivos, deberán ir acompañadas del comprobante de ingreso o registro en el

aplicativo de Inventarios del INSOR, donde conste que los bienes efectivamente se recibieron en la Entidad y acta de entrega y recibo a satisfacción firmada por el Supervisor del contrato. Sin el cumplimiento de estos requisitos no se podrán realizar el trámite de pago de las facturas.

7. GARANTÍAS

Serán exigibles las garantías expresadas a continuación, pero no limitadas a ellas.

AMPARO	SI	NO	CUANTÍA	VIGENCIA
Cumplimiento	X		Por cuantía equivalente al veinte por ciento (10%) del valor del contrato.	Por el término de ejecución del contrato y doce (12) meses más.
Calidad de los bienes y/o servicios	X		Por cuantía equivalente al veinte por ciento (10%) del valor del contrato.	Por el término de ejecución del contrato y doce (12) meses más.
Pago de salarios y prestaciones sociales e indemnizaciones laborales	X		Por cuantía equivalente al diez por ciento (5%) del valor del contrato.	Por el término de ejecución del contrato y tres (03) años más contados a partir de la expedición de la garantía única.