IMPLEMENTAR SOLUCION INTEGRAL DE TELECOMUNICACIONES PARA EL INSTITUTO NACIONAL DE MEDICINA LEGAL Y CIENCIAS FORENSES A NIVEL NACIONAL

Dirección Carrera 7a, 32-16 Edificio San Martin piso 10
dinformatica@medicinalegal.gov.co
conmutadores Teléfono: +(57) 6017940883 Ext: 10907
www.medicinalegal.gov.co
Bogotá D.C, - Colombia

Tabla de Contenido

1. CONECTIVIDAD 14

2. ANEXO 2. RED LAN Y SERVICIOS ADMINISTRADOS 40

2.1 Alcance técnico del servicio 40

2.1.1 SWITCH CORE - RED LAN 43

2.1.2 Integración SD-WAN / SD-LAN / SDBranch 44

2.1.3 Interfaces ópticas y accesorios 45

2.1.4 Integración NAC (Control de Acceso a la Red) – Funcionalidad mínima 46

2.1.5 Criterios mínimos de asignación automática de VLAN: 47

2.1.6 SFP / Uplinks y compatibilidad 47

2.1.7 Migración en rack y responsabilidades 47

2.1.8 Reportes mensuales obligatorios 48

2.2 Requerimientos técnicos – Solución Wireless (WLAN) + Portal Cautivo 48

2.2.1 Alcance WLAN 48

2.2.2 Controladora y portal cautivo (sin hardware para INMLCF) 51

2.2.3 Especificaciones mínimas de Access Points 51

2.2.4 Alimentación y accesorios 52

2.2.5 SOPORTE 52

2.3 SERVICIOS ADMINISTRADOS 53

2.3.1 COBERTURA DE LOS SERVICIOS 53

2.3.2 HORARIO DE ATENCIÓN 53

2.3.3 PERFILES DE LOS RECURSOS 53

2.3.3.2 SERVICIO BÁSICO SOPORTE EN SITIO OFIMATICA E IMPRESION 54

2.3.3.3 SERVICIO ESPECIALIZADO EN SEGURIDAD DE LA INFORMACION Y CONTINUIDAD DEL

NEGOCIO 55

2.4 SERVICIOS TRANSVERSALES A TODAS LAS SOLUCIONES 55

2.4.1 GERENTE DE PROYECTO DURANTE LA FASE DE IMPLEMENTACIÓN 56

2.4.2 GERENTE DE PROYECTO PARA LA FASE DE OPERACIÓN DEL SERVICIO 56

2.4.3 EL LÍDER TÉCNICO 57

3. CIBERSEGURIDAD 59

3.1 CONDICIONES TRANSVERSALES A LOS SERVICIOS DE CIBERSEGURIDAD (aplican a todas las soluciones) 59

3.1.1 Modalidad y continuidad del servicio 59

3.1.2 Licenciamiento 59

3.1.3 Documentación y reportes 60

3.2 GESTIÓN Y SOPORTE DE PLATAFORMAS DE SEGURIDAD FORTINET PROPIEDAD DEL INSTITUTO 60

3.2.1 Alcance del Servicio 60

3.2.2 Modalidad y operación 61

3.2.3 Requerimientos técnicos mínimos del servicio 61

3.2.4 Acceso, reportes y documentación 62

3.2.5 Reportes y Documentación 62

3.2.6 Experiencia y Perfil del Proveedor 63

3.3 SERVICIO ADMINISTRADO ANTIDDOS (MITIGACIÓN VOLUMÉTRICA EN INTERNET) 63

3.3.1 Alcance del servicio 63

3.3.2 Topología requerida 63

3.3.3 Técnicas mínimas de mitigación 64

3.3.4 Condiciones de habilitación 64

3.3.5 Capacidad, estabilización, notificaciones y reportes 64

3.4 SERVICIOS DE MONITOREO DE SEGURIDAD MEDIANTE PLATAFORMA SIEM (SECURITY

INFORMATION AND EVENT MANAGEMENT)..... 64

3.4.1 Funcionalidades mínimas obligatorias de la plataforma SIEM 67

3.4.2 Arquitectura mínima 68

3.4.3 Acceso y portal 68

3.4.4 Insumos a cargo del INMLCF 68

3.5 CENTRO DE OPERACIONES DE SEGURIDAD (SOC) COMO SERVICIO 68

3.5.1 Alcance 69

3.5.2 Gestión Operativa y Técnica 70

3.5.3 Actualizaciones y Parches 70

3.5.4 Buenas Prácticas de Seguridad 70

3.5.5 Reportes y Documentación 71

3.5.6 Mesa de Servicios y Canales de Atención 71

3.6 ZERO TRUST NETWORK ACCESS (ZTNA) 72

3.6.1 Modalidad y arquitectura 73

3.6.2 Licenciamiento y soporte 73

3.6.3 Capacidades mínimas 73

3.7 SERVICIO DE PROTECCIÓN DE CORREO ELECTRÓNICO (MSSP EN NUBE DEL FABRICANTE) 76

3.7.1 Usuarios y compatibilidad 76

3.7.2 Capacidades de Seguridad Obligatorias 77

3.7.3 Monitoreo, Trazabilidad y Reportes 77

3.7.4 Soporte y Operación 78

3.7.5 Obligaciones del Proveedor 78

3.8 SERVICIO DE PROTECCIÓN DE RIESGOS DIGITALES 78

3.8.1 Modalidad y alcance 79

3.8.2 Capacidades mínimas 79

3.9 CONSOLA DE GESTIÓN CENTRALIZADA DEDICADA Y DE USO EXCLUSIVO (SERVICIO DEDICADO, INSTANCIA EXCLUSIVA) 82

3.9.1 Objeto y arquitectura 82

3.9.2 Capacidad mínima y escalabilidad 83

3.9.3 Responsabilidades del Proveedor 83

3.9.4 Accesos, Administración y Seguridad 84

3.9.5 Autenticación y Control de Acceso 84

3.9.6 Gestión, Monitoreo y Alertamiento 85

3.9.7 Gestión Centralizada de Seguridad (NGFW / UTM) 86

3.9.8 Gestión Unificada de Red 86

3.9.9 Inteligencia Artificial y Automatización Avanzada 86

3.9.10 Soporte y acceso 87

3.10 CONSOLA DE ANALITICA Y TELEMETRÍA CENTRALIZADA DE USO DEDICADO Y EXCLUSIVO PARA LA ENTIDAD 88

3.10.1 Modalidad y alta disponibilidad 88

3.10.2 Capacidades mínimas 89

3.11 SERVICIO DE GESTIÓN DE IDENTIDAD Y ACCESO DEDICADO Y USO EXCLUSIVO PARA LA ENTIDAD 92

3.11.1 Modalidad del servicio 92

3.11.2 Arquitectura y alta disponibilidad 92

3.11.3 Capacidad y escalabilidad 93

3.11.4 Integraciones obligatorias 93

3.11.5 Autenticación y control de acceso 93

3.11.6 Gestión de usuarios y autoservicio 94

3.11.7 Autoridad certificadora 94

3.11.8 Administración, monitoreo y auditoría 95
3.11.9 Respaldo y continuidad 95
3.11.10 Compatibilidad de plataformas 95
3.11.11 Servicios de implementación y soporte 96
3.12 SERVICIO DE SECURE ACCESS SERVICE EDGE (SASE) 97
3.12.1 Alcance 98
3.12.2 Generalidades 98
3.12.3 Acceso Seguro a Internet (Secure Internet Access SIA) 99
3.12.4 Acceso Seguro a aplicaciones SaaS (Secure SaaS Access SSA) 99
3.12.5 Acceso Privado Seguro (Secure Private Access SPA) 99
3.12.6 Licencias incluidas 100
3.12.7 Seguridad para los equipos finales (Endpoint Security) 100
3.12.8 Integración NOC / SOC 101
3.12.9 Gestión 101
3.13 SERVICIO DE CONTROL DE ACCESO A LA RED 102
3.13.1 Alcance 102
3.13.2 Generalidades 102
3.13.3 Perfilado de Dispositivos 103
3.13.4 Authentication y Enforcement 104
3.13.5 Requisitos de Endpoint Compliance y Remediación 105
3.13.6 Gestión de Invitados 105
3.13.7 Gestión y Reporte 106
3.14 SERVICIOS DE PROTECCIÓN, RENDIMIENTO Y SEGURIDAD PARA APLICACIONES WEB. 107
3.14.1 Especificaciones Técnicas del Servicio 107
3.14.2 Generalidades 110

4. IPV6 111

4.1 Contexto y estado actual de la infraestructura 111

4.2 Compatibilidad obligatoria IPv4 / IPv6 (Dual Stack) 112

4.3 Gestión y preservación del direccionamiento IP 112

4.4 Integración de nuevos componentes, sistemas o servicios 113

4.5 Equivalencia de rendimiento, seguridad y gestión 113

4.6 Principio de continuidad del servicio 113

4.7 Carácter obligatorio y aceptación 114

4.8 Verificación y evidencias de cumplimiento 114

5. SERIVIOS WIFI MOVILES A NIVEL NACIONAL 114

5.1 El oferente deberá suministrar, habilitar y operar como mínimo: 115

5.2 El Contratista deberá suministrar y garantizar, como mínimo: 115

5.3 Requerimientos mínimos funcionales 116

5.3.1 Funcionalidad de punto de acceso WiFi (movilidad) 116

5.3.2 Capacidad mínima y continuidad por recargas 116

5.4 Requerimientos mínimos de monitoreo, autogestión y plataforma (Centro de Control) 116

5.4.1 Plataforma de monitoreo de consumo 116

5.4.2 Centro de Control para autogestión 116

5.5 Requerimientos mínimos de reportes 117

El Contratista deberá entregar reportes mensuales asociados al servicio, incluyendo (como mínimo) reporte de usabilidad. 117

Adicionalmente, se deberán incluir reportes como páginas visitadas, entre otros, en la medida de lo posible según capacidades del servicio y del operador. 117

5.6 Requerimientos mínimos de equipos y SIM 117

Los equipos y las SIM Cards que formen parte del servicio deben ser nuevos. 117

5.7 Requerimientos mínimos técnicos del equipo (router WiFi 4G/LTE o superior) – neutrales (sin marca) 117

5.7.1 Conectividad móvil (WWAN) 117

5.7.2 Conectividad WiFi (WLAN) 118

5.7.3 Interfaces mínimas 118

5.7.4 Requisito adicional cuando el dispositivo soporte voz (si aplica) 118

5.8 Compatibilidad mínima con la red del operador (cuando la Entidad aporte equipos o adquiera con terceros) 118

5.9 Requerimiento asociado a SD-WAN (cuando aplique como canal secundario) 119

5.10 Condición de cierre (equipos en modalidad de servicio) 119

6. REQUERIMIENTOS DEL PERIODO DE TRANSICIÓN 120

6.1 Condiciones Técnicas Obligatorias 121

6.2 Fecha Límite de Entrada en Operación 121

6.3 CONDICIÓN ECONÓMICA DEL PERÍODO DE TRANSICIÓN 122

6.4 Carácter Obligatorio y Esencial 122

7. ACUERDOS DE NIVELES DE SERVICIO (ANS/SLA) 123

7.1. Alcance y componentes cubiertos 123

7.2. Principios de medición y gobierno del SLA 123

7.3. Mesa de servicios, severidad y escalamiento 124

7.4. ANS/SLA específicos por componente 124

7.4.1 Conectividad (Internet, enlaces principales y de respaldo) 124

- Rehúso obligatorio 1:1: Para todos los canales principales de Internet y para los enlaces de respaldo (backup) se deberá aplicar rehúso 1:1 (sin sobresuscripción) y simetría, garantizando que el ancho de banda contratado corresponda al ancho de banda efectivamente disponible para la Entidad, tanto en sentido de subida como de bajada. 124

7.4.2 SD-WAN / Orquestación / Gestión centralizada 126

7.4.3 Red LAN (Core, Acceso, NAC/SD-Branch) y WLAN..... 126

7.4.4 Ciberseguridad (SOC/RSOC, SIEM, AntiDDoS, ZTNA, Correo, WAF/SASE y demás servicios)..... 126

7.4.5 Continuidad IPv6 (Dual Stack)..... 126

7.4.6 Servicios WiFi móviles..... 127

7.4. Período de transición..... 127

- Penalidades, créditos de servicio y mejora continua..... 127

RESUMEN

La contratación de la Solución Integral de Telecomunicaciones se justifica técnica, operativa y estratégicamente en la necesidad de:

- Unificar la gestión de redes, conectividad y seguridad bajo un modelo centralizado y administrado.
- Reducir riesgos operativos y de seguridad, garantizando alta disponibilidad y resiliencia ante fallas.
- Asegurar la interoperabilidad con la infraestructura existente, especialmente con plataformas de seguridad y red actualmente desplegadas.
- Soportar la migración y operación híbrida hacia la nube de Azure, garantizando conectividad segura, confiable y altamente disponible.
- Cumplir con los lineamientos de continuidad del servicio, seguridad de la información y modernización tecnológica exigidos a una entidad del orden nacional.

Capítulo 1. Conectividad

Define los requerimientos para la conectividad nacional del INMLCF, incluyendo:

- Enlaces principales y de respaldo (fibra, LTE y satelital LEO).
- Clasificación de sedes (Tipo 1, 2 y 3).
- Alta disponibilidad, balanceo y failover automático mediante SD-WAN.
- Conectividad segura hacia la nube de Microsoft Azure.
- Planes de contingencia para sedes con factibilidad terrestre negativa.

Justificación: Garantizar conectividad continua, homogénea y resiliente en todo el territorio nacional, incluyendo sedes remotas.

Capítulo 2. Red LAN y Servicios Administrados

Establece la contratación en modalidad de servicio de:

- Red LAN Core y Acceso.
- Integración SD-LAN, SD-WAN y NAC.
- Red inalámbrica WLAN con portal cautivo personalizado.
- Servicios administrados (DBA, soporte ofimático, seguridad de la información).

Justificación: Modernizar la red interna, centralizar la gestión, fortalecer la seguridad de acceso y optimizar la operación de TI.

Capítulo 3. Ciberseguridad

Incluye la implementación y operación de servicios como:

- Gestión y soporte de plataformas de seguridad existentes.
- Anti-DDoS.
- SIEM como servicio.
- SOC como servicio.
- ZTNA.
- Protección de correo electrónico.
- Protección de riesgos digitales.
- SASE.
- NAC.
- Protección de aplicaciones web (WAF, CDN, AntiDDoS capa 7).

Justificación: Fortalecer integralmente la postura de ciberseguridad del Instituto, garantizar detección temprana, respuesta oportuna y mitigación de amenazas.

Capítulo 4. IPv6

Consolida los requerimientos para:

- La continuidad del esquema Dual Stack IPv4/IPv6.
- Preservación del direccionamiento IP del Instituto.
- Integración obligatoria de nuevos servicios sin afectación operativa.

Justificación: Garantizar sostenibilidad tecnológica, cumplimiento de lineamientos nacionales y continuidad de los servicios ya desplegados en IPv6.

Capítulo 5. Servicios WiFi Móviles

Define la provisión de:

- 50 servicios WiFi móviles 4G LTE o superior.
- Planes de datos, monitoreo, autogestión y contingencia SD-WAN.

Justificación: Asegurar continuidad operativa en escenarios de contingencia o indisponibilidad del servicio principal.

Capítulo 6. Período de Transición

Establece:

- Condiciones técnicas, operativas y obligatorias durante la transición.
- Prohibición absoluta de indisponibilidad del servicio.
- Ejecución del período de transición sin costo para el INMLCF.

Justificación: Garantizar una migración controlada, sin impacto en la operación institucional y alineada con la migración a Azure.

Capítulo 7. Acuerdos de Niveles de Servicio (ANS/SLA)

Define:

- SLA por componente (conectividad, SD-WAN, LAN, ciberseguridad, IPv6, WiFi móviles).
- Mesa de servicios 7x24x365.
- Penalidades, créditos de servicio y mejora continua.

Justificación: Asegurar estándares medibles de calidad, trazabilidad contractual y control del desempeño del proveedor.

El Instituto Nacional de Medicina Legal y Ciencias Forenses requiere contratar la implementación de una Solución Integral de Telecomunicaciones como un servicio estratégico, esencial y transversal, indispensable para garantizar la continuidad de su misión institucional, la seguridad de la información, la modernización tecnológica y la operación confiable de sus servicios a nivel nacional.

La contratación de esta solución no constituye una simple adquisición de conectividad o equipos, sino la adopción de un modelo integral, administrado, resiliente y alineado con las mejores prácticas de gobierno digital, ciberseguridad y continuidad del negocio.

1. CONECTIVIDAD

El Instituto Nacional de Medicina Legal y Ciencias Forenses (INMLCF), a través del Grupo Nacional de Tecnologías de la Información y Desarrollo, requiere la implementación de una Solución Integral de Telecomunicaciones a nivel nacional. Esta solución debe asegurar la conectividad corporativa, la continuidad operativa, así como la disponibilidad y estabilidad de los servicios tecnológicos y misionales en todas las sedes, nodos y puntos de atención de la Entidad. El alcance incluye los bienes y servicios necesarios para la operación y mejora continua de la conectividad- SDWAN, LAN como lo son switch CORE, switch de acceso, WI-FI, servicios de ciberseguridad, continuidad ipv6, licenciamiento de equipos de propiedad de la entidad, servicios móviles y la mesa de ayuda, abarcando todos los lugares donde el INMLCF cumple sus funciones, conforme a las especificaciones técnicas detalladas en la Ficha técnica de Bienes, Productos o Servicios adjunta a este documento y según lo estipulado en el Reglamento de Funcionamiento y Operación de la Bolsa para el Mercado de Compras Públicas.

Ubicación: el contrato se desarrollará en todos los puntos de atención (sedes), nodos de la entidad descritos en la tabla de Conectividad (requerimiento de sedes a conectar), con las modificaciones y adiciones que se deriven de su ejecución. Por un periodo de 5 meses sin exceder el 31 de diciembre 2026.

ANEXO 1. CONECTIVIDAD							
1.1 PUNTOS A CONECTAR							
ITEM	REGIONAL	CIUDAD	DIRECCIÓN	PRODUCTO	MEDIO	BW (MBPS) - CANAL NUEVO	EQUIPO SDWAN
1	SEDE CENTRAL	Bogotá D.C.	Calle 7A No. 12 A – 51	Canal de Datos Principal	FIBRA	1.000	TIPO 1
2		Bogotá D.C.	Calle 7A No. 12 A – 51	Canal de Datos Secundario	FIBRA	1.000	
3		Bogotá D.C.	Calle 7A No. 12 A – 51	Canal de Internet Principal	FIBRA	2.000	TIPO 1
4		Bogotá D.C.	Calle 7A No. 12 A – 51	Canal de Internet Secundario	FIBRA	2.000	
5		Bogotá D.C.	CALLE 17 No. 34-39 BARRIO CUNDINAMARCA	Canal de Datos Principal	FIBRA	20	TIPO 2
6		Bogotá D.C.	CALLE 17 No. 34-39 BARRIO CUNDINAMARCA	Canal de Datos Secundario	FIBRA	10	
7		Bogotá D.C.	Cra 35 # 4B-43 (Veraguas)	Canal de Datos Principal	FIBRA	6	TIPO3
8		Bogotá D.C.	Cra 35 # 4B-43 (Veraguas)	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
9		Bogotá D.C.	Cra. 7 No. 32 42 Piso 12 y 14 torre Sur Edificio San Martín.	Canal de Datos Principal	FIBRA	345	TIPO 1
10		Bogotá D.C.	Cra. 7 No. 32 42 Piso 12 y 14 torre Sur Edificio San Martín.	Canal de Datos Secundario	FIBRA	300	
11	REGIONAL BOGOTA	Bogotá D.C.	Carrera 40 No. 10 A - 08 (UPJ)	Canal de Datos Principal	FIBRA	20	TIPO 2
12		Bogotá D.C.	Carrera 40 No. 10 A - 08 (UPJ)	Canal de Datos Secundario	FIBRA	20	
13		Bogotá D.C.	CARRERA 78 A N° 77 A -62	Canal de Datos Principal	FIBRA	6	TIPO 3
14		Bogotá D.C.	CARRERA 78 A N° 77 A -63	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
15		Bogotá D.C.	Diagonal 62 Sur No. 20 F - 20. piso 2.	Canal de Datos Principal	FIBRA	6	TIPO 3
16		Bogotá D.C.	Diagonal 62 Sur No. 20 F - 20. piso 2.	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
17		Bogotá D.C.	Calle 85 sur no. 94 - 35 Bosa.	Canal de Datos Principal	FIBRA	6	TIPO 2
18		Bogotá D.C.	Calle 85 sur no. 94 - 35 Bosa.	Canal de Datos Secundario	FIBRA	6	
19		Bogotá D.C.	Carrera 69 No. 36-70 sur.	Canal de Datos Principal	FIBRA	6	TIPO 3
20		Bogotá D.C.	Carrera 69 No. 36-70 sur.	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
21		Bogotá D.C.	Calle 12 No 30-35 Piso 3	Canal de Datos Principal	FIBRA	20	TIPO 2
22		Bogotá D.C.	Calle 12 No 30-35 Piso 3	Canal de Datos Secundario	FIBRA	20	
23		Bogotá D.C.	avenida 19 # 27-09, piso 2 "CAPIV"	Canal de Datos Principal	FIBRA	4	TIPO 3
24		Bogotá D.C.	avenida 19 # 27-09, piso 2 "CAPIV"	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	

25		Soacha	KR 6 No. 15-96 BARRIO SAN LUIS	Canal de Datos Principal	FIBRA	6	TIPO 2
26		Soacha	KR 6 No. 15-96 BARRIO SAN LUIS	Canal de Datos Secundario	FIBRA	4	
27		Fusagasugá	Hospital San Rafael Transv. 12 # 22-51	Canal de Datos Principal	FIBRA	6	TIPO 3
28		Fusagasugá	Hospital San Rafael Transv. 12 # 22-52	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
29		Zipaquirá	Hospital Universitario de la Samaritana Unidad Funcional Zipaquirá CL.10 #6-70	Canal de Datos Principal	FIBRA	6	TIPO 3
30		Zipaquirá	Hospital Universitario de la Samaritana Unidad Funcional Zipaquirá CL.10 #6-71	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
31		Facatativá	Hospital San Rafael Cra. 2a. # 1-80	Canal de Datos Principal	FIBRA	6	TIPO 3
32		Facatativá	Hospital San Rafael Cra. 2a. # 1-81	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
33		La Mesa	Hospital Pedro León Alvarez	Canal de Datos Principal	FIBRA	6	TIPO 3
34		La Mesa	Hospital Pedro León Alvarez	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
35		Villeta	Hospital Fernando Salazar Calle 1a. # 7-56	Canal de Datos Principal	FIBRA	6	TIPO 3
36		Villeta	Hospital Fernando Salazar Calle 1a. # 7-57	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
37		Leticia	Hospital Regional Leticia	Canal de Datos Principal	SATELITAL LEO	6	
38		Leticia	Hospital Regional Leticia	Canal de Datos Secundario	SATELITAL VSAT GEO	6	
39		Cáqueza	Hospital San Rafael Av.5a. # 5-80	Canal de Datos Principal	FIBRA	6	TIPO 3
40		Cáqueza	Hospital San Rafael Av.5a. # 5-81	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
41		Ubaté	Hospital El Salvador Cra. 4 No. 5-44	Canal de Datos Principal	FIBRA	6	TIPO 3
42		Ubaté	Hospital El Salvador Cra. 4 No. 5-45	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
43		Soata	CARRERA 4 #11- 64	Canal de Datos Principal	FIBRA	6	TIPO 3
44		Soata	CARRERA 4 #11- 65	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
45		Chocontá	E.S.E Hospital San Martín de Porres Cra. 4 #8-12	Canal de Datos Principal	FIBRA	6	TIPO 3
46		Chocontá	E.S.E Hospital San Martín de Porres Cra. 4 #8-13	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
47		Villavicencio	Carrera 6 No. 24A - 14 BARRIO MENEGUA	Canal de Datos Principal	FIBRA	40	TIPO 1
48	REGIONAL	Villavicencio	Carrera 6 No. 24A - 14 BARRIO MENEGUA	Canal de Datos Secundario	FIBRA	15	
49	ORIENTE	Granada	Cra 11 # 15-39 BR Camilo Torres	Canal de Datos Principal	FIBRA	6	TIPO 3
50		Granada	Cra 11 # 15-39 BR Camilo Torres	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
51		San José del Guaviare	Carrera 23 Calle 21 Casa de Justicia	Canal de Datos Principal	FIBRA	6	TIPO 3
52		San José del Guaviare	Carrera 23 Calle 21 Casa de Justicia	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
53		Acacías	Carrera 10 con Calle 14 - Barrio Juan Mellao	Canal de Datos Principal	FIBRA	6	TIPO 2
54		Acacías	Carrera 10 con Calle 14 - Barrio Juan Mellao	Canal de Datos Secundario	FIBRA	4	
55		Puerto López	Hospital Local Calle 8.N 6 - 50 Barrio Gaitán	Canal de Datos Principal	FIBRA	6	TIPO 3
56		Puerto López	Hospital Local Calle 8.N 6 - 50 Barrio Gaitán	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
57		Yopal	Marginal de la Selva Diagonal 9 No 13C-68 Barrio La Corocora	Canal de Datos Principal	FIBRA	20	TIPO 2
58		Yopal	Marginal de la Selva Diagonal 9 No 13C-68 Barrio La Corocora	Canal de Datos Secundario	FIBRA	12	
59		Mitú	Carrera 14 # 15-55 Barrio Centro	Canal de Datos Principal	SATELITAL LEO	6	
60		Mitú	Carrera 14 # 15-55 Barrio Centro	Canal de Datos Secundario	SATELITAL VSAT GEO	6	
61		Puerto Inírida	Hospital Local Miguel Elkin Patarroyo Carrera 9 No. 16-14	Canal de Datos Principal	SATELITAL LEO	6	
62		Puerto Inírida	Hospital Local Miguel Elkin Patarroyo Carrera 9 No. 16-15	Canal de Datos Secundario	SATELITAL VSAT GEO	6	
63		Tunja	CALLE 24 No 5 A -61	Canal de Datos Principal	FIBRA	30	TIPO 2
64		Tunja	CALLE 24 No 5 A -62	Canal de Datos Secundario	FIBRA	15	
65		Sogamoso	Hospital San José Cl. 8 # 11-43	Canal de Datos Principal	FIBRA	6	TIPO 3
66		Sogamoso	Hospital San José Cl. 8 # 11-44	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
67		Duitama	Hospital Regional Av. Las américas Cra. 35 Piso 1.	Canal de Datos Principal	FIBRA	6	TIPO 3
68		Duitama	Hospital Regional Av. Las américas Cra. 35 Piso 1.	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
69		Chiquinquira	Hospital San Salvador Cra. 13 # 18-60	Canal de Datos Principal	FIBRA	4	TIPO 3
70		Chiquinquira	Hospital San Salvador Cra. 13 # 18-61	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
71		Garagoa	Transversal 8 N° 6-06 Contiguo al Hospital Regional Valle de Tenza	Canal de Datos Principal	FIBRA	6	TIPO 3
72		Garagoa	Transversal 8 N° 6-06 Contiguo al Hospital Regional Valle de Tenza	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
73		Puerto Carreño	Hospital Calle 18 #10 43 Barrio la Primavera	Canal de Datos Principal	SATELITAL LEO	6	
74		Puerto Carreño	Hospital Calle 18 #10 43 Barrio la Primavera	Canal de Datos Secundario	SATELITAL VSAT GEO	6	

75	REGIONAL NOROCCIDENTE	Medellín	Cra 65 Nro. 80-325	Canal de Datos Principal	FIBRA	80	TIPO 1
76		Medellín	Cra 65 Nro. 80-326	Canal de Datos Secundario	FIBRA	40	
77		Medellín	Cra 65 Nro. 80-325	Canal de Datos Principal	FIBRA	2	TIPO 3
78		Medellín	Cra 65 Nro. 80-326	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
79		Rionegro	Cra. 48 #56-59	Canal de Datos Principal	FIBRA	8	TIPO 3
80		Rionegro	Cra. 48 #56-60	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
81		Bello	Diagonal 65 N° 42 A - 11 - Sede Casa de Justicia de Bello	Canal de Datos Principal	FIBRA	6	TIPO 3
82		Bello	Diagonal 65 N° 42 A - 11 - Sede Casa de Justicia de Bello	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
83		Andes	Hospital San Rafael Av. Medellín Nro. 48-20	Canal de Datos Principal	FIBRA	6	TIPO 3
84		Andes	Hospital San Rafael Av. Medellín Nro. 48-21	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
85		Apartado	Hospital Antonio Roldan Betancourt Cra. 98 no. 106-176	Canal de Datos Principal	FIBRA	6	TIPO 3
86		Apartado	Hospital Antonio Roldan Betancourt Cra. 98 no. 106-177	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
87		Chigorodó	Cra. 108A No. 101A-57	Canal de Datos Principal	FIBRA	6	TIPO 3
88		Chigorodó	Cra. 108A No. 101A-58	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
89		Envigado	Diagonal 33 No. 35C Sur-31 Barrio los Naranjos Sede Clínica Santa Gertrudis	Canal de Datos Principal	FIBRA	6	TIPO 3
90		Envigado	Diagonal 33 No. 35C Sur-31 Barrio los Naranjos Sede Clínica Santa Gertrudis	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
91		Segovia	Barrio el Ventiadero Centro de Salud La Cruzada	Canal de Datos Principal	FIBRA	6	TIPO 2
92		Segovia	Barrio el Ventiadero Centro de Salud La Cruzada	Canal de Datos Secundario	FIBRA	4	
93		Caucasia	Kilómetro 2 vía el Bagre- Manzana 11 Centro Logístico- Barrio Pensilvania	Canal de Datos Principal	FIBRA	6	TIPO 3
94		Caucasia	Kilómetro 2 vía el Bagre- Manzana 11 Centro Logístico- Barrio Pensilvania	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
95		Turbo	Hospital Francisco Valderrama Kilometro 1 Salida Apartado	Canal de Datos Principal	FIBRA	6	TIPO 3
96		Turbo	Hospital Francisco Valderrama Kilometro 1 Salida Apartado	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
97		Yarumal	Avenida los Libertadores, Hospital San Juan De Dios	Canal de Datos Principal	FIBRA	6	TIPO 3
98		Yarumal	Avenida los Libertadores, Hospital San Juan De Dios	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
99		La Ceja	Cra. 17 No. 20-53 Casa de Justicia y Paz	Canal de Datos Principal	FIBRA	6	TIPO 3
100		La Ceja	Cra. 17 No. 20-53 Casa de Justicia y Paz	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
101		Taraza	Calle 25 No. 29-25 barrio, La Bomba	Canal de Datos Principal	FIBRA	6	TIPO 3
102		Taraza	Calle 25 No. 29-25 barrio, La Bomba	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
103		Quibdó	Calle 25 No. 6 - 08	Canal de Datos Principal	FIBRA	20	TIPO 2
104		Quibdó	Calle 25 No. 6 - 09	Canal de Datos Secundario	FIBRA	10	
105		Istmina	Casa de Justicia de Istmina	Canal de Datos Principal	FIBRA	6	TIPO 2
106		Istmina	Casa de Justicia de Istmina	Canal de Datos Secundario	FIBRA	4	
107		Montería	Carrera 7 con Calle 10 Esquina B/ Buena vista	Canal de Datos Principal	FIBRA	20	TIPO 2
108		Montería	Carrera 7 con Calle 10 Esquina B/ Buena vista	Canal de Datos Secundario	FIBRA	10	
109		Lorica	Cra 28 N°17-127 B/ San Pedro	Canal de Datos Principal	FIBRA	6	TIPO 2
110		Lorica	Cra 28 N°17-127 B/ San Pedro	Canal de Datos Secundario	FIBRA	4	
111		Puerto Boyacá	Carrera 5 Nro. 26 02 Hospital José Cayetano Vásquez	Canal de Datos Principal	FIBRA	6	TIPO 2
112		Puerto Boyacá	Carrera 5 Nro. 26 02 Hospital José Cayetano Vásquez	Canal de Datos Secundario	FIBRA	4	

113	REGIONAL NORORIENTE	Bucaramanga	CALLE 45 # 1-51 Campohermoso	Canal de Datos Principal	FIBRA	60	TIPO 1
114		Bucaramanga	CALLE 45 # 1-51 Campohermoso	Canal de Datos Secundario	FIBRA	30	
115		Barrancabermeja	Avenida 52 N 8A Diagonal Cristo Petrolero	Canal de Datos Principal	FIBRA	6	TIPO 2
116		Barrancabermeja	Avenida 52 N 8A Diagonal Cristo Petrolero	Canal de Datos Secundario	FIBRA	6	
117		Vélez	Calle 8 No.2-30	Canal de Datos Principal	FIBRA	6	TIPO 3
118		Vélez	Calle 8 No.2-31	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
119		Cimitarra	Casa fiscal No.3 Frente Colegio Sica.	Canal de Datos Principal	FIBRA	6	TIPO 3
120		Cimitarra	Casa fiscal No.3 Frente Colegio Sica.	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
121		San Gil	Carrera 11 No. 4-14 Sector la Playa	Canal de Datos Principal	FIBRA	6	TIPO 3
122		San Gil	Carrera 11 No. 4-14 Sector la Playa	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
123		Codazzi	Hospital Agustín Codazzi Calle 14 No. 8 - 67	Canal de Datos Principal	FIBRA	6	TIPO 3
124		Codazzi	Hospital Agustín Codazzi Calle 14 No. 8 - 68	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
125		Valledupar	Hospital Rosario Pumarejo de Lopez Calle 16 con Cra 17 - Morgue	Canal de Datos Principal	FIBRA	8	TIPO 3
126		Valledupar	Hospital Rosario Pumarejo de Lopez Calle 16 con Cra 17 - Morgue	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
127		Valledupar	Calle 13C No. 15-79 Barrio Alfonso Lopez	Canal de Datos Principal	FIBRA	12	TIPO 2
128		Valledupar	Calle 13C No. 15-79 Barrio Alfonso Lopez	Canal de Datos Secundario	FIBRA	8	
129		Bosconia	Carrera 18 # 11-07 Comisaria de Familia e Inspección de Policía	Canal de Datos Principal	FIBRA	6	TIPO 3
130		Bosconia	Carrera 18 # 11-07 Comisaria de Familia e Inspección de Policía	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
131		Aguachica	Calle 4 No. 19 - 47 Aguachica	Canal de Datos Principal	FIBRA	6	TIPO 3
132		Aguachica	Calle 4 No. 19 - 47 Aguachica	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
133		Chiriguaná	Calle 7 N 5 -26 Alcaldía Municipal Calle Bolivar	Canal de Datos Principal	FIBRA	6	TIPO 3
134		Chiriguaná	Calle 7 N 5 -26 Alcaldía Municipal Calle Bolivar	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
135		Cúcuta	Calle 16N # 6-97 Sector Corral de Piedra (SIJIN-PONAL),	Canal de Datos Principal	FIBRA	20	TIPO 2
136		Cúcuta	Calle 16N # 6-97 Sector Corral de Piedra (SIJIN-PONAL),	Canal de Datos Secundario	FIBRA	10	
137		Ocaña	Calle 11 # 34-35, Fiscalía General, Barrio Buenos Aires.	Canal de Datos Principal	FIBRA	6	TIPO 3
138		Ocaña	Calle 11 # 34-35, Fiscalía General, Barrio Buenos Aires.	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
139		Málaga	calle 13 No. 4P Carrera5	Canal de Datos Principal	FIBRA	6	TIPO 3
140		Málaga	calle 13 No. 4P Carrera6	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
141		Pamplona	Carrera 9 Calle 5a Hospital San Juan de Dios	Canal de Datos Principal	FIBRA	6	TIPO 3
142		Pamplona	Carrera 9 Calle 5a Hospital San Juan de Dios	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
143		Arauca	Carrera. 20 N°5-50 Barrio Fundadores	Canal de Datos Principal	FIBRA	16	TIPO 2
144		Arauca	Carrera. 20 N°5-50 Barrio Fundadores	Canal de Datos Secundario	FIBRA	4	
145		Saravena	Carrera 19A N° 28 - 53 Barrio Modelo	Canal de Datos Principal	FIBRA	6	TIPO 3
146		Saravena	Carrera 19A N° 28 - 53 Barrio Modelo	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
147		Tame	CL 14A 35 10 LOTE 9 MZ F URB LOS MANGOS	Canal de Datos Principal	FIBRA	6	TIPO 3
148		Tame	CL 14A 35 10 LOTE 9 MZ F URB LOS MANGOS	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
149		Puerto Berrio	Hospital La Cruz Cra. 7 No. 48-03	Canal de Datos Principal	FIBRA	6	TIPO 3
150		Puerto Berrio	Hospital La Cruz Cra. 7 No. 48-04	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
151		Santa Rosa del Sur	Calle 6 # 11-22 Sede Transito y Transporte Barrio el Carmen	Canal de Datos Principal	FIBRA	6	TIPO 3
152		Santa Rosa del Sur	Calle 6 # 11-22 Sede Transito y Transporte Barrio el Carmen	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	

153	REGIONAL NORTE	Barranquilla	Carrera 23 No. 53D - 56 Barrio Andes	Canal de Datos Principal	FIBRA	60	TIPO 1
154		Barranquilla	Carrera 23 No. 53D - 56 Barrio Andes	Canal de Datos Secundario	FIBRA	30	
155		Barranquilla	Cementerio Villa eleyla Carrera 19 N32b-250	Canal de Datos Principal	FIBRA	6	TIPO 3
156		Barranquilla	Cementerio Villa eleyla Carrera 19 N32b-251	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
157		Cartagena	Barrio Zaragocilla, al lado del Hospital Universitario de Cartagena (Calle 29 No. 50-210)	Canal de Datos Principal	FIBRA	20	TIPO 2
158		Cartagena	Barrio Zaragocilla, al lado del Hospital Universitario de Cartagena (Calle 29 No. 50-210)	Canal de Datos Secundario	FIBRA	10	
159		Carmen de Bolívar	Calle 23 No. 56-32 Hospital Nuestra Señora del Carmen	Canal de Datos Principal	FIBRA	6	TIPO 3
160		Carmen de Bolívar	Calle 23 No. 56-32 Hospital Nuestra Señora del Carmen	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
161		San Andrés Isla	Manzana 5 Casa 10 Entrada 2 vía San Luis	Canal de Datos Principal	FIBRA	6	TIPO 3
162		San Andrés Isla	Manzana 5 Casa 10 Entrada 2 vía San Luis	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
163		Magangué	Hospital Divina Misericordia Calle 16 C # 13-146 Barrio San Jose	Canal de Datos Principal	FIBRA	6	TIPO 3
164		Magangué	Hospital Divina Misericordia Calle 16 C # 13-146 Barrio San Jose	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
165		Riohacha	Calle 7No.15-45 Diagonal al Palacio de Justicia	Canal de Datos Principal	FIBRA	16	TIPO 3
166		Riohacha	Calle 7No.15-45 Diagonal al Palacio de Justicia	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
167		Maicao	Calle 9 No.11-23 Barrio el boscan.	Canal de Datos Principal	FIBRA	6	TIPO 3
168		Maicao	Calle 9 No.11-23 Barrio el boscan.	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
169		Santa Marta	Calle 26A No. 9-85	Canal de Datos Principal	FIBRA	16	TIPO 2
170		Santa Marta	Calle 26A No. 9-86	Canal de Datos Secundario	FIBRA	8	
171		Plato	Calle 4 # 13-44 Barrio el Centro Plato Magdalena	Canal de Datos Principal	FIBRA	6	TIPO 2
172		Plato	Calle 4 # 13-44 Barrio el Centro Plato Magdalena	Canal de Datos Secundario	FIBRA	4	
173		Ciénaga	Calle 12 No. 18-03	Canal de Datos Principal	FIBRA	6	TIPO 3
174		Ciénaga	Calle 12 No. 18-04	Canal de Datos Secundario	FIBRA	Bolsa de 2TB de conectividad gestionada	
175		Banco	Hospital La Candelaria. Cll 7 Carretera a Chiriguana	Canal de Datos Principal	FIBRA	6	TIPO 3
176		Banco	Hospital La Candelaria. Cll 7 Carretera a Chiriguana	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
177		Fundación	Calle 9 # 73-36 Barrio Centro	Canal de Datos Principal	FIBRA	6	TIPO 3
178		Fundación	Calle 9 # 73-36 Barrio Centro	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
179		Fonseca	Calle 15 No.21-3, Barrio Alto Prado	Canal de Datos Principal	FIBRA	6	TIPO 3
180		Fonseca	Calle 15 No.21-3, Barrio Alto Prado	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
181		Sincelejo	Calle 38 No.25A-211 Troncal de Occidente	Canal de Datos Principal	FIBRA	16	TIPO 3
182		Sincelejo	Calle 38 No.25A-211 Troncal de Occidente	Canal de Datos Secundario	FIBRA	Bolsa de 2TB de conectividad gestionada	
183		San Marcos	CALLE 15 #34-59 ESE CENTRO DE SALUD SAN JOSE, BARRIO SAN JOSE.	Canal de Datos Principal	FIBRA	6	TIPO 3
184		San Marcos	CALLE 15 #34-59 ESE CENTRO DE SALUD SAN JOSE, BARRIO SAN JOSE.	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	

185	REGIONAL OCCIDENTE	Pereira	Avenida Las Américas No. 98-25	Canal de Datos Principal	FIBRA	60	TIPO 1
186		Pereira	Avenida Las Américas No. 98-26	Canal de Datos Secundario	FIBRA	30	
187		Dos Quebradas	Diagonal 24 # 21T28,Dosquebradas, Risaralda.	Canal de Datos Principal	FIBRA	6	TIPO 3
188		Dos Quebradas	Diagonal 24 # 21T28,Dosquebradas, Risaralda.	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
189		Pereira	Cra. 8 No. 42-38 Oficina 212 Edificio B de la Fiscalía	Canal de Datos Principal	FIBRA	8	TIPO 3
190		Pereira	Cra. 8 No. 42-38 Oficina 212 Edificio B de la Fiscalía	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
191		Pereira	Av. las Américas sector Belmonte galpón 5 bodega 4	Canal de Datos Principal	FIBRA	8	TIPO 3
192		Pereira	Av. las Américas sector Belmonte galpón 5 bodega 5	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
193		Santa Rosa de Cabal	CARRERA 13 Nº 29-91	Canal de Datos Principal	FIBRA	6	TIPO 2
194		Santa Rosa de Cabal	CARRERA 13 Nº 29-92	Canal de Datos Secundario	FIBRA	6	
195		Belén de Umbría	Cra 13 # 4-135 Hospital San José	Canal de Datos Principal	FIBRA	6	TIPO 3
196		Belén de Umbría	Cra 13 # 4-135 Hospital San José	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
197		Supía	Carrera 7 Nº 24-42 Barrio Libertadores. Casa de la Justicia	Canal de Datos Principal	FIBRA	6	TIPO 3
198		Supía	Carrera 7 Nº 24-42 Barrio Libertadores. Casa de la Justicia	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
199		Cartago	Calle 11 No. 12 A – 12	Canal de Datos Principal	FIBRA	8	TIPO 3
200		Cartago	Calle 11 No. 12 A – 13	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
201		Apia	Hospital San Vicente de Paul Cra 7 # 7 - 13	Canal de Datos Principal	FIBRA	6	TIPO 3
202		Apia	Hospital San Vicente de Paul Cra 7 # 7 - 14	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
203		Manizales	CARRERA 27 No. 48-85	Canal de Datos Principal	FIBRA	20	TIPO 2
204		Manizales	CARRERA 27 No. 48-86	Canal de Datos Secundario	FIBRA	8	
205		Salamina	CALLE 3 # 9A-21 Hospital Felipe Suarez	Canal de Datos Principal	FIBRA	6	TIPO 3
206		Salamina	CALLE 3 # 9A-21 Hospital Felipe Suarez	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
207		Marsella	Clínica: Calle 9 No 9-14 Piso 1 Alcaldía Municipal. Patología Calle 14 No. 16 - 20 Hospital San Jose	Canal de Datos Principal	FIBRA	6	TIPO 2
208		Marsella	Clínica: Calle 9 No 9-14 Piso 1 Alcaldía Municipal. Patología Calle 14 No. 16 - 20 Hospital San Jose	Canal de Datos Secundario	FIBRA	4	
209		Chinchiná	Hospital San Marcos	Canal de Datos Principal	FIBRA	6	TIPO 3
210		Chinchiná	Hospital San Marcos	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
211		Anserma	HOSPITAL SAN VICENTE DE PAUL, Carrera 5A - Calle 1A	Canal de Datos Principal	FIBRA	6	TIPO 3
212		Anserma	HOSPITAL SAN VICENTE DE PAUL, Carrera 5A - Calle 1A	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
213		La Dorada	Cra. 6 10 B . 04	Canal de Datos Principal	FIBRA	6	TIPO 2
214		La Dorada	Cra. 6 10 B . 05	Canal de Datos Secundario	FIBRA	4	
215		Aguadas	Hospital San Jose Cra 3 entre calles 16 y 17	Canal de Datos Principal	FIBRA	6	TIPO 2
216		Aguadas	Hospital San Jose Cra 3 entre calles 16 y 18	Canal de Datos Secundario	FIBRA	4	
217		Armenia	Carrera 40A Calle 44 Esquina Barrio Villa Liliana.	Canal de Datos Principal	FIBRA	18	TIPO 2
218		Armenia	Carrera 40A Calle 44 Esquina Barrio Villa Liliana.	Canal de Datos Secundario	FIBRA	6	
219		Calarca	Cl 43 26-13	Canal de Datos Principal	FIBRA	4	TIPO 3
220		Calarca	Cl 43 26-14	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	

221		Cali	Calle 4B No. 36-01	Canal de Datos Principal	FIBRA	80	TIPO 1
222		Cali	Calle 4B No. 36-02	Canal de Datos Secundario	FIBRA	40	
223		Cali	Calle 73 No. 7G-28 Barrio Alfonso López	Canal de Datos Principal	FIBRA	6	TIPO 2
224		Cali	Calle 73 No. 7G-28 Barrio Alfonso López	Canal de Datos Secundario	FIBRA	4	
225		Cali	Calle 73ª No. Diagonal 26P esq Casa Justicia	Canal de Datos Principal	FIBRA	6	TIPO 3
226		Cali	Calle 73ª No. Diagonal 26P esq Casa Justicia	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
227		Siloé	Carrera 52 No. 3-02 El Lido - Estación de policía	Canal de Datos Principal	FIBRA	6	TIPO 3
228		Siloé	Carrera 52 No. 3-02 El Lido - Estación de policía	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
229		Cali	Calle 10 No. 6-26 Edificio Antiguo Telecom	Canal de Datos Principal	FIBRA	6	TIPO 2
230		Cali	Calle 10 No. 6-26 Edificio Antiguo Telecom	Canal de Datos Secundario	FIBRA	4	
231		Cali	Calle 6 No. 59-15 Barrio Joaquín Borrero Sinisterra	Canal de Datos Principal	FIBRA	6	TIPO 3
232		Cali	Calle 6 No. 59-15 Barrio Joaquín Borrero Sinisterra	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
233		Cali	Calle 73 Diagonal 26M-90	Canal de Datos Principal	FIBRA	7	TIPO 3
234		Cali	Calle 73 Diagonal 26M-90	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
235		Sevilla	Calle 51 No. 50-10 - Piso 4 - Edificio Alcaldía	Canal de Datos Principal	FIBRA	6	TIPO 3
236		Sevilla	Calle 51 No. 50-10 - Piso 4 - Edificio Alcaldía	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
237		Sevilla	Carrera 52 No. 61-183	Canal de Datos Principal	FIBRA	6	TIPO 3
238		Sevilla	Carrera 52 No. 61-184	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
239		Roldanillo	Avenida Santander No. 10-50 Hospital San Antonio	Canal de Datos Principal	FIBRA	6	TIPO 3
240		Roldanillo	Avenida Santander No. 10-50 Hospital San Antonio	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
241		Tuluá	Carrera 25C No.48-101 Nuevo Príncipe	Canal de Datos Principal	FIBRA	6	TIPO 3
242		Tuluá	Carrera 25C No.48-101 Nuevo Príncipe	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
243		Buga	Calle 5 No. 11-76 Piso 2	Canal de Datos Principal	FIBRA	6	TIPO 2
244		Buga	Calle 5 No. 11-76 Piso 3	Canal de Datos Secundario	FIBRA	4	
245		Buga	Carrera 18 Calle 9	Canal de Datos Principal	FIBRA	6	TIPO 2
246	REGIONAL	Buga	Carrera 18 Calle 10	Canal de Datos Secundario	FIBRA	4	
247	SUROCCIDENTE	Palmira	Calle 22 No. 32-74	Canal de Datos Principal	FIBRA	8	TIPO 2
248		Palmira	Calle 22 No. 32-75	Canal de Datos Secundario	FIBRA	4	
249		Yumbo	Calle 4 No. 2-24	Canal de Datos Principal	FIBRA	6	TIPO 3
250		Yumbo	Calle 4 No. 2-25	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
251		Buenaventura	Av. Simón Bolivar No. 17-40 - Barrio El Jorge Diagonal Urgencias Hospital Luis Ablanquec de la Plata	Canal de Datos Principal	FIBRA	8	TIPO 2
252		Buenaventura	Av. Simón Bolivar No. 17-40 - Barrio El Jorge Diagonal Urgencias Hospital Luis Ablanquec de la Plata	Canal de Datos Secundario	FIBRA	4	
253		Jamundí	Cll 4 No. 9-17 Av Circunvalar Jamundí contiguo Hospital Piloto Jamundí	Canal de Datos Principal	FIBRA	6	TIPO 3
254		Jamundí	Cll 4 No. 9-17 Av Circunvalar Jamundí contiguo Hospital Piloto Jamundí	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
255		Pasto	Calle 22 No. 7 - 93 Hospital Departamental - Parque Bolívar	Canal de Datos Principal	FIBRA	16	TIPO 2
256		Pasto	Calle 22 No. 7 - 93 Hospital Departamental - Parque Bolívar	Canal de Datos Secundario	FIBRA	8	
257		Tumaco	Ciudadela Sector Nuevo Horizonte Enseguida del Centro Hospital Divino Niño	Canal de Datos Principal	FIBRA	6	TIPO 3
258		Tumaco	Ciudadela Sector Nuevo Horizonte Enseguida del Centro Hospital Divino Niño	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
259		Ipiales	Avenida Panamericana Norte Hospital Civil Regional	Canal de Datos Principal	FIBRA	6	TIPO 3
260		Ipiales	Avenida Panamericana Norte Hospital Civil Regional	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
261		Tuquerres	Calle 27 No. 14-58 - Hospital San José	Canal de Datos Principal	FIBRA	6	TIPO 3
262		Tuquerres	Calle 27 No. 14-58 - Hospital San José	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
263		Popayán	Av. 17 Sur No. 10-95	Canal de Datos Principal	FIBRA	20	TIPO 2
264		Popayán	Av. 17 Sur No. 10-96	Canal de Datos Secundario	FIBRA	8	
265		Santander de Quilichao	Carrera 9 No. 2 Sur-36 - Barrio Canalón	Canal de Datos Principal	FIBRA	6	TIPO 3
266		Santander de Quilichao	Carrera 9 No. 2 Sur-36 - Barrio Canalón	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
267		Santander de Quilichao	Carrera 1-01 Barrio Santa Teresita	Canal de Datos Principal	FIBRA	6	TIPO 3
268		Santander de Quilichao	Carrera 1-01 Barrio Santa Teresita	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	

269	REGIONAL SUR	Neiva	Calle 13 No. 5 - 140	Canal de Datos Principal	FIBRA	20	TIPO 1
270		Neiva	Calle 13 No. 5 - 141	Canal de Datos Secundario	FIBRA	15	
271		Neiva	Carrera 5 sur No.17-65 Zona Industrial Sur	Canal de Datos Principal	FIBRA	20	TIPO 2
272		Neiva	Carrera 5 sur No.17-65 Zona Industrial Sur	Canal de Datos Secundario	FIBRA	15	
273		Garzón	Cra. 8 Calle 8 Of 102 (Palacio de Justicia)	Canal de Datos Principal	FIBRA	6	TIPO 3
274		Garzón	Cra. 8 Calle 8 Of 102 (Palacio de Justicia)	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
275		Pitalito	Diag. 3 sur # 1a - 89 Av. Juan Bosco (Hospital San Antonio)	Canal de Datos Principal	FIBRA	6	TIPO 3
276		Pitalito	Diag. 3 sur # 1a - 89 Av. Juan Bosco (Hospital San Antonio)	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
277		La Plata	Cra. 8 # 10A - 32 (Casa de Justicia)	Canal de Datos Principal	FIBRA	6	TIPO 3
278		La Plata	Cra. 8 # 10A - 32 (Casa de Justicia)	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
279		Ibagué	Calle 45 No. 8 Sur-58, Zona Industrial El Papayo	Canal de Datos Principal	FIBRA	30	TIPO 2
280		Ibagué	Calle 45 No. 8 Sur-58, Zona Industrial El Papayo	Canal de Datos Secundario	FIBRA	15	
281		Chaparral	Diagonal 8 No. 12 - 00 (Casa de Justicia)	Canal de Datos Principal	FIBRA	6	TIPO 3
282		Chaparral	Diagonal 8 No. 12 - 00 (Casa de Justicia)	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
283		Espinal	CENTRO DE CONVIVENCIA CIUDADANA, MZ E y F B/VILLA PAZ	Canal de Datos Principal	FIBRA	6	TIPO 3
284		Espinal	CENTRO DE CONVIVENCIA CIUDADANA, MZ E y F B/VILLA PAZ	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
285		Honda	Calle 9 # 22A – 193 (Hospital San Juan de Dios)	Canal de Datos Principal	FIBRA	6	TIPO 2
286		Honda	Calle 9 # 22A – 193 (Hospital San Juan de Dios)	Canal de Datos Secundario	FIBRA	4	
287		Florencia	Carrera 10 No. 5A - 28 Barrio Avenidas	Canal de Datos Principal	FIBRA	12	TIPO 2
288		Florencia	Carrera 10 No. 5A - 28 Barrio Avenidas	Canal de Datos Secundario	FIBRA	4	
289		Mocoa	Calle 8 # 2 - 27 (Casa de Justicia) Barrio San Agustín.	Canal de Datos Principal	FIBRA	6	TIPO 3
290		Mocoa	Calle 8 # 2 - 27 (Casa de Justicia) Barrio San Agustín.	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
291		Puerto Asís	Calle 14 Cra 19 esquina Casa de la Justicia	Canal de Datos Principal	FIBRA	6	TIPO 3
292		Puerto Asís	Calle 14 Cra 19 esquina Casa de la Justicia	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	
293		San Miguel	Centro de Convivencia Ciudadana (CCC) del barrio 7 de agosto en Calle 3 Carrera 12 esquina,	Canal de Datos Principal	FIBRA	4	TIPO 2
294		San Miguel	Centro de Convivencia Ciudadana (CCC) del barrio 7 de agosto en Calle 3 Carrera 12 esquina,	Canal de Datos Secundario	FIBRA	4	
295		San Miguel	ubicada a la entrada del municipio de San Miguel (con coordenadas geográficas 0.35279, -76.91033)	Canal de Datos Principal	FIBRA	4	TIPO 3
296		San Miguel	ubicada a la entrada del municipio de San Miguel (con coordenadas geográficas 0.35279, -76.91033)	Canal de Datos Secundario	LTE	Bolsa de 2TB de conectividad gestionada	

Para las sedes donde no se tenga definido un enlace de contingencia a través de fibra óptica, el oferente deberá presentar las siguientes cotizaciones, con el fin de evaluar un plan de contingencia que podrá ser de infraestructura entro de las opciones se encuentran:

- Servicio LTE, garantizando cobertura del 100%.
- Canales de Internet satelital de órbita baja (LEO), con un plan de navegación de 500 GB mensuales.
- Canales dedicados en fibra óptica.

Para las sedes de Mitú, Puerto Carreño, Puerto Inírida y Leticia únicamente aplica el esquema solicitado en el anexo de conectividad con las siguientes características mínimas o superiores:

- *Canal Ppal En Órbita (LEO),*

  - Tipo: Antena electrónica de **matriz faseada (phased array)**.
  - Orientación: Automática.
  - Banda de operación: **Ku y/o Ka**.
  - Compatibilidad: Constelaciones satelitales **LEO**.
  - Instalación: Exterior, con soporte para montaje fijo.
  - Condiciones ambientales:
  - Operación a la intemperie.
  - Rango de temperatura operativa mínimo: **–10 °C a +50 °C**.
  - Operación continua 24/7.
  - Velocidad mínima de descarga: **≥ 15 Mbps**.
  - Velocidad mínima de carga: **≥ 3 Mbps**.
  - Latencia promedio: **≤ 80 ms**.
  - Disponibilidad mensual del servicio: **≥ 97 %**.
  - Puertos LAN: Mínimo 1 puerto Ethernet 10/100/1000 Mbps.
  - Conectividad Wi-Fi:
  - Estándar IEEE 802.11ac o superior.
  - Banda de 2,4 GHz (5 GHz opcional).
  - Funcionalidades mínimas:
  - Firewall integrado.
  - Soporte de cifrado WPA2 o superior.
  - Actualización de firmware.
  - Gestión: Administración local.

Los anteriores parámetros se consideran suficientes para garantizar la operación básica de las Sedes Tipo 3, atendiendo su nivel de criticidad y uso institucional.

- *Canal Backup En VSAT GEO)*

De esta manera, la entidad estableció diferentes tipos de sede para definir las especificaciones técnicas mínimas o superiores de los equipos SDWAN según cada ubicación:

Sede Tipo 1.

Para las Sedes Tipo 1, entendidas como aquellas que disponen de dos (2) equipos SD-WAN en esquema de alta disponibilidad y cuentan con dos (2) canales de acceso en fibra óptica, el nivel de acuerdo de servicio (ANS) de disponibilidad de la red de acceso deberá ser, como mínimo, del 99,98% mensual. Por ello las características mínimas o superiores son:

- *IPS throughput: hasta 14 Gbps*
- *NGFW throughput: hasta 11,5 Gbps*
- *Threat Protection throughput: hasta 10,5 Gbps*
- *Latencia: ultra baja, optimizada mediante procesadores de seguridad (SPU) propietarios*
- *Interfaces de red*
- *Puertos de alta velocidad:*
  - ✓ *Múltiples 25 GbE SFP28*
  - ✓ *10 GbE SFP+*
  - ✓ *1 GbE SFP*
- *Puertos Ethernet RJ-45 1 GbE*
- *Alta densidad de interfaces, diseñada para entornos de alto tráfico y consolidación de servicios*

Sede Tipo 2.

Para las Sedes Tipo 2, entendidas como aquellas que disponen de un (1) equipo SD-WAN y cuentan con doble canal de acceso en fibra óptica, el nivel de acuerdo de servicio (ANS) de disponibilidad de la red de acceso deberá ser, como mínimo, del 99,9% mensual. El equipo debe cumplir con las siguientes características mínimas requeridas o superiores:

- *IPS Throughput: 2.6 Gbps*
- *NGFW Throughput: 1.6 Gbps*
- *Threat Protection Throughput: 1 Gbps*
- *Concurrent Sessions (TCP): 1.5 millones*
- *New Sessions/Second (TCP): 56 000*
- *Interfaces:*
  - ✓ *2 x GE RJ45 WAN Ports*
  - ✓ *2 x GE RJ45 para Gestión y HA*
  - ✓ *12 x GE RJ45*
  - ✓ *2 x 10 GE SFP+ Slots*
  - ✓ *4 x GE SFP Slots*

Sede Tipo 3.

Para las sedes tipo 3, entendidas como aquellas que cuenten con una **solución de canal en fibra óptica y LTE**, el **nivel de acuerdo de servicio (ANS) de disponibilidad de la red de acceso** deberá ser, como mínimo, del **99,7% mensual**. El equipo debe cumplir con las siguientes características mínimas requeridas o

superiores:

- ✓ *PS Throughput: 1.4 Gbps*
- ✓ *NGFW Throughput: 1 Gbps*
- ✓ *Threat Protection Throughput: 700 Mbps*
- ✓ *Concurrent Sessions (TCP): 700 000*
- ✓ *New Sessions/Second (TCP): 35 000*
- ✓ *Interfaces:*
- ✓ *2 x GE RJ45 WAN Ports*
- ✓ *1 x GE RJ45 DMZ Port*
- ✓ *7 x GE RJ45 Internal Ports*

De esta manera, se garantiza de forma temporal la continuidad del servicio en la sede afectada.

El INMLCF aceptará equipos usados con una antigüedad máxima de 36 meses para la instalación y prestación de todos los servicios. Sin embargo, será necesario presentar una certificación directa del fabricante dirigida al INMLCF, expedida con una fecha no mayor a 30 días antes del cierre de este proceso, en la que se confirme que los equipos se encuentran con soporte y garantía de fabrica vigente. Además, el oferente deberá garantizar que los equipos no tienen EOL (Fin de Ciclo de Vida) durante la vigencia inicial del contrato y por 12 meses adicionales.

El proveedor debe entregar una certificación del fabricante que confirme que los equipos cumplen con las regulaciones de licencia de exportación (export compliance) requeridas para su suministro al INMLCF.

El INMLCF está adquiriendo un servicio; por tanto, verificará la capacidad de todos los dispositivos que utilice el contratista, con el fin de garantizar el cumplimiento de los parámetros requeridos y la viabilidad del objeto contractual.

El proveedor deberá estar certificado como MSSP (Managed Security Service Provider) del fabricante de la solución ofertada, este deberá adjuntar a la oferta la certificación vigente que lo acredite como tal.

El proveedor debe presentar, en su propuesta, una solución SD-WAN Seguro que incluya los mismos campos definidos por el INMLCF en el requerimiento de conectividad (ver Anexo conectividad) y que cumpla, como mínimo, con las siguientes características:

El oferente deberá acreditar y garantizar que la plataforma ofertada es plenamente compatible y permite una integración funcional, nativa y al cien por ciento (100 %) con la marca y los equipos actualmente instalados y de propiedad del Instituto Nacional de Medicina Legal y Ciencias Forenses (INMLCF).

La solución propuesta deberá asegurar la interoperabilidad total, el correcto funcionamiento y el

aprovechamiento integral de las capacidades técnicas existentes, sin requerir reemplazos, adaptaciones, licenciamientos adicionales ni desarrollos especiales por parte de la Entidad.

Los CPE (Customer Premises Equipment) que hacen parte del servicio deberán soportar IPv4 e IPv6 (Dual Stack) a nivel de enrutamiento y corresponder a la última serie disponible, con el fin de garantizar soporte y garantía de fábrica durante la vigencia del contrato.

La tecnología ofrecida deberá soportar IPv4 e IPv6, de acuerdo con las especificaciones definidas por la Entidad (servicio de internet).

Se deberá realizar el despliegue del overlay de SD-WAN de forma que cada sede pueda contar con diferentes arquitecturas de conectividad. En consecuencia, las conexiones subyacentes (underlay) podrán incluir instancias únicas o múltiples de redes privadas/MPLS, internet público y/o conectividad 3G/4G/LTE, de naturaleza privada o pública, según las opciones descritas. El underlay requerido por la entidad para el despliegue de la tecnología SD-WAN Seguro es Internet – Internet.

Se requiere que, desde la plataforma de administración de SD-WAN, sea posible configurar políticas que restrinjan la conectividad, de manera que los CPE solo establezcan conexiones entre nodos que se encuentren en la misma red de transporte.

Los dispositivos de comunicaciones deberán permitir administración y monitoreo mediante el protocolo seguro SSH versión 3, con cifrado, y su visualización en la solución ofrecida.

La solución ofertada deberá permitir el despliegue de políticas específicas del overlay y contemplar, como mínimo, los siguientes criterios de configuración: balanceo de carga, enlace principal y respaldo (backup), y enrutamiento por aplicaciones.

Para el enrutamiento basado en aplicaciones, la solución deberá validar las características de los túneles del plano de datos entre los CPE y utilizar la información recopilada para calcular rutas óptimas para el tráfico.

Se deberá contar con la capacidad de considerar, para la selección de rutas, factores distintos a los utilizados por protocolos de enrutamiento estándar, tales como prefijos, métricas y estado del enlace.

Las políticas de enrutamiento deberán permitir granularidad basada, como mínimo, en aplicaciones, direcciones IP, puertos UDP/TCP y marcación de calidad de servicio (QoS).

La solución deberá permitir definir preferencias sobre las conexiones que utilizarán las aplicaciones en cada sede o tipo de sede, de acuerdo con políticas seleccionadas que podrán asociarse, entre otros,

a jitter, latencia, número de sesiones, ocupación del canal y fallas de conectividad. Asimismo, deberá establecer la contingencia correspondiente conforme a los ANS (acuerdos de nivel de servicio, SLA) definidos.

Todas las configuraciones deberán definirse de manera centralizada desde la plataforma de administración de SD-WAN hacia el CPE, o los CPE, según los tipos de sede previamente definidos. La plataforma de administración deberá estar ubicada en el centro de datos alterno ofertado por el operador e incluirse como parte integral del servicio.

La solución SD-WAN ofertada deberá contar con capacidades de monitoreo y medición en el plano de datos, y sondear periódicamente los túneles en los CPE para recopilar latencia, pérdida, duplicación de paquetes y demás estadísticas necesarias para el enrutamiento basado en aplicaciones.

Para los CPE, la solución deberá cumplir, como mínimo, con las siguientes características de seguridad entre los CPE y la plataforma de administración:

Cada CPE deberá realizar una autenticación inicial contra la plataforma centralizada de administración de SD-WAN del operador, con el fin de validar su registro.

Una vez autenticado, el CPE deberá obtener desde la plataforma la configuración del overlay y las políticas de administración y control.

El proceso de autenticación de un nuevo dispositivo conectado a la nube SD-WAN deberá basarse en una base de datos de seriales u otro mecanismo equivalente definido en la plataforma de administración.

La solución SD-WAN ofertada deberá cumplir con los siguientes requisitos mínimos de seguridad:

Los equipos CPE en sedes remotas deberán generar sus propias claves de cifrado o utilizar certificados digitales.

Las claves de cifrado deberán tener caducidad y eliminarse de forma controlada en toda la red, o permitir la generación de llaves de encriptación aleatorias.

El tráfico entre CPE deberá cifrarse mediante IPsec, preservando la integridad de los paquetes, para evitar ataques de intermediario (man-in-the-middle).

El tráfico entre CPE deberá poder transmitirse a través de túneles dinámicos, de acuerdo con el RFC 7018, utilizando preshared keys o certificados digitales, tanto para IPv4 como para IPv6.

El CPE de la solución SD-WAN deberá contar con un motor integrado de inspección profunda de paquetes

(DPI) que permita el descubrimiento y la administración de aplicaciones. En consecuencia, cada CPE remoto deberá recopilar información sobre todos los flujos de aplicaciones que transiten por la red.

La solución en cada sede deberá permitir el acceso directo a internet (Direct Internet Access, DIA) según la entidad lo requiera, mediante el cual los equipos realicen conexión directa a internet en las sedes cuya conectividad a internet esté incluida dentro del alcance de la presente oferta, optimizando el uso de recursos del Internet centralizado.

La solución deberá brindar visibilidad sobre el comportamiento de las aplicaciones, incluyendo, como mínimo: usuarios conectados, tráfico consumido (subida/descarga), tipo de aplicación y características de la conexión (jitter, latencia, calidad de la conexión, entre otras).

La solución deberá medir el estado de los enlaces mediante métodos activos (TCP, ICMP u otros generados desde el dispositivo SD-WAN) y, adicionalmente, mediante el análisis del tráfico de usuario para determinar retardo, jitter y pérdida de paquetes.

La solución ofertada deberá permitir medir la calidad de los enlaces mediante Mean Opinión Score (MOS) y, con base en el resultado, tomar decisiones que permitan mejorar las políticas de enrutamiento inteligente las cuales son definidas a través del Jitter, pérdida de paquetes y latencia.

La solución deberá permitir la duplicación de paquetes para la adaptación a medios ruidosos. Asimismo, deberá soportar Forward Error Correction (FEC).

La solución deberá permitir aplicar reglas de SD-WAN para aplicaciones personalizadas de la entidad.

La solución SD-WAN ofertada deberá permitir la selección dinámica de rutas mediante enrutamiento inteligente, con base en parámetros tales como latencia, jitter, pérdida de paquetes, peso y otros, que garanticen el adecuado desempeño de las aplicaciones de la entidad.

Los dispositivos de la solución SD-WAN deberán estar en capacidad de establecer una VPN con la sede central, con el fin de mantener el acceso a los aplicativos internos de la entidad.

La solución deberá soportar enrutamiento de tráfico basado en el usuario, además de la aplicación o la dirección IP de origen o destino.

La solución de SDWAN deberá contemplar la nube de Microsoft Azure adquirida por el INMLCF como una sede adicional del instituto y deberá cumplir las siguientes características:

La Entidad, en el marco de su estrategia de transformación digital y fortalecimiento de la infraestructura de TI, requiere la contratación de un servicio integral para el diseño, implementación, puesta en marcha, soporte y operación de una solución de SD-WAN sobre infraestructura de nube pública.

El objetivo principal es garantizar la interconexión segura, ágil y de alta disponibilidad de las sedes institucionales con los servicios alojados en la nube. Para ello, se establece como requisito mandatorio el despliegue de la solución SD-WAN bajo una arquitectura Multi-Región (Single Availability Zone por región) en el entorno de Azure, asegurando la resiliencia del servicio ante contingencias regionales y optimizando el enrutamiento de tráfico crítico mediante políticas de calidad de servicio (QoS) y selección dinámica de rutas.

Este despliegue deberá integrarse de manera nativa con las sedes SD-WAN de la entidad y el servicio de seguridad perimetral, permitiendo una gestión centralizada, visibilidad total del tráfico y el cumplimiento de los niveles de servicio (SLA) exigidos para la entidad.

Para el cumplimiento del objeto anteriormente descrito, el proponente deberá cumplir con las siguientes consideraciones técnicas mínimas para el diseño de la solución:

- *Suministrar el licenciamiento para el despliegue de un equipo de SD-WAN Seguro por cada Región. Este dispositivo deberá soportar las siguientes consideraciones técnicas:*
- *Azure Expected Bandwidth: 12 500 Mbps.*
- *Firewall Throughput (UDP Packets) in Mbps - 1280 bytes: 12 500*
- *Firewall Throughput (UDP Packets) in Mbps - 512 bytes: 11 900*
- *Firewall Throughput (UDP Packets) in Mbps - 64 bytes: 1 950*
- *New Sessions / Second (TCP): 17 200*
- *HTTP Throughput w/ Application profile (64K size) in Mbps: 12 700*
- *HTTP Throughput w/ IPS profile (44K size) in Mbps: 12 700*
- *HTTP Throughput w/ IPS profile (1M size) in Mbps: 12 700*
- *NGFW Throughput (Mbps): 2 960*
- *Threat Protection Throughput (Mbps): 2 950*
- *SSL Inspection throughput (Mbps): 5 510*
- *La entidad será responsable de suministrar el cómputo y networking requeridos para la puesta en marcha de este servicio. Sin embargo, el oferente será responsable de asesorar e indicar a la*

entidad cada uno de los requerimientos técnicos para la implementación, puesta en marcha, operación y soporte de la tecnología SD-WAN en Azure a través de una Virtual Network de Seguridad, la cual se interconectará con la Virtual Network de producción vía Virtual Network Peering.

- *La solución de SD-WAN desplegada en Azure deberá actuar como el núcleo de seguridad e inspección centralizada, garantizando el control total tanto del tráfico norte-sur (ingreso y egreso entre la nube pública, internet y las sedes institucionales) como del tráfico este-oeste (movimiento lateral entre redes virtuales). Para ello, el diseño técnico debe asegurar que el 100% de los flujos de datos sean interceptados y validados mediante el uso de tablas de enrutamiento personalizadas o servicios de orquestación nativos con capacidades de inspección profunda de paquetes (DPI) para prevenir amenazas externas y mitigar cualquier intento de comunicación no autorizada entre los activos internos de la entidad.*

Obligación de Integración con el Sistema de Monitoreo de la Entidad

El PROVEEDOR deberá configurar, habilitar e integrar la totalidad de los activos de red y componentes de la solución suministrada (incluyendo, pero sin limitarse a, dispositivos de conectividad, seguridad, SD-WAN, enlaces y equipos asociados) con el sistema de monitoreo i infraestructura local (on-premises) o en la nube de Microsoft Azure, garantizando su correcta interoperabilidad y operación.

Dicha integración deberá realizarse de manera obligatoria mediante:

SNMP versión 3 (SNMPv3), asegurando mecanismos de autenticación, integridad y cifrado, para la supervisión del estado, desempeño, disponibilidad y alertamiento de los activos de red.

IPFIX (NetFlow) o el protocolo correspondiente de análisis de tráfico, para la recolección, exportación y análisis de flujos de red, permitiendo la visibilidad del consumo de ancho de banda, aplicaciones, direcciones origen y destino, patrones de tráfico y demás métricas requeridas para la gestión operativa, capacidad y seguridad.

El PROVEEDOR deberá asegurar que la información recolectada sea continua, confiable, íntegra y visible en tiempo real o cuasi real desde las plataformas de monitoreo de la Entidad, independientemente de su ubicación tecnológica (on-premises o nube Azure), sin costos adicionales y durante toda la vigencia del contrato.

- *Así mismo, el PROVEEDOR será responsable de realizar todas las configuraciones, ajustes, pruebas, validaciones técnicas y correcciones necesarias para garantizar la correcta operación e interoperabilidad de los protocolos mencionados, conforme a las políticas de seguridad, monitoreo y arquitectura tecnológica definidas por la Entidad.*

*El **incumplimiento de esta obligación será considerado incumplimiento grave del contrato**, habilitando a la Entidad para la aplicación de las penalidades correspondientes y demás medidas contractuales a que haya lugar.*

Conectividad WAN segura.

La solución ofertada deberá contar, como mínimo, con un método de cifrado basado en IPsec, para garantizar el transporte seguro mediante túneles dinámicos. Se requiere que el overlay generado soporte

IPsec con cifrado fuerte (algoritmos mínimos AES-128 o AES-256, con autenticación mínima SHA-256), de manera que se proteja la información ante posibles ataques de intermediario (man-in-the-middle). Para este fin, los equipos deberán contar con hardware de propósito específico para cifrado.

La solución debe estar respaldada por un laboratorio de investigación y desarrollo que ofrezca inteligencia en tiempo real entregando actualizaciones de seguridad completas, investigadores de amenazas de seguridad, ingenieros y especialistas forenses.

La solución debe soportar filtrado de contenido mediante 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.

Debe basarse en categorías de aplicaciones que permitan seleccionar grupos de firmas basados en un tipo de categoría.

Los equipos deberán ser capaces de analizar contenido cifrado (SSL o SSH) para habilitar, como mínimo, las funcionalidades de filtrado de URL, control de aplicaciones, prevención de fuga de información (DLP), antivirus e IPS.

- *El Antivirus deberá integrarse de forma nativa con una solución de protección de amenazas de día cero locales o en la nube del fabricante, de tal manera que envíen muestras de archivos a dicha solución para su análisis.*

Control y visibilidad de aplicaciones: la solución deberá facilitar topologías flexibles y seguras por aplicación o segmento de internet, optimizar la prioridad del tráfico para más de 4.000 aplicaciones y permitir la personalización de aplicaciones propias de la entidad.

El reconocimiento de aplicaciones deberá realizarse de forma independiente del puerto y del protocolo del tráfico, e identificar la aplicación desde el primer paquete recibido.

Administración y gestión centralizada dedicada y de uso exclusivo para la entidad: el oferente deberá presentar una solución que permita realizar cambios de reglas mediante una plataforma centralizada y proporcionar monitoreo integrado de aplicaciones. Esta plataforma debe ser dedicada y de uso exclusivo para la entidad. La administración deberá realizarse a través de una interfaz gráfica de usuario (GUI) vía web, por HTTPS, ya sea de manera centralizada o descentralizada en cada dispositivo. El INMLCF deberá contar con usuarios de solo visualización para acceder a estas interfaces, con el fin de validar configuraciones y auditar los equipos.

Ante la falla del controlador/orquestador de la solución, o la pérdida de conectividad hacia este, la solución deberá permitir la configuración de nuevas políticas de enrutamiento SD-WAN y monitores de tráfico directamente sobre los equipos SD-WAN en las diferentes ubicaciones. Cuando el controlador/orquestador se encuentre nuevamente en línea, o se restablezca la conexión con él, deberá ser posible importar en el orquestador los cambios realizados.

El oferente deberá garantizar que los CPE se encuentren en correcto estado, sin alertas, y actualizados a la última versión estable. Con cada actualización realizada, deberá entregar un informe ejecutivo con las tareas ejecutadas y el estado actual de la plataforma. Si las actividades de actualización generan indisponibilidad, se deberá presentar un plan de trabajo con ocho (8) días hábiles de anticipación. En caso de que la necesidad de actualización o mantenimiento sea crítica (afecta la continuidad del negocio), se deberá informar de manera inmediata para tramitar internamente los permisos y ejecutar la actividad en el menor tiempo posible.

Todas las funcionalidades descritas anteriormente, se deberán garantizar para todos los equipos que hagan parte de la solución de SD-WAN, tanto en las sedes de la entidad como los equipos desplegados en nube pública.

Análisis y reportes de la solución con plataforma dedicada y de uso exclusivo: la solución ofertada deberá cumplir, como mínimo, con los siguientes reportes mediante una solución centralizada y de uso exclusivo para la entidad, ubicada en el centro de datos del operador y prestada como parte integral del servicio:

- *Visualización detallada de: utilización de ancho de banda, disponibilidad, estado de los enlaces, top 10 de consumo de ancho de banda por direcciones IP y top de aplicaciones.*
- *Informes de tráfico por sitio: disponibilidad del servicio, uso de ancho de banda por circuito de acceso, uso de ancho de banda por aplicación, calidad de experiencia (QoE) por cada circuito de conexión, retardo (delay) y pérdida de paquetes.*
- *Georreferenciación: identificación de un dispositivo SD-WAN dentro de un área geográfica amplia; no incluye la identificación de una dirección específica con ubicación precisa.*
- *Top 10 de URL y aplicaciones bloqueadas, e IP que las consultaban.*
- *Se deberán entregar, como mínimo, los siguientes informes sobre los equipos con características de seguridad configuradas:*
    - ✓ *Informes de firewall: registros (logs) de reglas con acción deny.*
    - ✓ *Informes de tráfico web: top de sitios visitados, direcciones de origen y destino, y reputación de URL (URL reputation).*
    - ✓ *Informes de políticas: filtrado de URL.*

- ✓ *Informe mensual de control de cambios.*
- ✓ *Informes sobre VPN: usuarios, duración de sesiones y horas de conexión.*
- ✓ *Informes de virus, ataques o amenazas.*
- ✓ *Informe de disponibilidad de cada nodo activo en la red.*

Nota: las sedes con UTM propiedad del INMLCF no deben tener configuradas estas características, ya que pueden superponerse con las políticas ya aplicadas en los equipos del INMLCF y provocar el incumplimiento de alguna de ellas. A menos que, el oferente suministre un dispositivo SD-WAN de la misma referencia que el de la entidad, con el fin de poder formar un clúster en Alta Disponibilidad para las sedes que apliquen.

Servicio de conectividad en los puntos de atención indicados en estos términos de referencia.
El proveedor deberá habilitar una línea gratuita para el "Servicio de Atención y Soporte Técnico", con horario de atención 24 horas al día, los 365 días del año.
Conexión al NAP: el proveedor deberá estar inscrito en el NAP Colombia; para ello, deberá adjuntar certificado expedido por la C.C.I.T.
La relación de reúso del servicio ofrecido deberá ser 1:1 y con simetría para los canales principales de internet, así como para los enlaces de respaldo (backup).

1	***Operación y mantenimiento de SD-WAN*** *El proveedor deberá garantizar la operación y el mantenimiento de los equipos SD-WAN que hacen parte de la solución implementada, sin que estas actividades generen costos adicionales para el Instituto Nacional de Medicina Legal y Ciencias Forenses (INMLCF).*
2	***Reportes de la solución SD-WAN*** *El proveedor deberá entregar los reportes definidos en la sección correspondiente a SD-WAN,*

	con el propósito de proporcionar visibilidad y control sobre el tráfico autorizado de la entidad.
3	***Herramienta de gestión remota*** *El proveedor deberá contar con una herramienta de gestión remota que permita identificar de manera oportunidad cualquier tipo de falla o afectación en el servicio de conectividad garantizando tiempos de atención eficientes. Asimismo, deberá otorgar al INMLCF, cuatro (4) usuarios accesos a dicha herramienta para labores de seguimiento, control y auditoría.*
4	***Redundancia de enlaces del proveedor*** *El proveedor del servicio de internet deberá contar con redundancia en sus enlaces de salida, tanto a nivel nacional como internacional, incluyendo mecanismos de contingencia y respaldo que aseguren la continuidad del servicio.*
5	***Direccionamiento IP público – Nivel Central*** *El proveedor deberá especificar y garantizar direcciones IP públicas fijas para el canal de internet de la sede del Nivel Central.* *Se deberá suministrar, como mínimo, el siguiente esquema de direccionamiento:* • ***Un (1) pool de direccionamiento con al menos 48 direcciones IP públicas fijas.***

POOL	***DESCRIPCIÓN***	***OPCIÓN***
1	*48 IP PÚBLICAS FIJAS (MÍNIMO)*	*48 IP FIJAS*

Nota: *Se permitirá que las 48 direcciones IP públicas requeridas sean suministradas de manera contigua, es decir, dentro de un único pool de direccionamiento.*

6	***Servicio para Protección anti-DDoS*** *Se debe incluir una solución de protección anti-DDoS en nube que cubra las aplicaciones expuestas en Azure en capa 4 y capa 7 así como cualquier sede que defina la entidad. Además, para las sedes de la entidad se deberá suministrar el servicio de AntiDDoS en capa 3 y capa 4. La solución deberá permitir la mitigación de ataques directamente en los puntos de entrada a internet. El proveedor deberá indicar cual es la herramienta utilizada.*
7	***Acuerdos de niveles de servicio (SLA)*** *El proveedor deberá describir de manera detallada los acuerdos de niveles de servicio (SLA), los cuales deberán contemplar, como mínimo, los siguientes aspectos:* • *Disponibilidad del servicio.* • *Tiempos de atención y solución de fallas.* • *Latencia.* • *Niveles de escalamiento.* • *Mecanismos de aseguramiento para los servicios de conectividad.*
8	***Tiempos de aprovisionamiento*** *Para la implementación de los servicios se requiere que todos los servicios estén instalados y operativos el 01 de Julio de 2026.* *Para para todas las sedes de SD-WAN, como la conectividad hacia Azure, los servicios de SD-LAN, SDWAN en Nube Pública, Servicio De Identidad Y Acceso, Servicio Zero Trust Network Access (Ztna), Reconocimiento De Marca, Protección Para Correo Electrónico, entre otros, el proveedor deberá establecer un cronograma de implementación en conjunto con la entidad entendiendo que el INMLCF realizará la migración a Azure y deberá estar alienado a las actividades de Azure.*
9	***Gestión de canales de datos y control contractual***

	Para los siguientes requerimientos: • *Nuevos puntos de canales de datos.* • *Traslados de canales de datos.* • *Cancelación de canales de datos.* • *Suspensión de canales de datos.* *Se deberán mantener los mismos tiempos establecidos en el ítem 12.* *La supervisión del contrato por parte del INMLCF tendrá la facultad de gestionar las solicitudes que se generen y de aceptar las ofertas relacionadas con la adquisición de nuevos canales o con los trámites asociados a canales de datos existentes, conforme a las estipulaciones técnicas y contractuales vigentes para la prestación de servicios de telecomunicaciones, seguridad y tecnologías de la información, previa revisión y balance del contrato.* *Lo anterior tiene como finalidad garantizar la viabilidad presupuestal para atender las solicitudes y gestionar los requerimientos al interior de la entidad.* *Asimismo, el control y la vigilancia ejercidos por la supervisión permitirán regionalizar los recursos del contrato, con el fin de determinar y controlar el presupuesto correspondiente a cada regional. Para la gestión de nuevos puntos, traslados, cancelaciones, suspensiones o nuevos servicios, se deberá contar con un control presupuestal que permita un seguimiento adecuado del contrato.* *En caso de requerirse una adición presupuestal, esta deberá ser tramitada y aprobada previamente por el INMLCF, siempre que corresponda a soluciones ofrecidas por el proveedor.*
10	***Requerimientos físicos de la solución*** *El proveedor deberá detallar los requerimientos físicos necesarios para la puesta en marcha y operación de la solución ofrecida, incluyendo como mínimo:* • *Condiciones eléctricas requeridas.*

	• *Rango de temperatura ambiente del sitio de instalación.* • *Racks o gabinetes necesarios.* • *Espacio requerido para la ubicación de equipos.* • *Condiciones de interconexión con los equipos de datos existentes.*
11	***Certificación del fabricante*** *El proveedor deberá aportar certificación del fabricante que acredite las tecnologías SD-WAN ofertadas sobre el Core de la red del operador, en calidad de* ***Partner Expert MSSP (Managed Security Service Provider).***
12	*El proveedor deberá garantizar cobertura en cada una de las zonas contratadas, previendo futuros traslados de las unidades o puntos de atención.*
13	*El proveedor deberá garantizar la prestación del servicio al Instituto mediante atención especializada durante la instalación y con posterioridad a esta, brindando soporte a la solución implementada. Asimismo, deberá entregar la topología y los diagramas de la solución implementada y, al finalizar el contrato, la topología y los anchos de banda finales.*
14	*El proveedor deberá ofrecer flexibilidad para la adición de nuevos servicios, así como para el traslado o la adición de puntos de atención que se requieran durante la vigencia del contrato, previa confirmación de la factibilidad técnica y económica por parte del operador y aprobación por parte del Instituto de los costos adicionales asociados, de acuerdo con las necesidades del Instituto Nacional de Medicina Legal y Ciencias Forenses.*
15	*El proveedor debe contemplar dentro de la tarifa de servicio propuesta, los equipos necesarios para la prestación del servicio.*
16	*El proveedor debe suministrar equipos y demás componentes tecnológicos de excelente*

	calidad, tal que garanticen la estabilidad de las conexiones sin interrupción del servicio.
17	*El proveedor podrá mejorar la propuesta de tipo de conexión y velocidades por punto de atención, siempre y cuando no afecte el presupuesto total asignado, quedando a discrecionalidad del Instituto el servicio a tomar. En este punto, el proveedor podrá proponer conexiones de canales dedicados con salida principal a internet desde el nivel central, habilitando un esquema de intranet.*
18	*Los servicios solicitados deberán implementarse y entregarse en operación. La fecha de entrega de cada servicio deberá quedar registrada en el acta de aceptación y recepción, la cual deberá ser firmada por el encargado de cada punto de atención (el facilitador de la regional o la persona designada en el punto de atención del INMLCF) y el supervisor del contrato.*
19	*El proveedor debe cumplir con los tipos de conexiones y anchos de banda requeridos por el INMLCF para cada uno de los canales de datos.* *En caso de presentarse una factibilidad terrestre negativa en las direcciones indicadas, el proveedor deberá reemplazarla por un enlace satelital VSAT TDMA en banda Ku + enlace de orbita baja LEO (Multiórbita), con disponibilidad de 99,6% (se aclara que este tipo de enlaces no corresponden a un servicio satelital dedicado SCPC; sin embargo, presenta un buen desempeño para el servicio requerido). En ningún caso podrá ser reemplazado por un enlace satelital básico VSAT en banda Ka,. Este cambio deberá ser propuesto por el proveedor y posteriormente aceptado por el INMLCF.* *Todo lo anterior, sin costo adicional para el Instituto.*
20	*El proveedor deberá garantizar y conservar la configuración de redundancia mediante un esquema de SD-WAN con dos canales de internet para 52 sedes que defina la entidad del nivel nacional (regionales, seccionales y algunas unidades básicas), generando un esquema de alta disponibilidad para los enlaces en ciudades capitales y sedes con alto volumen de atención, donde funciona cada Dirección Regional, incluyendo canales alternos que se llegaren a instalar. En este caso, el proveedor deberá realizar todas las actividades*

	necesarias para dejar en funcionamiento la redundancia de ambos canales mediante balanceo dinámico, considerando los elementos requeridos para redireccionar el tráfico cuando se presente indisponibilidad en alguno de los canales. *Es decir, ante la indisponibilidad del canal de datos, el tráfico deberá enrutarse de forma automática al canal alterno, el cual asumirá los servicios (voz y datos), y viceversa. De esta manera, se garantiza la disponibilidad de los servicios de voz, datos e internet.* *Las demás sedes que no cuenten con este esquema mencionado deben incluir la contingencia o canal de respaldo con Fibra, Satelital LEO (órbita baja) o LTE, garantizando cobertura del 100%, esto según lo defina la entidad.*
21	*El proveedor deberá presentar una solución del servicio del canal de internet principal (H.A) y del canal de internet secundario (H.A) en modalidad activo-activo, de manera que, si por algún motivo uno de los dos canales falla, el canal secundario continúe su operación normal (y viceversa), dado que las rutas y configuraciones también se encuentran activas en ambos. El canal de internet principal y el canal de internet secundario deberán configurarse en anillos de fibra diferentes.*
22	*En caso de que la entidad requiera un esquema de caracterización por aplicación con el fin de brindar QoS sobre los canales que componen la solución SD-WAN, el proveedor deberá entregar los servicios garantizando la configuración correspondiente en sus equipos.*
23	*Para la sede San Martín, es necesario contar con dos (2) equipos de SDWAN Seguro f en redundancia y Alta Disponibilidad; por lo tanto, se deberá contemplar una solución alterna en alquiler para el equipo requerido para el esquema SD-WAN. El dispositivo propuesto deberá cumplir con las siguientes consideraciones técnicas:* • *IPS Throughput: 14 Gbps* • *NGFW Throughput: 11.5 Gbps* • *Threat Protection Throughput: 10.5 Gbps* • *Concurrent Sessions (TCP): 8 millones*

	• *New Sessions/Second (TCP): 550 000* • *2 x GE R45 para Gestión y HA* • *16 x GE R45* • *8 x GE SFP Slots* • *4 x 10GE/GE SFP+/SP Slots* • *4 x 25GE/10GE SFP28/SFP+ Ultra Low Latency*
24	*Conectividad Nube Publica Servicios de Azure: El INMLCF requiere una conexión Express Routing hacia la nube de azure en cada región para la conexión de los servicios de nube con la red de conectividad del instituto para lo cual el proveedor deberá cumplir los siguientes requisitos:* • *Ancho de Banda requerido por cada Región: 1000 Mbps, Los servicios de Express Routing deberán ser entregar en la región EAST US y West US a través de un puerto hosteado.* • *Los servicios de conectividad provistos en cada región deberán ser totalmente independientes y no tener puntos de falla en común en el transporte internacional. Es decir, cada servicio de conectividad deberá ser aprovisionado a través de rutas internacionales independientes.*
25	*Para sedes nuevas que la entidad requiera cotizar posteriormente y adicionales a los incluidos en el anexo 1.1 Conectividad los tiempos máximos de aprovisionamiento que comprenden factibilidad, instalación, puesta en funcionamiento y entrada en operación del servicio— deberán ser los siguientes:* • *Soluciones provistas directamente por el proveedor: máximo 45 días calendario.* • *Soluciones provistas con aliados: máximo 60 días calendario.*

	• *Soluciones provistas con otros operadores: máximo 90 días calendario.*

El proveedor establecerá, junto con la entidad, un cronograma de implementación alineado a las actividades de migración hacia Azure previstas por el INMLF. Una vez se disponga de los canales y servicios de ciberseguridad necesarios para proteger la nube, la ejecución tomará un mes previo al cierre del contrato.

2. ANEXO 2. RED LAN Y SERVICIOS ADMINISTRADOS

Contratar bajo la modalidad de servicio la implementación, renovación, administración, soporte y puesta en funcionamiento de la Solución de Red LAN del INMLCF, incluyendo Switching (Core y Acceso), capacidades de NAC/SDBranch integradas con SD-WAN, y solución Wireless (WLAN) con portal cautivo personalizado para la entidad, garantizando gestión centralizada, alta disponibilidad, segmentación y controles de seguridad.

Así mismo se hace necesario contratar con los servicios administrados, que apoyan labores especificas dentro del INMLCF.

2.1 Alcance técnico del servicio

El servicio deberá incluir como mínimo:

- Suministro en calidad de servicio, implementación, operación y soporte de dos (2) switches Core para el Datacenter de la sede principal del INMLCF, configurados en Alta Disponibilidad (HA).
- Suministro en calidad de servicio, implementación, operación y soporte de una solución SD-LAN (switches de acceso a nivel nacional) e integración con

capacidades de Control de Acceso a la Red (NAC) mediante integración nativa WAN+LAN con la tecnología SD-WAN.

ANEXO 2. LAN							
2.1 INVENTARIO SW A NIVEL NACIONAL VIGENCIA 2026							
Nº	REGIONAL	SEDE	DIRECCIÓN	SWITCH 24	SWITCH 24 POE mínimo de 370 W	SWITCH 48	SWITCH 48 POE mínimo de 740 W
1	SEDE PRINCIPAL	CENTRO DE COMPUTO	Calle 7A No. 12 A – 51	0	4	0	0
2		CENTRO DE COMPUTO		0	0	2	0
3		PISO 1		0	0	0	5
4		PISO 2		0	0	0	6
5		PISO 3		0	0	1	0
6		PISO 3		0	0	0	4
7		PISO 4		0	0	0	2
8		PISO 5		0	0	0	4
9		PISO 6		0	0	0	3
10		PISO 7		0	0	0	3
11		EDI SAF		0	0	0	4
12		EDI SANTA INES		0	0	0	4
13		ALMACEN	Troncal Carrera 10 # 1-59 Sur Edificio San Jorge.	0	0	0	1
14		EDI SAN MARTIN	Carrera 7A #32-16	0	0	0	11
15		VERAGUAS	Cra 35 # 4B-43 (Veraguas)	0	2	0	0
16	R.BOGOTA	U.B ATENCION AL MENOR	Calle 12 No 30-35 Piso 3	1	0	0	0
17		U.B ATENCION AL MENOR	Calle 12 No 30-35 Piso 3	0	1	0	0
18		PUENTE ARANDA	Carrera 40 No. 10 A - 08 (UPJ)	1	0	0	0
19		PUENTE ARANDA	Carrera 40 No. 10 A - 08 (UPJ)	0	1	0	0
20		KENNEDY	Carrera 69 No. 36-70 sur	0	2	0	0
21		GRANJA	CARRERA 78 A N° 77 A -62	0	2	0	0
22		CAPIV	Avenida 19 # 27-09, piso 2 "CAPIV"	1	0	0	0
23		CIUDADA BOLIVAR	Diagonal 62 Sur No. 20 F - 20. piso 2.	1	0	0	0

24	R. SUROCCIDENTE	CALI	Calle 4B No. 36-01	2	0	0	0
25		CALI	Calle 4B No. 36-01	0	9	0	0
26		CALI	Calle 4B No. 36-01	0	0	1	0
27		CALI	Calle 4B No. 36-01	0	0	0	1
28		POPAYAN	Av. 17 Sur No. 10-95	0	1	0	0
		URI BUNKER	Carrera 10 con calle 13 Fiscalía de Cali	0	1	0	0
29		TULUA	Carrera 25C No.48-101 Nuevo Príncipe	0	1	0	0
30	R ORIENTE	TUNJA	CALLE 24 No 5 A -61	0	1	0	2
31		VILLAVO	Carrera 6 No. 24A - 14 BARRIO MENEGUA	1	0	0	0
32				0	3	0	0
33				0	0	1	0
34				0	0	0	2
35		YOPAL	Marginal de la Selva Diagonal 9 No 13C-68 Barrio La Corocora	0	1	0	0
36		SOACHA	KR 6 No. 15-96 BARRIO SAN LUIS	0	0	0	1
37	R NOROCCIDENTE	MEDELLIN	Cra 65 Nro. 80-325	0	0	0	6
38				0	7	0	0
39				0	0	1	0
40		MONTERIA	Carrera 7 con Calle 10 Esquina Barrio Buena vista	0	0	0	1
41		QUIBDO	Calle 25 No. 6 - 08 Barrio Pan de Yuca	0	1	0	0

42	R NORORIENTE	BUCARAMAGA	CALLE 45 # 1-51 Campohermoso	1	0	0	0
43				0	4	0	0
				0	0	1	0
44				0	0	0	3
45				0	0	1	0
46		VALLEDUPAR	Carrera 16 # 13C - 15 ALFONSO LÓPEZ	1	0	0	0
47		VALLEDUPAR	Hospital Rosario Pumarejo de Lopez Calle 16 con Cra 17 - Morgue	1	0	0	0
48		ARAUCA	Carrera. 20 N°5-50 Barrio Fundadores	0	0	0	1
49	R OCCIDENTE	PEREIRA	Avenida Las Américas No. 98-25	1	0	0	0
50				0	7	0,00	0
51				0	0	0,00	2
			Av. las Américas sector Belmonte galpón 5 bodega 4	0	1	0,00	
52	R NORTE	BARRANQUILLA	Carrera 23 No. 53D - 56 Barrio Andes	0	0	1,00	0
53		BARRANQUILLA	Carrera 23 No. 53D - 56 Barrio Andes	0	0	0,00	10
54		CARTAGENA	Barrio Zaragocilla, al lado del Hospital Universitario de Cartagena (Calle 29 No. 50-210)	0	0	0,00	1
55		RIOHACHA	Calle 7No.15-45 Diagonal al Palacio de Justicia	0	1	0,00	0
56		MAICAO	Calle 9 No.11a -23 Barrio el boscan.	0	1	0,00	0
57		SANTA MARTA	Calle 26A No. 9-85	0	1	0,00	0
58		SANTA MARTA	Calle 26A No. 9-85	0	0	0,00	1
59		SINCELEJO	Calle 38 No.25A-211 Troncal de Occidente	0	1	0,00	0
60		SINCELEJO	Calle 38 No.25A-211 Troncal de Occidente	0	0	0,00	1

61	R SUR	NEIVA	Cra. 8 5-22, Centro	0	0	0,00	1
62		NEIVA	Carrera 5 sur No.17-65 Zona Industrial Sur	0	2	0,00	1
63		IBAGUE	Calle 45 No. 8 Sur-58, Zona Industrial El Papayo	0	2	0,00	0
64		IBAGUE	Calle 45 No. 8 Sur-58, Zona Industrial El Papayo	0	0	0,00	1
65		CHAPARRAL	Diagonal 8 No. 12 - 00 (Casa de Justicia)	0	1	0,00	0
67		FLORENCIA	Carrera 10 No. 5A - 28 Barrio Avenidas	0	1	0,00	0
	TOTAL			11	59	9	82

- Suministro en calidad de servicio, implementación, operación y soporte de WLAN con 50Access Points administrados por controladora y portal cautivo, sin adquisición de hardware por parte del INMLCF para la controladora/portal. La gestión y control de tráfico se realizará de manera centralizada mediante la integración nativa de los switches y Access Point con el equipo SD-WAN que hace parte de la solución de conectividad.
- Soporte 7x24x365 primer nivel, segundo nivel y escalamiento con fabricante, atención de incidentes, acompañamiento técnico especializado y entrega de reportes periódicos.
- Actividades de instalación y migración, así como ajuste de conectividad en rack, incluyendo migración de cableado existente hacia los nuevos equipos suministrados en servicio.

2.1.1 SWITCH CORE - RED LAN

Requerimientos de compatibilidad, integración y gestión

Unificación tecnológica (fabricante)

- Los equipos LAN (Core, acceso y WLAN) deben ser del mismo fabricante que la solución SD-WAN ofertada/implementada, para asegurar gestión centralizada, integración nativa de seguridad y operación unificada.

- La solución debe permitir monitoreo, control y administración integrados para mejorar operación, resolución de problemas y tiempos de respuesta ante incidentes.
- El proveedor deberá indicar la referencia, marca y fabricante de la solución ofertada.

2.1.2 Integración SD-WAN / SD-LAN / SDBranch

- La solución debe permitir convergencia con la red WAN, gestionando políticas como extensión de la SD-WAN.
- La administración de políticas de seguridad deberá realizarse desde el componente SD-WAN como parte de la solución ofertada.
- La solución debe permitir integración de políticas con la red Wi-Fi (misma marca/fabricante), ampliando el perímetro de seguridad.
- El proveedor deberá indicar la referencia, marca y fabricante de la solución ofertada.

- **Requerimientos técnicos – Switch Core (Datacenter sede principal)**
- **Cantidad y alta disponibilidad**

MARCA Y REFERENCIA	*CANTIDAD*
Switch Core de 48 puertos ópticos (incluye 48 Módulos SFP+ Corto Alcance (Longitud onda: 850nm, rango Transmisión: 300 metros y conector: Dúplex LC) y 48 Patch Cord de fibra de 3 metros, cada uno de los equipos.	*2*

- Se deberá suministrar e implementar dos (2) switches Core en el Datacenter de la sede principal, configurados en HA. Cada uno de estos dispositivos deberán contar con 48 puertos ópticos de 10 Gbps. Asi mismo, el oferente deberá suministrar los módulos SFP+ Multimodo y/o Monomodo para todos los puertos del Switch Core, según requiera la entidad.
- Arquitectura y seguridad
- Los switches Core deberán soportar separación de roles de distribución y agregación entre el Datacenter y la red campus, mejorando aislamiento entre tráfico de usuarios y servidores.
- Deberán habilitar controles avanzados, como mínimo: bloqueo de tráfico intra-VLAN, autenticación 802.1X y cuarentena de dispositivos (en coherencia con NAC).

- El diseño debe aportar a una postura de defensa en profundidad y reducción de riesgo de movimiento lateral.
- Redundancia y rendimiento
- Los switches Core deberán optimizar el ancho de banda mediante agregación de enlaces y minimizar dependencia de Spanning Tree, usando un protocolo de clusterización (o equivalente de la marca) para redundancia y resiliencia.

2.1.3 Interfaces ópticas y accesorios

- Se requiere que los dos switches Core dispongan de noventa y seis (96) módulos SFP+ (corto y largo alcance) para garantizar disponibilidad total de puertos ópticos.
- Referencia/Especificación incluida en el documento base: 2 Switchcon 48 módulos SFP+ corto alcance por equipo (850nm, 300m, conector dúplex LC) e incluye 48 patch cord de fibra de 3m por equipo.
- Se requiere 4 módulos SFP+ de largo alcance para uso en switches de acceso.
- El proveedor deberá suministrar todos los elementos en servicios, realizar la instalación de los servicios en las sedes indicadas por el instituto y realizar la operación del servicio por el tiempo del contrato del presente proceso.
- A continuación, se describen las consideraciones técnicas que debe soportar cada uno de los Switches Core:
    - ✓ Interfaces: 48 puertos 10G/1G SFP+/SFP y 6 puertos 40G QSFP+ o 4 puertos 100G/40G QSFP28/QSFP+ ports
    - ✓ Switching Capacity (Duplex): 1760 Gbps.
    - ✓ Packets Per Second (Duplex) 64 bytes: 1518 Mpps
    - ✓ Mac Address Storage: 144K
    - ✓ Network Latency: < 800 ns
    - ✓ VLANs Soportadas: 4K
    - ✓ Link Aggregation Group Size: 48
    - ✓ Queues/Port: 8

- ✓ Packet Buffers: 8
- ✓ Memory: 8 GB DDR3
- ✓ Flash: 128MB NOR
- ✓ Drive: 128GB SSD

La solución de SD-LAN se encuentra dimensionada para la implementación de un total de ciento sesenta y tres (163) switches a nivel nacional, de acuerdo con la distribución definida en el documento base del proceso contractual. Para este dimensionamiento inicial, se requieren los siguientes componentes:

- Cincuenta y nueve (59) switches de veinticuatro (24) puertos, con capacidad PoE, suministro mínimo de 370 W, donde la totalidad de los puertos deberá soportar los estándares IEEE 802.3af/at.
- Ochenta y dos (82) switches de cuarenta y ocho (48) puertos, con capacidad PoE, suministro mínimo de 740 W, donde la totalidad de los puertos deberá soportar los estándares IEEE 802.3af/at.
- Dos (2) Switch Core Fibra Para Datacenter De 48 Ptos en Fibra Capa 3.
- Once (11) switches de veinticuatro (24) puertos, sin capacidad PoE.
- Nueve (9) switches de cuarenta y ocho (48) puertos, sin capacidad PoE.

2.1.4 Integración NAC (Control de Acceso a la Red) – Funcionalidad mínima

La solución deberá permitir habilitar funcionalidades de NAC básicas de forma nativa entre los equipos SD-WAN y LAN (switches y AP) en las sedes que requiera el instituto, permitiendo:

- Visibilidad y control de dispositivos conectados con administración centralizada.
- Segmentación dinámica del tráfico.
- Aplicación de controles de acceso por perfil de usuario y tipo de dispositivo.
- Detección dinámica de dispositivos y asignación de VLAN.
- Definición de VLANs y políticas predeterminadas; definición de VLAN de destino y políticas asociadas.
- Que permita integración de las políticas con la red Wifi ofertada siendo del mismo fabricante la solución siendo parte de la infraestructura de seguridad y ampliando el perímetro.

2.1.5 Criterios mínimos de asignación automática de VLAN:

- Dirección MAC.
- Fabricante (vendor) de hardware.
- Sistema operativo.
- Usuario de Directorio Activo.
- Tag o etiquetas provistas por el servicio de ZTNA.

2.1.6 SFP / Uplinks y compatibilidad

- El proveedor debe incluir los SFP requeridos para uplinks en sedes con fibra óptica para todas las sedes de la Entidad donde opere SD-LAN, con referencias compatibles con especificaciones del fabricante y de la última serie.

2.1.7 Migración en rack y responsabilidades

- El proveedor deberá contemplar migración del cableado existente a los nuevos equipos a nivel de rack.
- El INMLCF se encargará de conexiones de energía y cableado requerido;
- Durante el proceso de implementación, el proveedor deberá proponer un cronograma de migración de switches, suministrando el servicio SDBranch del fabricante durante la ejecución del proyecto, cumpliendo características como lo es la organización de los racks de comunicaciones, el maquillado de los elementos a intervenir y distribución de puertos requeridos.
- Debe considerarse que los servicios deben estar implementados antes de 1 de agosto de 2026.

2.1.8 Reportes mensuales obligatorios

El proveedor deberá entregar **informes mensuales** dentro de los primeros **cuatro (4) días** del mes, que incluyan como mínimo:

- Resumen del estado de los Access Point.
- Reporte gerencial que resuma la utilización de los canales de WiFi.
- Reporte gerencial que resuma la cantidad de clientes conectados a la solución inalámbrica.
- Top 10 de APs por uso.
- Uso por SSID.
- Top de Aplicaciones, Sistemas Operativos, tipos de dispositivos y Clientes por uso en la red.
- **Detección de dispositivos**: reporte gerencial que resuma los dispositivos conectados a la red clasificados de la siguiente manera:
- Vendor o fabricante.
- Top 10 de Sistema Operativo
- Información del direccionamiento IP y MAC del dispositivo.

2.2 Requerimientos técnicos – Solución Wireless (WLAN) + Portal Cautivo

2.2.1 Alcance WLAN

- Se requiere instalación, soporte e implementación de **50 Access Points** en sede central y regionales del INMLCF.

ITEM	CUIDAD	REGIONAL	DIRECCIÓN	CANTIDAD
1	Bogotá (Entrada Clínica)	Bogotá	Calle 7a #12a-51	6
2	Bogotá (portería principal)	Bogotá	Calle 7a #12a-51	
3	Bogotá (6to piso)	Bogotá	Calle 7a #12a-51	
4	Bogotá (Sala dirección General)	Bogotá	Carrera 7A #32-16	
5	Bogotá (Auditorio)	Bogotá	Calle 7a #12a-51	
6	Bogotá (Antigua SAF)	Bogotá	Calle 7a #12a-51	
7	Bogotá (San Martin) }	Bogotá	Carrera 7A #32-16	4

8	Bogotá (San Martin)	Bogotá	Carrera 7A #32-16	
9	Bogotá (San Martin)	Bogotá	Carrera 7A #32-16	
11	Bogotá (Sala dirección General)	Bogotá	Carrera 7A #32-16	
12	UB. Kennedy	Bogotá	Carrera 69 No. 36-70 sur	1
13	UB. atención al menor	Bogotá	Calle 12 No 30-35 Piso 3	1
14	Medellín (clínica)	Noroccidente	Carrea 65 # 80-25 Barrio Caribe	4
15	Medellín (Identificación)	Noroccidente	Carrea 65 # 80-25 Barrio Caribe	
16	Medellín (Sala de espera Principal)	Noroccidente	Carrea 65 # 80-25 Barrio Caribe	
17	Medellín (auditorio)	Noroccidente	Carrea 65 # 80-25 Barrio Caribe	
18	Quibdó	Noroccidente	Calle 25 # 06-08 Br. Pan de Yuca (Antiguo DAS)	1
19	Montería	Noroccidente	Carrera 7ma Calle 10 Esquina Br. Buenavista	1
20	Bucaramanga	Nororiente	CALLE 45 # 1-51 Campohermoso	2
21	Bucaramanga (Auditorio)	Nororiente	CALLE 45 # 1-51 Campohermoso	
22	Valledupar	Nororiente	Hospital Rosario Pumarejo de López Calle 16 con Cra 17 - Morgue	1
23	Cúcuta	Nororiente	Calle 8A # 3-50 Edificio Santander -	1
24	Arauca	Nororiente	CARRERA 20 N° 5 - 50 BARRIO FUNDADORES	1
25	Barranquilla (patología)	Norte	Carrera 23 No. 53D - 56 Barrio Andes	3
26	Barranquilla (clínica)	Norte	Carrera 23 No. 53D - 56 Barrio Andes	
27	Barranquilla (auditorio)	Norte	Carrera 23 No. 53D - 56 Barrio Andes	
28	Cartagena	Norte	Calle 29 No 50-100 Barrio Zaragocilla Hospital Universitario del Caribe	1
29	Riohacha	Norte	Calle 7 No.15-45 Diagonal Palacio de Justicia	1
30	Santa Marta	Norte	Cale 26 A No.9-85	1
31	Sincelejo	Norte	Calle 38 No.25A-211 Troncal de Occidente	1

32	Pereira (clínica)	Occidente	Avenida Las Américas No. 98-25	3
33	Pereira (patología)	Occidente	Avenida Las Américas No. 98-25	
34	Pereira (Auditorio)	Occidente	Avenida Las Américas No. 98-25	
35	Manizales	Occidente	CARRERA 27 No. 48-85	1
36	Armenia	Occidente	Carrera 40A Calle 44 Esquina Barrio Villa Liliana.	1
37	Tunja	Oriente	CALLE 24 No 5 A -61	1
38	Villavicencio (clínica)	Oriente	Carrera 6 No. 24A - 14 BARRIO MENEGUA	2
39	Villavicencio (toma de muestras)	Oriente	Carrera 6 No. 24A - 14 BARRIO MENEGUA	
40	Yopal	Oriente	Marginal de la Selva Diagonal 9 No 13C- 68 Barrio La Corocora	1
41	Cali (clínica 1)	Suroccidente	CALLE 4B No. 36-01	4
42	Cali (clínica 2)	Suroccidente	CALLE 4B No. 36-01	
43	Cali (Servicios Complementarios)	Suroccidente	CALLE 4B No. 36-01	
44	Cali (Auditorio)	Suroccidente	CALLE 4B No. 36-01	
45	Pasto	Suroccidente	Calle 22 No. 7-93 Hospital Universitario Departamental de Nariño	1
46	Popayán	Suroccidente	Av. 17 Sur No. 10-95	1
47	Neiva	Sur	Calle 13 No. 5 - 140	1
48	Ibagué	Sur	Calle 45 No. 8 Sur-58, Zona Industrial El Papayo	1
49	Florencia	Sur	Carrera 10 No. 5A - 28 Barrio Avenidas	1
50	Mocoa	Sur	Calle 8 # 2 - 27 (Casa de Justicia) Barrio San Agustín	1
TOTAL				**50**

- La solución WLAN deberá ser parte integral del servicio e integrarse con la SD-WAN ofertada para desplegar políticas de seguridad centralizadas.

- El proveedor deberá entregar la Topología a implementar y documentación a alto nivel en un primer reporte y mantenerla actualizada si hay cambios estructurales en instalaciones.

2.2.2 Controladora y portal cautivo (sin hardware para INMLCF)

- Los Access Points deberán ser configurables mediante una controladora, la cual será el dispositivo SD-WAN.
- El proveedor proporcionará la controladora y el portal cautivo personalizado sin requerir adquisición de hardware por parte del INMLCF.
- Todos los elementos (APs y controladora) deberán ser del mismo fabricante de la solución SD-WAN ofertada.
- El proveedor debe desarrollar e implementar un portal cautivo personalizado que permita el acceso completo a la solución sin costo alguno para el INMLCF, debe terner como mínimo los sigiuentes aspectos a tener:
- El logo de la Entidad.
- Debe tener como mínimo 3 perfil.
- Se deben crear gpo de navegación.
- Se le deben sumunistrar a la entidad como mínimo 3 usuarios de gestión en el portal cautivo personalizado.
- El portal cautivo personalizado debe contar con una interfaz de usuario grafica.

2.2.3 Especificaciones mínimas de Access Points

Los AP deberán cumplir como mínimo:

- Wi-Fi 6E o superior.
- Tri-Radio: 2.4 GHz + 5 GHz + 5 GHz/6 GHz, con 4 antenas internas.
- 2x2 MU-MIMO.
- Velocidades: hasta 574 Mbps + 1201 Mbps + 2402 Mbps (según radios).
- Conectividad Bluetooth y capacidad de radio BLE con potencia de 10 dBm.
- Antena PIFA.
- Radios y capacidades de canal/modulación conforme a lo indicado (20/40/80/160, 1024 QAM, etc.).
- Máximo de clientes: 512 dispositivos por radio.
- BSSID: hasta 24 BSSID.

- Soporte de estándares mínimos listados (802.11a/b/d/e/g/h/i/j/k/n/r/u/v/w/ac/ax, 802.1Q, 802.1X, 802.3ad/af/at/az/bz).
- Seguridad: compatible con WPA2 y WPA3.

2.2.4 Alimentación y accesorios

- El AP debe admitir alimentación por PoE (sin requerir power injector). Si se requiere, el Power Injector deberá ser incluido por el proveedor sin costo para INMLCF.
- La solución debe incluir puertos necesarios y equipos homologados por el fabricante para la irradiación de la señal inalámbrica en Colombia.
- Si para instalación se requieren elementos (canaletas, cableado estructurado, puntos de red), estos deberán ser suministrados por el proveedor, incluyendo instalación en los sitios indicados por INMLCF y provisión de cables/puntos de red si aplica.
- Instalación de parches de seguridad y actualización proactiva de la plataforma en términos de seguridad, estará a cargo del proveedor.

2.2.5 SOPORTE

El proveedor deberá proporcionar una línea de atención 7x24x365 operativa las 24 horas del día, los 365 días del año, para la gestión de fallas y requerimientos relacionados con problemas, inconsistencias o cualquier situación que pueda afectar el funcionamiento normal de la solución de networking. Los casos de soporte podrán ser reportados mediante llamada telefónica a la mesa de ayuda o vía correo electrónico.

El soporte remoto será realizado exclusivamente por personal calificado, el cual debe contar con la experiencia y los conocimientos técnicos necesarios para respaldar la solución instalada. Este equipo de soporte asumirá la responsabilidad de llevar a cabo las actividades técnicas pertinentes según el nivel de especialidad y complejidad que requiera cada caso, garantizando respuestas oportunas y soluciones adecuadas a los problemas presentados.

En la propuesta económica presentada por el proveedor, se deberán contemplar todos los costos

asociados al servicio de soporte técnico, así como los aspectos relevantes que aseguren la correcta prestación de dicho servicio. Esto implica que no deben existir costos ocultos o adicionales que puedan afectar la continuidad y calidad del soporte ofrecido.

2.3 SERVICIOS ADMINISTRADOS

Se debe suministrar los servicios profesionales, para la administración, mejora, diagnostico, soporte y optimización de los componentes de la infraestructura tecnológica de la entidad las cuales serán utilizadas de acuerdo con las necesidades operativas del INML.

Para esto se requiere la prestación de los siguientes servicios:

- SERVICIO ESPECIALIZADO EN DBA
- SERVICIO ESPECIALIZADO EN SEGURIDAD DE LA INFORMACION Y CONTINUIDAD DEL NEGOCIO SERVICIO BÁSICO SOPORTE EN SITIO OFIMATICA (IMPRESIÓN)

2.3.1 COBERTURA DE LOS SERVICIOS

A continuación, se describe el alcance de la cobertura de los servicios relacionado con el horario de atención a soportar.

2.3.2 HORARIO DE ATENCIÓN

Servicio en Sitio Lunes a viernes 5x8 para todos los servicios

2.3.3 PERFILES DE LOS RECURSOS

2.3.3.1 SERVICIO AVANZADO BASES DE DATOS

Se requiere (1) recurso para el servicio de administración de bases de datos con conocimiento en diferentes motores de bases de datos, el cual apoyara la planificación y diseño de la infraestructura de datos de la organización a partir del desarrollo de procedimientos y estándares para la gestión y seguridad

de la información. Para esto se requiere que realice labores de administración, mantenimiento y custodia de las bases de datos incluyendo la definición y uso de las herramientas de software que defina para tal fin.

El servicio deberá tener la siguiente experiencia:

Experiencia mínima de 3 años especifica en la administración y gestión de bases de datos, habilidades de diseño, planificación implementación y administración de las plataformas relacionadas con las bases de datos en entornos físicos y virtualizados, habilidad de comunicación con equipos de desarrollo, habilidad para el manejo de usuarios.

El servicio deberá tener mínimo el siguiente nivel académico:

Profesional en Ingeniería de Sistemas, ciencias de la computación, o afines preferiblemente con certificación o estudios certificados por las empresas de software de motores de bases de datos.

2.3.3.2 SERVICIO BÁSICO SOPORTE EN SITIO OFIMATICA E IMPRESION

Se requieren (1) recurso para el servicio de soporte ofimático en sitio, el servicio deberá tener conocimientos técnicos en herramientas ofimáticas, sistemas operativos como Windows, IOS, Linux, impresoras, así como, amplios conocimientos en Office 2010 o superior, Mantenimiento de hardware y software, reposición de equipos. Deberá tener Vocación de servicio al cliente, comunicación asertiva, tolerante, buena redacción, con capacidad de trabajar en equipo.

A continuación, se describen algunas de las actividades del servicio

El servicio deberá tener la siguiente experiencia:

Experiencia mínima de dos (2) años en soporte de equipos de cómputo y sus accesorios, con mínimo un (1) año de experiencia en proceso de renovación de equipos de cómputo (Alistamiento, Toma de Backup, Instalación, configuración etc.). Deseables certificaciones ITIL V3 Fundamentos o superior

El servicio deberá tener mínimo el siguiente nivel académico:

Técnico, Tecnólogo en Ingeniería de sistemas, electrónica, telecomunicaciones, informática, telemática y afines.

2.3.3.3 SERVICIO ESPECIALIZADO EN SEGURIDAD DE LA INFORMACION Y CONTINUIDAD DEL NEGOCIO

Se requiere el servicio de seguridad de la información y continuidad del negocio, el cual adelantara labores de actualización del plan de recuperación de desastres para 10 sistemas de información o dispositivos.

Los servicios por desarrollar son:

- Análisis de riesgos de continuidad de negocio para un proceso.
- Análisis de impacto al negocio para un proceso.
- Plan de Recuperación de Desastres con los respectivos procedimientos de Failover y Fabilback para 10 sistemas de información.

Para estos servicios se debe considerar los aspectos de calidad del servicio, alta disponibilidad implementación de controles preventivos y correctivos para procurar la disponibilidad continúa de los sistemas críticos de la Organización.

2.4 SERVICIOS TRANSVERSALES A TODAS LAS SOLUCIONES

De manera transversal a la solución y sin costo adicional para la Entidad, el proveedor deberá disponer de los profesionales necesarios para el liderazgo del proyecto, entre ellos el Gerente de Proyecto de Implementación, el Gerente de Proyecto de Operación y los recursos especializados que se requieran. La provisión de dichos perfiles estará orientada al cumplimiento integral del alcance, los hitos contractuales y los Acuerdos de Niveles de Servicio (ANS), sin que se establezcan dedicaciones horarias mínimas ni esquemas rígidos de presencialidad. El proveedor será responsable de planear, coordinar y ejecutar las actividades de implementación y estabilización requeridas para garantizar que la solución se encuentre debidamente operativa. Los roles son los siguientes:”

2.4.1 GERENTE DE PROYECTO DURANTE LA FASE DE IMPLEMENTACIÓN

Se requiere contar durante toda la implementación de los servicios con un gerente de proyectos con experiencia en manejo de proyectos de telecomunicaciones. El gerente de proyectos es la persona encargada de la planeación y ejecución de la implementación de los servicios ofertados. Debe asistir a reuniones presenciales o virtuales de seguimiento semanal, quincenal o mensual de acuerdo con las necesidades del INMLFC, en las cuales se revisará la gestión de cronograma y planes de trabajo entre otros. Su dedicación podrá ser parcial al proyecto siempre y cuando garantice las actividades a realizar y el cumplimiento del cronograma de la ejecución de los servicios.

2.4.2 GERENTE DE PROYECTO PARA LA FASE DE OPERACIÓN DEL SERVICIO

El Gerente de Proyecto estará durante el tiempo total del contrato. Podrá ser de tiempo parcial sin embargo deberá contar con disponibilidad de tiempo y cuando sea requerido por el INML. deberá estar de manera presencial o virtual. Es la persona encargada de la parte operativa y el canal oficial entre las partes, durante toda la vigencia del contrato.

Perfil Profesional: Ingeniero de Sistemas, Electrónico, telecomunicaciones o carreras afines, con posgrado, especialización y/o maestría en Gerencia de Proyectos deseable certificación vigente de PMP del Project Management Institute y certificación ITIL Foundation nivel Intermedio v3 o superior vigente

Las actividades mínimas para desarrollar:

- Controlar la calidad del proyecto y monitoreo preventivo o proactivo con los recursos de la operación del proveedor.
- Convocar y asistir a las reuniones de seguimiento necesarias virtuales o presenciales según requerimiento del INML.
- Elaborar y firmar las actas de reuniones de seguimiento y entregables de cada etapa y mejoras tangibles de la operación.
- Elaboración de estrategias para impedir que una problemática o situación sea consecutiva bajo la misma incidencia.
- Velar por que se cumplan los objetivos contractuales, el alcance, el plan de trabajo que se requiere para el logro del objetivo del proyecto.

- Mantener el proyecto encaminado en sus objetivos y emitir las acciones correctivas, preventivas y de mejora para lograr el alcance del proyecto en el tiempo y costos definidos.
- Velar por que todo el equipo asignado por la empresa cumpla con la metodología de proyectos definida por la entidad.
- Identificar y realizar seguimiento a los riesgos identificados para el proyecto y proponer planes de acción para mitigar inconvenientes.
- Realizar el seguimiento y gestión de la ejecución durante todo el proyecto.
- Garantizar que todos los entregables cumplan con la calidad y criterios de aceptación definidos con la entidad o solicitados por el supervisor.
- Apoyar en los requerimientos, reuniones y entregables de la documentación a los diferentes entes de control o cualquier solicitud por parte de la entidad.
- Plantear alternativas de mejoramiento continuo de acuerdo con su experiencia y mejores prácticas o bajo solicitud del supervisor.

2.4.3 EL LÍDER TÉCNICO

Deberá estar asignado durante toda la vigencia del contrato, cumpliendo con una dedicación exclusiva a tiempo completo, de lunes a viernes, en el horario de 8:00 a.m. a 5:00 p.m. El INMLCF, requiere que sea la asistencia presencial en las instalaciones por la entidad.

- Rol general

Es el responsable de la operación técnica del proyecto y actuará como canal oficial de comunicación entre el contratista y el INMLCF durante toda la ejecución contractual, asegurando la adecuada coordinación técnica, la gestión de incidentes y el cumplimiento de los objetivos del proyecto.

- Funciones y responsabilidades

El Líder Técnico tendrá, como mínimo, las siguientes responsabilidades:

- Dar respuesta y atención oportuna a las consultas técnicas realizadas por el cliente.
- Asegurar la confidencialidad, integridad y disponibilidad de la información, en lo relacionado con las Tecnologías de la Información y las Comunicaciones.

- Apoyar la coordinación del proyecto ante incidentes de la operación de la infraestructura tecnológica, mediante la definición e implementación de un plan de respuesta a incidentes, que permita una atención eficaz y oportuna.
- Generar y mantener una base documental asociada a la resolución de incidentes y eventos operativos del proyecto.
- Preparar, administrar y controlar los planes de trabajo, cronogramas de tareas e identificación de prioridades técnicas.
- Coordinar las actividades técnicas del equipo de trabajo, garantizando la adecuada y oportuna implementación de los diferentes componentes del sistema.
- Asesorar al cliente en la implementación del componente de infraestructura tecnológica objeto del contrato.
- Proponer y validar metodologías de investigación que soporten la elaboración de documentos técnicos publicables, a partir de la información proveniente de los sistemas de información del cliente y de otros levantamientos necesarios.
- Elaborar, analizar y presentar los informes técnicos, documentación y reportes del proyecto, con el fin de evaluar su avance, desempeño y evolución.
- Establecer, implementar y mantener políticas de seguridad de la información, alineadas con las mejores prácticas y los lineamientos institucionales.
- Orientar y definir lineamientos técnicos al equipo de respuesta ante incidentes del proyecto.
- Planear y diseñar las actividades técnicas a ejecutar, asegurando la correcta implementación de los diferentes componentes del sistema.
- Verificar la calidad técnica de los entregables del proyecto y su conformidad con los requerimientos contractuales.
- Realizar monitoreo permanente de la infraestructura de red, identificando posibles fallas y gestionando su solución de manera eficaz y oportuna.
- Instalar, configurar y ajustar dispositivos de interconexión de redes, cuando así lo requiera la operación del proyecto.

Competencias clave esperadas

- Liderazgo técnico y capacidad de coordinación de equipos.
- Enfoque en continuidad del servicio y gestión de incidentes.
- Orientación a resultados, documentación y control.
- Alto sentido de responsabilidad, confidencialidad y ética profesional.

3. CIBERSEGURIDAD

Establecer los requerimientos técnicos mínimos y obligatorios para la implementación, operación, administración, soporte y monitoreo de las soluciones de ciberseguridad requeridas por el INMLCF, bajo esquemas de servicio administrado y/o servicio dedicado según se indica en el detalle de los servicios, de manera que contribuyan a mejorar la postura de seguridad de la entidad, el cual involucra la continuidad, disponibilidad, seguridad, trazabilidad y mejora continua de la postura de ciberseguridad institucional. También se considera procedente aclarar que los siguientes servicios: Conectividad Azure Ha, Servicio De Acceso De Red Segura, Servicio Waf As A Service, Rsoc Y Servicios De Protección, Rendimiento Y Seguridad Para Aplicaciones Web (Secure Access Service Edge), el tiempo de entrega es del 1 de diciembre de 2026.

3.1 CONDICIONES TRANSVERSALES A LOS SERVICIOS DE CIBERSEGURIDAD (aplican a todas las soluciones)

3.1.1 Modalidad y continuidad del servicio

- Los servicios que así se indiquen deberán operar en modalidad 24x7x365, con atención continua de incidentes, eventos, requerimientos y cambios, mediante un SOC (Centro de Operaciones de Seguridad).
- El proveedor deberá asegurar la continuidad operativa y la disponibilidad de las plataformas administradas/dedicadas durante toda la vigencia contractual.

3.1.2 Licenciamiento

- Todos los dispositivos/plataformas gestionadas deberán contar con licenciamiento legítimo, vigente y adecuado.
- La renovación y mantenimiento del licenciamiento requerido para la correcta prestación del servicio será responsabilidad exclusiva del proveedor, cuando aplique.

Seguridad, cumplimiento y acceso El proveedor deberá fortalecer la postura de seguridad de la información del INMLCF, mejorando los pilares de confidencialidad, integridad y disponibilidad mediante

la implementación de controles técnicos y operativos que aseguren el cumplimiento estricto de las políticas institucionales y los marcos de referencia de seguridad vigentes.

- EL Proveedor debe crear el acceso a los funcionarios del INMLCF a plataformas que hacen parte de los servicios, este deberá brindarse mediante usuarios definidos, preferiblemente con acceso solo lectura salvo autorización expresa.

Se deberán mantener registros auditables de acciones administrativas, accesos, cambios y consultas forenses, según corresponda a cada plataforma.

3.1.3 Documentación y reportes

- El proveedor deberá entregar reportes periódicos/mensuales (según aplique) de operación, incidentes/eventos atendidos, tendencias, alertas y recomendaciones de acuerdo con las soluciones ofertadas.
- El proveedor deberá entregar documentación técnica (arquitectura, topología de alto nivel, componentes, flujos de información) y, cuando aplique, diagramas y direccionamiento utilizado.

3.2 GESTIÓN Y SOPORTE DE PLATAFORMAS DE SEGURIDAD FORTINET PROPIEDAD DEL INSTITUTO

Establecer los requerimientos técnicos mínimos y obligatorios para la prestación del servicio de gestión, soporte y administración de las plataformas de seguridad Fortinet del Instituto Nacional de Medicina Legal y Ciencias Forenses (INMLCF), los cuales deberán ser incluidos en el pliego de condiciones del proceso de contratación. El servicio deberá ser suministrado bajo la modalidad de servicio administrado, fortaleciendo la continuidad, disponibilidad, seguridad y correcta operación de la infraestructura de seguridad perimetral de la Entidad.

3.2.1 Alcance del Servicio

El proveedor deberá asumir la gestión integral de la plataforma de seguridad Fortinet actualmente

instalada en el INMLCF, la cual incluye, como mínimo, los siguientes componentes:

- 2 FORTIGATE 1101E en esquema de HA
- 3 FORTIGATE 100F
- 4 FORTIFATE 80F

El alcance comprende la administración, monitoreo, soporte, mantenimiento, actualización, afinamiento y operación continua de dichas plataformas, de conformidad con las políticas de seguridad definidas por el INMLCF.

Todos los dispositivos y plataformas gestionadas deberán contar con **licenciamiento legítimo, vigente y adecuado**.

La renovación y mantenimiento del licenciamiento requerido para la correcta prestación del servicio será **responsabilidad exclusiva del proveedor**.

3.2.2 Modalidad y operación

El proveedor deberá prestar el servicio en modalidad **24x7x365**, de manera remota, con atención continua de incidentes, eventos de seguridad, requerimientos y cambios, a través de un Centro de Operaciones de Seguridad (SOC).

3.2.3 Requerimientos técnicos mínimos del servicio

El proveedor deberá garantizar, como mínimo, el cumplimiento de los siguientes requerimientos:

- **Administración y operación**
- Administración integral: reglas/políticas, perfiles de inspección, objetos, rutas, VPN y configuraciones asociadas.
- Gestión de incidentes y requerimientos por severidad.
- Gestión continua de cambios con **trazabilidad y control**.
- **Monitoreo y gestión de eventos**
- Monitoreo permanente de eventos, tráfico, disponibilidad y desempeño.
- Centralización/correlación de logs, con conservación y consulta de históricos.
- Consultas por IP, usuario y tráfico para auditoría y control.

- **Soporte y mantenimiento**

- Soporte especializado para fallas/incidentes/eventos **7x24x365**.
- Parches/firmware/hotfix recomendados por fabricante sin afectar la arquitectura existente.
- Afinamiento periódico: revisión de reglas inactivas/sobrepuestas/ineficientes, y activación de nuevas funcionalidades.
- **Gestión con fabricante**
- Gestión integral del soporte con Fortinet y trámite de **RMA** cuando aplique durante la vigencia del contrato.
- Trámite de RMA (Return Material Authorization) ante el fabricante en caso de fallas de hardware o requerimientos de reemplazo.
- Se requiere el suministro para la renovación y la administración del licenciamiento vigente, incluyendo la garantía y el soporte de los equipos que son propiedad de la Entidad.**3.1.4 Cumplimiento y capacidades del SOC del proveedor**

- El servicio deberá ser prestado por un SOC que cuente con certificaciones vigentes en **ISO/IEC 20000**, o estándares equivalentes.
- Se requiere que el SOC ofertado debe ser miembro del first.
- El proveedor deberá contar con certificación **MSSP (Managed Security Services Provider)** otorgada por el fabricante de los equipos que son de propiedad de la Entidad.
- Se deberá garantizar la confidencialidad, integridad y disponibilidad de la información del INMLCF, de acuerdo con las políticas de seguridad

3.2.4 Acceso, reportes y documentación

- Habilitar usuarios para consulta de configuraciones, políticas y reportes (solo lectura salvo autorización).
- Entrega de reportes de operación/incidentes/eventos y documentación técnica/diagramas e informes de afinamiento.

3.2.5 Reportes y Documentación

El proveedor deberá entregar, como mínimo:

- Reportes periódicos de operación, incidentes atendidos, eventos de seguridad y estado de la plataforma que hacen parte del servicio.
- Documentación técnica y diagramas de alto nivel de la solución gestionada.

- Informes de afinamiento y recomendaciones de mejora en seguridad.

3.2.6 Experiencia y Perfil del Proveedor

- Experiencia demostrable en la gestión y soporte de plataformas de seguridad de la marca de los equipos que son de propiedad de la Entidad, en entornos de misión crítica.
- Disponibilidad de personal técnico certificado por fabricante de la marca de los equipos de propiedad de la entidad y con experiencia en operación de SOC.

El incumplimiento de cualquiera de los requerimientos técnicos establecidos en el presente documento será causal de rechazo de la oferta. Todos los servicios deberán prestarse conforme a las políticas, lineamientos y necesidades del INMLCF, garantizando la continuidad operativa y el fortalecimiento de la postura de seguridad de la Entidad.

3.3 SERVICIO ADMINISTRADO ANTIDDOS (MITIGACIÓN VOLUMÉTRICA EN INTERNET)

3.3.1 Alcance del servicio

Mitigar ataques volumétricos DoS/DDoS originados desde Internet y garantizar disponibilidad del Internet del INMLCF (cuando los servicios estén en la nube del proveedor de conectividad).

- Operación permanente sobre los canales de Internet, **sin instalación de equipos en sedes**.

3.3.2 Topología requerida

El proveedor deberá realizar como mínimo:

- Presentar la topología de red a implementar integrando los equipos que son de propiedad del INMLCF.
- Inspección del tráfico entrante hacia bloques IP definidos por INMLCF.
- Desvío automático hacia infraestructura de mitigación ante detección.
- Integración con analítica de tráfico y centros de monitoreo de amenazas del proveedor.

- Depuración del tráfico legítimo y restitución del servicio durante ataques.

3.3.3 Técnicas mínimas de mitigación

- **Flow Inspect**: analítica Capa 3/4, detección de anomalías y clasificación legítimo/malicioso.
- **Fast Through**: desvío automático cuando el consumo sea **3x** el ancho de banda del canal ofertado por **1 minuto**; limpieza inmediata.
- **Feeds de inteligencia**: centro de monitoreo global con información de múltiples ISP, sensores botnets/darknet, campañas persistentes, fraude y ataques geopolíticos.

3.3.4 Condiciones de habilitación

- INMLCF entregará bloques IP públicos a proteger.
- Bloques deben ser de uso exclusivo, asignados por el proveedor o propiedad del INMLCF, y no ser /32.

3.3.5 Capacidad, estabilización, notificaciones y reportes

- Capacidad de mitigación: hasta **3x** el ancho de banda del canal ofertado (mejor esfuerzo si supera el umbral).
- Periodo de estabilización mínimo **1 mes** (learning/tuning), mitigación manual por SOC y luego mitigación automática.
- Notificación de alertas críticas altas y eventos de mitigación en curso; monitoreo continuo por SOC.
- Informes mensuales con tráfico inspeccionado, alertas, acciones SOC, mitigaciones, gestión de tickets; e informe de falla ante indisponibilidad por DDoS (a solicitud).

3.4 SERVICIOS DE MONITOREO DE SEGURIDAD MEDIANTE PLATAFORMA SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

Las Entidades del Estado, incluido el Instituto Nacional de Medicina Legal y Ciencias Forenses – INMLCF, no cuentan de manera permanente con la cantidad suficiente de especialistas ni con la capacidad operativa necesaria para atender, analizar e investigar de forma integral la totalidad de los eventos de seguridad generados por los dispositivos de infraestructura tecnológica y plataformas de seguridad, ni para determinar oportunamente la causa raíz de incidentes o ataques cibernéticos.

En este contexto, y con el fin de fortalecer la postura de ciberseguridad institucional, garantizar la detección temprana de amenazas y facilitar el análisis centralizado de eventos de seguridad, **el oferente deberá suministrar e implementar una solución de SIEM bajo la modalidad de servicio (SIEM as a Service)**, a través de la cual el INMLCF reciba notificaciones oportunas, alertas correlacionadas y visibilidad integral sobre los eventos de seguridad generados en su infraestructura tecnológica.

El servicio ofertado deberá contemplar, como mínimo, los siguientes componentes y capacidades técnicas obligatorias:

- **Plataforma SIEM como servicio**
  - Capacidad de recepción, normalización, almacenamiento y correlación de eventos de seguridad.
  - Integración con mínimo 32 servidores que se encuentra en la infraestructura local y Azure del INMLCF.
  - Procesamiento mínimo de 650 EPS, mediante sonda colectora en el Datacenter del proveedor.
  - Despliegue de 32 agentes avanzados para recolección de logs en servidores que se encuentran en la infraestructura local y en la nube de Azure del INMLFC.

- **Casos de uso de seguridad**

  - El proveedor debe contar con al menos 200 casos, de los cuales la Entidad requerirá que el proveedor desarrolle e implemente sesenta (60) **casos de uso base**. Estos casos serán definidos conjuntamente con el INMLCF durante la fase de despliegue e implementación del servicio.

- Los casos de uso estarán alineados con los eventos efectivamente colectados y con las necesidades de seguridad de la Entidad.
- En caso de que alguno de los casos de uso definidos no genere información relevante, el INMLCF podrá solicitar su modificación o sustitución por alguno de los 200 casos, sujeta a revisión y factibilidad técnica por parte del proveedor.

- **Fuentes de eventos mínimas**

- Los eventos colectados por la plataforma SIEM deberán cubrir, como mínimo, los dispositivos y plataformas de seguridad definidos en el capítulo **Gestión, Soporte y Mantenimiento de Plataformas de Seguridad de la marca ofertada**, así como los sistemas críticos de la Entidad.

- **Acceso y visibilidad para la Entidad**

- El servicio deberá contemplar el acceso a una **interfaz gráfica de administración y monitoreo**, que permita al INMLCF:

- Visualizar en tiempo real el comportamiento de sus equipos y sistemas.
- Consultar eventos, alertas y casos de seguridad.
- Gestionar y hacer seguimiento a los casos generados.
- Crear y exportar reportes personalizados de seguridad.

- **Agentes y recolección de logs**

- Despliegue de **treinta y dos (32) agentes avanzados** para la recolección de eventos de seguridad en servidores del INMLCF.

- El INMLCF será responsable de realizar las configuraciones internas necesarias para permitir el envío de logs y la instalación de los agentes en la solución de la Nube de Azure y en el data center local de Entidad, de acuerdo con las guías técnicas del fabricante.

- **Documentación técnica**

- El proveedor debe entregar de documentación completa de la solución implementada, incluyendo:

- Arquitectura de la solución.
- Topología de alto nivel.
- Componentes involucrados.
- Flujos de información y eventos.

3.4.1 Funcionalidades mínimas obligatorias de la plataforma SIEM

El proveedor debe presentar la solución ofertada deberá cumplir, como mínimo, con las siguientes funcionalidades técnicas, debidamente soportadas mediante documentación oficial del fabricante:

- Timestamp normalization; Log source virtualization; Scheduled collection.
- Transmisión comprimida y cifrada.
- Recolección: Windows Event Logs (local/remoto), Syslog UDP/TCP/seguro, NetFlow/IPFIX/J-Flow/sFlow, traps SNMP.
- Monitoreo endpoints: desempeño, integridad de archivos, actividad de usuarios, procesos y conexiones.
- Logs de BD remotas: SQL/MySQL/DB2/Oracle, ODBC v3.5 y OLE DB.

El proveedor debe presentar las funcionalidades deberán ser verificables mediante la matriz de compatibilidad del fabricante.

3.4.2 Arquitectura mínima

- Colectores de eventos, procesador de datos, motor de correlación e IA, administrador central.
- Servidor colector de datos en Datacenter del proveedor para recibir/almacenar/procesar eventos de infraestructura local y Azure.

3.4.3 Acceso y portal

- Interfaz gráfica para visualizar en tiempo real, consultar eventos/alertas/casos, seguimiento y reportes personalizados.
- El proveedor deberá habilitar un **portal de monitoreo** y en ella dos (2) usuarios de lectura en la plataforma ofertada que permita al INMLCF, lo siguiente:
  - Visualizar en tiempo real el estado de sus activos,
  - Gestionar los casos de seguridad generados
  - Elaborar reportes personalizados, asegurando una visibilidad integral de la gestión de seguridad de la información institucional.

3.4.4 Insumos a cargo del INMLCF

- Arquitectura de red y sistemas críticos actualizados; segmentos de red; matrices de comunicación (técnico-operativo, seguridad, responsable).

3.5 CENTRO DE OPERACIONES DE SEGURIDAD (SOC) COMO SERVICIO

El Instituto Nacional de Medicina Legal y Ciencias Forenses – INMLCF requiere la prestación de un **Centro de Operaciones de Seguridad (SOC) bajo la modalidad de servicio**, con el fin de garantizar el **monitoreo, análisis, gestión y respuesta oportuna a eventos e incidentes de seguridad** asociados a la infraestructura tecnológica y a los dispositivos de seguridad de la Entidad.

El servicio deberá suplir la falta de capacidades internas especializadas para la atención continua de eventos de seguridad, la investigación de incidentes y el análisis de causa raíz de posibles ataques o vulnerabilidades.

El SOC deberá ser provisto como un **servicio administrado (Managed Security Services)**, operado por personal especializado del proveedor, sin que ello implique la transferencia de responsabilidades de gobierno, control o toma de decisiones estratégicas por parte del INMLCF.

El proveedor deberá garantizar, como mínimo, los siguientes alcances:

3.5.1 Alcance

Monitoreo y Operación

- El proveedor debe suministrar la herramienta de Monitoreo ininterrumpido 24 horas al día, 7 días a la semana, 365 días al año de los dispositivos y plataformas de seguridad e infraestructura definidos por el INMLCF. A continuación, se describe los componentes de seguridad que hacer parte del alcance del servicio de SOC.
  - Firewall de Nueva Generación desplegados en Azure.
  - Servicio de protección de correo electrónico.
  - Servicio de Zero Trust Network Access.
- La herramienta suministrada por el proveedor en los que respecta la Correlación y análisis de eventos de seguridad con el fin de identificar incidentes reales, amenazas activas y comportamientos anómalos.

Gestión de Incidentes

- Atención, análisis y resolución remota **ilimitada de incidentes de seguridad**, conforme a los niveles de severidad definidos.
- Investigación técnica de incidentes para la identificación de la causa raíz.
- Escalamiento oportuno de incidentes críticos a los contactos definidos por el Grupo Nacional de Tecnologías de Información y Desarrollo – GNTID.

Notificación de Alertas

- Notificación inmediata de **alertas de alto riesgo** a la dirección de correo electrónico oficial definida por el INMLCF.
- Las notificaciones deberán incluir, como mínimo: descripción del evento, nivel de severidad, impacto potencial y recomendaciones iniciales.

3.5.2 Gestión Operativa y Técnica

Gestión de Cambios y Configuración

- Gestión continua de cambios y configuraciones de las plataformas de seguridad **24x7**, conforme a las políticas y autorizaciones del INMLCF.
- No se permitirán cambios de arquitectura sin autorización expresa de la Entidad.

3.5.3 Actualizaciones y Parches

- Instalación de parches de seguridad, hotfixes y actualizaciones proactivas relacionadas con la seguridad de las plataformas gestionadas.
- Las actualizaciones no deberán afectar la disponibilidad ni la arquitectura de los servicios existentes.

3.5.4 Buenas Prácticas de Seguridad

El proveedor deberá:

- Proporcionar recomendaciones de buenas prácticas de seguridad **cinco (5) días a la semana**, en horario de **08:00 a 17:00 horas**.
- Implementar, previa autorización del INMLCF, las buenas prácticas de seguridad acordadas dentro del mismo horario.

3.5.5 Reportes y Documentación

- Generación **automatizada de reportes mensuales** sobre las plataformas y dispositivos gestionados.
- Los reportes deberán incluir, como mínimo:
  - Eventos relevantes detectados.
  - Incidentes gestionados.
  - Tendencias de seguridad.
  - Recomendaciones técnicas.
- El proveedor deberá suministrar un **repositorio seguro** para el almacenamiento de los reportes, el cual deberá estar disponible para la Entidad cuando esta lo solicite.

3.5.6 Mesa de Servicios y Canales de Atención

- El proveedor deberá disponer de, al menos, los siguientes canales para la apertura y seguimiento de tickets:
  - Aplicación web.
  - Correo electrónico.
  - Línea telefónica.

Los tiempos de atención deberán ajustarse a los niveles de servicio definidos contractualmente.

- El servicio SOC ofertado deberá cubrir todos los dispositivos de seguridad definidos por el INMLCF para incidentes de impacto **moderado o menor**, sin costos adicionales para la Entidad.
- En los casos en que la solución dependa directamente del fabricante, los tiempos de resolución se ajustarán a los acuerdos vigentes con este.

- Cuando la resolución de un incidente requiera un RMA (Return Material Authorization), el proveedor deberá:
  - ✓ Gestionar el proceso ante el fabricante.

- ✓ Coordinar la importación de equipos o partes de reemplazo.
- ✓ Gestionar el retorno de los equipos o piezas defectuosas.

- El INMLCF proporcionará al proveedor acceso autorizado a la cuenta de licenciamiento del fabricante o el contacto oficial para la gestión del caso.

- Todos los dispositivos y plataformas gestionadas deberán contar con **licenciamiento legítimo, vigente y adecuado**.
- La renovación y mantenimiento del licenciamiento requerido para la correcta prestación del servicio será **responsabilidad exclusiva del proveedor**.

- La capacidad de corrección del servicio SOC se enfocará en **mitigar la vulnerabilidad y contener la anomalía detectada**, con el fin de prevenir impactos adicionales.

3.6 ZERO TRUST NETWORK ACCESS (ZTNA)

Como parte de la estrategia de Seguridad Digital de la entidad, se ha definido la implementación y operación de la tecnología de Acceso de Red de Confianza Cero (ZTNA - Zero Trust Network Access) como el estándar para el control de acceso de usuarios remotos a los activos de información institucionales. Bajo esta premisa, el proveedor deberá suministrar un servicio integral que permita la transición desde modelos de confianza implícita hacia un esquema de validación continua, donde el acceso a las aplicaciones y recursos críticos se conceda de manera granular y dinámica, basándose exclusivamente en la identidad del usuario y la postura de seguridad del dispositivo, garantizando así la protección de la infraestructura independientemente de la ubicación de red del colaborador. Este servicio deberá integrarse de forma nativa con la solución de SD-WAN y la solución de seguridad perimetral desplegada en Azure. A continuación, se describen el alcance esperado, junto con las especificaciones técnicas de la solución:

3.6.1 Modalidad y arquitectura

- Servicio ZTNA bajo modalidad **Cloud**, alojada **en la nube del fabricante**, sin infraestructura dedicada adicional por la Entidad.
- Integración nativa con seguridad perimetral existente; integración exclusiva con firewalls de sede principal del INMLCF como **Proxy de Acceso ZTNA**.
- Entrega de diagrama de arquitectura propuesta.

3.6.2 Licenciamiento y soporte

- Licenciamiento mínimo para **1.000 dispositivos** (workstations).
- Soporte de fábrica **7x24x365** durante toda la vigencia.
- Soporte técnico **FortiCare 24x7** (según políticas del fabricante).

3.6.3 Capacidades mínimas

- **Funcionalidades de Seguridad ZTNA**

La solución deberá incluir, como mínimo, las siguientes capacidades funcionales:

- **Control de Acceso y Confianza Cero**
  - Evaluación **continua y en tiempo real** de la identidad del usuario y la postura de seguridad del dispositivo antes y durante cada sesión de acceso.
  - Aplicación de **políticas de acceso dinámicas**, basadas en etiquetas de Zero Trust y contexto del endpoint.
  - Capacidad de **acceso granular por aplicación**, permitiendo definir políticas específicas por recurso.
  - Funcionamiento tanto para **usuarios remotos como usuarios en campus**, soportando entornos híbridos.

- **Agente de Endpoint Unificado**

- La solución deberá contar con un **agente de software unificado** para estaciones de trabajo y dispositivos finales.
- El agente deberá incluir, como mínimo, las siguientes funcionalidades:
  - Acceso Seguro ZTNA
  - Cliente VPN (SSL VPN e IPsec VPN)
  - Filtrado de contenido web
  - Análisis y gestión de vulnerabilidades
  - Telemetría del endpoint
  - Control de cumplimiento del dispositivo
- **Seguridad Avanzada de Endpoint**
- Control de dispositivos.
- Filtrado web por categorías, con acciones configurables (Bloquear, Advertir, Permitir, Monitorear).
- Gestión de vulnerabilidades con:
  - Escaneo programable.
  - Aplicación automática de parches virtuales.
  - Instalación automática de actualizaciones según criticidad.
  - Exclusiones configurables por aplicación o vulnerabilidad.
- Información en **tiempo real del estado de los dispositivos**.

- **Acceso Seguro sin VPN (Access Proxy)**
  - Proxy de acceso a aplicaciones web mediante **HTTPS**, sin necesidad de VPN tradicional.
  - Proxy de reenvío TCP (TFAP) para acceso seguro a aplicaciones no web.

- **Identidad, Autenticación y Postura**

- Integración con **Directorios Activos On-Premises o Cloud** de la Entidad.
- Soporte de autenticación mediante **LDAP y SAML**.
- Integración con **proveedores de identidad (IdP)** para autenticación multifactor (MFA).
- Integración con **Microsoft Entra ID** para autenticación y telemetría de dispositivos remotos.

- **Sistemas Operativos Soportados**

La solución ofertada deberá soportar, como mínimo, los siguientes sistemas operativos:

Windows 7+; Windows Server 2012+; macOS 11+; Ubuntu 18.04+; Debian 11+; RHEL 7.4+; CentOS Stream 7.4/8+; Fedora 36+; iOS 9+; Android 5+; Chrome OS (filtrado).

- **Soporte y Disponibilidad del Servicio**

Soporte técnico **FortiCare™ 24x7**, conforme a las políticas vigentes del fabricante.

Administración, Monitoreo y Reportes

- La solución ofertada debe tener contar con la Consola web centralizada para la administración del servicio.
- Los servicios administrados incluyen la gestión completa y monitoreo a las alertas de seguridad.
- El oferente debe realizar gestión completa y monitoreo del servicio **24x7**.
- Los reportes que hace parte de la oferta serán aquellos que sean consultados y descargados directamente desde la plataforma del servicio:
- Informe gerencial del acceso ZTNA (sobre la información que describa el acceso a la red de confianza cero (ZTNA) en la red de la entidad.
- Informe que resuma la instalación, sistemas operativos, dispositivos, versión del agente de ZTNA y resumen del cliente.
- Informe de las vulnerabilidades detectadas mediante los análisis del agente de ZTNA en toda la red.

3.7 SERVICIO DE PROTECCIÓN DE CORREO ELECTRÓNICO (MSSP EN NUBE DEL FABRICANTE)

El INMLCF buscar contratar un **servicio de protección de correo electrónico en modalidad de servicio (MSSP)**, orientado a fortalecer la confidencialidad, integridad y disponibilidad del servicio de correo electrónico institucional del INMLCF, mitigando riesgos asociados a **spam, phishing, malware conocido y avanzado, amenazas de día cero, suplantación de identidad (BEC) y fuga de información**.

- El servicio deberá ser suministrado **exclusivamente en modalidad de servicio**, por la duración total del contrato, incluyendo licenciamiento, operación, administración, soporte, mantenimiento y actualizaciones.
- El proveedor será responsable integral de la **administración, monitoreo y soporte** de la solución.
- La solución deberá permitir **crecimiento o disminución flexible** del número de buzones protegidos, bajo el modelo MSSP.

3.7.1 Usuarios y compatibilidad

- Protección de **2.890 buzones** de **Office 365**.
- Integración con AD on-prem/cloud; LDAP/SAML; IdP para MFA; integración con **Microsoft Entra ID** para autenticación y telemetría.
- **Arquitectura de la Solución**
- El servicio deberá estar **desplegado en la nube del fabricante** de la solución.
- **No se aceptan** soluciones On-Premise, nubes privadas ni soluciones desplegadas sobre Azure, AWS, Google Cloud, Oracle Cloud, VMware Cloud u otras similares.
- La infraestructura deberá garantizar **alta disponibilidad y escalabilidad**, sin impacto en la continuidad del servicio.
- Se debe presentar la Arquitectura de alto nivel de la solución a implementar.

3.7.2 Capacidades de Seguridad Obligatorias

La solución ofertada, deberá incluir como mínimo:

- **Antispam** con tasa de detección superior al **99 %**.
- **Antimalware avanzado** para amenazas conocidas y desconocidas.
- **Protección contra phishing** y ataques de suplantación de identidad (BEC).
- **Sandbox en nube integrado**, del mismo fabricante, para análisis de malware de día cero (no se aceptan sandbox independientes).
- **Prevención de fuga de información (DLP)**.
- Capacidad de **neutralizar o reconstruir** mensajes y archivos adjuntos maliciosos.
- **Reescritura y análisis dinámico de URLs** contenidas en los correos electrónicos.
- **Cifrado de correo electrónico basado en identidad**.

- **Inteligencia de Amenazas**
  - La solución deberá estar respaldada por un **laboratorio de investigación y desarrollo del fabricante**, con inteligencia de amenazas en tiempo real.
  - Actualizaciones automáticas y permanentes de firmas, motores y modelos de detección.

3.7.3 Monitoreo, Trazabilidad y Reportes

- Los servicios administrados incluyen la gestión completa y monitoreo del servicio.
- Los servicios administrados incluyen seguimiento 7x24 a las alertas de seguridad.
- El reporte incluido en el servicio será descargado directamente de la plataforma.
- Reporte que describe las estadísticas sobre el tamaño medio y total del correo, número de correos y conexiones, retrasos, políticas de IP, políticas de destinatarios y lista de accesos principales. Filtros de entrada para los principales dominios y usuarios que envían spam, clasificadores por hora y disposición, y temas principales.

- Informe del Top 10 clientes IP, remitentes, remitentes de virus, usuarios locales, destinatarios y destinatarios de virus.
- Resumen de la protección de correo por dominio.

3.7.4 Soporte y Operación

- Soporte técnico provisto por el proveedor bajo un esquema **7x24x365**.
- Atención de incidentes, fallas, cambios de configuración y afinamientos de la solución.
- El servicio deberá incluir **acuerdos de niveles de servicio (ANS)** alineados a la criticidad del correo electrónico institucional.

3.7.5 Obligaciones del Proveedor

- Incluir **todos los costos** asociados a licencias, operación, soporte, mantenimiento y actualizaciones durante la vigencia contractual.
- El proveedor debe presentar un **análisis de la arquitectura actual** del correo electrónico del INMLCF y aplicar mejores prácticas para la implementación.
- Fortalecer la **confidencialidad, integridad y disponibilidad** de la información institucional.
- El proveedor debe entregar un informe de alta gerencia posterior a la implementación detallando, el estado de la solución final.

- **Consideraciones Finales**

El INMLCF adquiere un **servicio integral de protección de correo electrónico**, por lo cual la responsabilidad sobre la operación, administración y continuidad de la solución recae exclusivamente en el proveedor durante toda la vigencia del contrato.

3.8 SERVICIO DE PROTECCIÓN DE RIESGOS DIGITALES

3.8.1 Modalidad y alcance

La Entidad requiere la contratación de un **Servicio Integral de Protección de Riesgos Digitales**, prestado bajo la modalidad de **servicio administrado (SaaS)**, orientado a la identificación, monitoreo, análisis y mitigación de amenazas externas que puedan afectar la confidencialidad, integridad, disponibilidad y reputación digital de la Entidad, garantizando la continuidad operativa y el fortalecimiento de sus capacidades de ciberseguridad.

- La solución deberá ser provista **100 % bajo modalidad SaaS**, sin requerir la instalación de hardware o infraestructura local para su operación.
- El servicio deberá incluir **gestión, monitoreo y soporte administrado** durante toda la vigencia contractual.

3.8.2 Capacidades mínimas

- **Gestión de Inteligencia de Amenazas**
- Provisión de una solución de **ciberinteligencia de amenazas en modalidad de servicio**, que permita visibilidad y gestión integral del riesgo digital de la Entidad.
- Capacidad de monitorear y gestionar **mínimo quinientos (500) activos** de la Entidad durante la vigencia del contrato.
- Recolección de inteligencia desde múltiples fuentes, incluyendo **Dark Web, fuentes abiertas (OSINT) e investigación técnica especializada**.
- Clasificación de la inteligencia con **calificación de confianza basada en estándares de la industria**, tales como el Admiralty System.
- Asociación de la inteligencia de amenazas al **marco MITRE ATT&CK**, permitiendo análisis estructurado de tácticas, técnicas y procedimientos (TTP).
- Actualización de la inteligencia en **tiempo real**, conforme se identifique nueva información o contexto relevante.
- **Monitoreo de Dark Web y Superficie de Ataque Externa**

- Monitoreo extensivo y continuo de la **Dark Web**, incluyendo foros privados, mercados clandestinos, salas de chat ocultas, redes P2P, botnets y plataformas de mensajería.
- Identificación de **filtraciones de información**, tales como credenciales, información personal (PII), datos financieros y archivos confidenciales.
- Capacidad de detección y análisis de **fugas de credenciales**, presentadas en líneas de tiempo claras y trazables.
- Supervisión de nuevas **vulnerabilidades y exploits** discutidos activamente en Dark Web y fuentes abiertas.
- **Protección de Marca y Phishing**
- Monitoreo de la Entidad como marca para la detección temprana de **campañas de phishing inminentes**.
- Identificación de **dominios similares o de apariencia engañosa**, incluyendo aquellos que utilicen logotipos o elementos visuales de la Entidad.
- Detección de sitios de phishing mediante el uso de **marcas de agua digitales**.
- Capacidad de **eliminación (takedown)** de contenido sospechoso, sitios web, perfiles o dominios maliciosos, incluyendo un número mínimo de acciones de takedown durante el contrato.
- **Gestión de Shadow IT y Exposición de Activos**
- Identificación y escaneo de **Shadow IT**, incluyendo puertos abiertos, dispositivos mal configurados y certificados SSL.
- Identificación de **activos expuestos en Internet**, cambios en la superficie de ataque, variaciones en puertos abiertos y certificados SSL vencidos o próximos a vencer.
- Capacidad de integración con **proveedores de nube pública** para la identificación y monitoreo de activos (por ejemplo, AWS, Azure u otros).
- Identificación de información sensible expuesta en **repositorios de código** y en buckets de almacenamiento en la nube.
- **Investigación y Análisis de Indicadores de Compromiso (IOC)**

- Funcionalidades para el análisis e investigación bajo demanda de **IOC**, tales como direcciones IP, dominios, hashes y CVE.
- Consulta de reputación, listas negras, ubicación geográfica, información de red y reportes históricos de inteligencia.
- **Monitoreo de Proveedores y Riesgo de Terceros**
- Evaluación del **riesgo de proveedores**, incluyendo superficie de ataque, menciones en la Dark Web, incidentes de ransomware, brechas de seguridad y distribución geográfica de activos.
- **Capacidades de Integración y Administración**
  - Administración del servicio a través de **portal web** y **API REST**.
  - Disponibilidad de toda la información mediante **API REST**, permitiendo su integración con capacidades de SecOps y otras plataformas de la Entidad.
  - Integración con plataformas de colaboración como **Microsoft Teams o Slack** para el envío de alertas y notificaciones.
  - Soporte para **acceso basado en roles**, alertas personalizadas y notificaciones críticas.

- **Monitoreo, Soporte e Informes**
  - El proveedor debe realizar el seguimiento y monitoreo de alertas de seguridad **7x24**.
  - Disponibilidad de **soporte técnico 24x7**, conforme a las políticas de soporte vigentes del fabricante o proveedor del servicio.
  - Generación de reportes ejecutivos y gerenciales, incluyendo:
- Reporte del total de amenazas identificadas y activos expuestos.
- Informe de filtraciones de credenciales detectadas en la Dark Web.
- Informe del nivel de riesgo y superficie de ataque de la Entidad.
- Reportes del Centro de Inteligencia del Adversario.
- Reporte de acciones de eliminación (takedown) ejecutadas y disponibles.

- **Activos Considerados en el Servicio**

La solución deberá contemplar como activos, entre otros:

- Sistemas Autónomos (ASN).
- Direcciones IP.
- Dominios.
- Certificados digitales.

3.9 CONSOLA DE GESTIÓN CENTRALIZADA DEDICADA Y DE USO EXCLUSIVO (SERVICIO DEDICADO, INSTANCIA EXCLUSIVA)

3.9.1 Objeto y arquitectura

El proponente deberá suministrar, implementar, poner en operación y soportar una **solución de gestión centralizada con integración nativa con los equipos de seguridad perimetral y SD-WAN**, bajo la modalidad de **servicio dedicado**, de uso **exclusivo para el INMLCF**, orientada a la administración integral de la infraestructura de seguridad perimetral, SD-WAN, red cableada e inalámbrica de la Entidad.

- **Modalidad de Prestación y Arquitectura**
- La solución deberá ser suministrada como una **instancia dedicada, aislada y exclusiva**, garantizando la confidencialidad, integridad y autonomía administrativa de las políticas de seguridad de la Entidad.

- El servicio deberá operar sobre una **máquina virtual (VM)** desplegada en **nube pública o privada**, cumpliendo con los estándares de seguridad informática definidos por la Entidad.
- No se aceptarán soluciones compartidas, multi-tenant o que no aseguren segregación lógica y administrativa total.

3.9.2 Capacidad mínima y escalabilidad

- La solución deberá soportar **como mínimo doscientos (200) dispositivos o Virtual Domains (VDOMs)** de forma simultánea.
- El proveedor deberá garantizar la **escalabilidad ilimitada de recursos**:
- Sin restricciones en número de vCPU.
- Sin limitaciones en expansión de memoria RAM.
- Capacidad de crecimiento dinámico acorde con la expansión institucional.
- El proveedor será responsable de suministrar y dimensionar los recursos de cómputo necesarios para garantizar el rendimiento óptimo y funcionamiento de la plataforma.

3.9.3 Responsabilidades del Proveedor

- El proveedor será responsable, como mínimo, de:
- Implementación, puesta en marcha y configuración inicial de la plataforma.
- Costos del licenciamiento completo del servicio durante la vigencia contractual, junto con los recursos de cómputo necesarios y la conectividad para acceder al servicio.
- Administración y **soporte técnico nivel 1, 2 y 3**, bajo un esquema de **coadministración con la Entidad**.
- Garantizar la continuidad operativa y disponibilidad del servicio.

- **Compatibilidad Tecnológica Obligatoria**

- La solución ofertada deberá ser **totalmente compatible** con los siguientes entornos de virtualización y nube:

- VMware ESXi 5.5 y 6.0
- Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2
- Citrix XenServer 6.0+
- Open Source Xen 4.1+
- KVM
- Amazon Web Services (AWS)
- No se aceptarán propuestas que limiten la interoperabilidad tecnológica definida por la Entidad.

3.9.4 Accesos, Administración y Seguridad

- La plataforma deberá soportar acceso administrativo por:
- Interfaz web segura (HTTPS)
- SSH
- Cliente de gestión
- API abierta
- Deberá permitir **accesos concurrentes de múltiples administradores**, con mecanismos de **bloqueo de cambios** ante accesos simultáneos.
- Se deberán definir **perfiles de acceso granulares**, incluyendo:
- Lectura
- Escritura
- Creación de usuarios
- Modificación de configuraciones
- Todas las acciones de los usuarios deberán quedar **registradas y auditables**.

3.9.5 Autenticación y Control de Acceso

- La solución deberá permitir autenticación administrativa mediante:

- Cuentas locales
- TACACS
- LDAP
- RADIUS
- Certificados digitales X.509 (PKI)
- Asimismo, deberá soportar sincronización horaria mediante **NTP** y administración segura de interfaces de red con control de servicios (HTTP, HTTPS, SSH, SNMP, Telnet).

3.9.6 Gestión, Monitoreo y Alertamiento

- Generación automática de alertas por:
- Correo electrónico
- SNMP (v2 y v3)
- Syslog
- Capacidad de búsqueda avanzada de comandos en CLI.
- Soporte completo para **XML API y JSON API**.

- **3.8.7. Respaldo y Recuperación**

- La solución deberá soportar **backup y restore completo** de la configuración.
- Deberá permitir la **programación automática de respaldos**.
- Los respaldos deberán poder transferirse a:
- FTP
- SCP
- SFTP

3.9.7 Gestión Centralizada de Seguridad (NGFW / UTM)

- La plataforma deberá permitir, de forma centralizada:
- Gestión de políticas de firewall, aplicaciones, IPS, Antivirus, Anti-Spyware y Filtro URL.
- Validación de reglas (detección de shadowing).
- Comparación de configuraciones actuales y versiones históricas.
- Rollback de configuraciones.
- Creación de flujos de aprobación de cambios.
- Distribución remota de firmware y licencias.
- Gestión centralizada de NAT64, NAT46 y políticas Anti-DoS.
- Orquestación de VPNs (hub, spoke, dial-up), incluyendo autenticación y criptografía.
- Creación y ejecución centralizada de scripts CLI con historial auditable.

3.9.8 Gestión Unificada de Red

- La solución deberá actuar como un **centro de control unificado**, permitiendo:
- Gestión de switches y access points.
- Aprovisionamiento Zero-Touch.
- Configuración de VLANs, puertos y radiofrecuencia.
- Aplicación de políticas de seguridad consistentes desde el núcleo hasta el borde de la red.

3.9.9 Inteligencia Artificial y Automatización Avanzada

- La solución deberá integrar un **asistente de IA generativa**, con licenciamiento incluido, que permita:
- Creación automatizada de scripts (CLI/Jinja).
- Orquestación de topologías VPN.
- Análisis predictivo de vulnerabilidades, incluyendo dispositivos IoT.

- Ejecución de acciones de mitigación inmediata sobre la infraestructura gestionada.

3.9.10 Soporte y acceso

El proveedor será responsable, como mínimo, de:

- Suministrar a la entidad la topología de la solución propuesta a implementar en la plataforma tecnológica del INMLCF.
- Implementación, puesta en marcha y configuración inicial de la plataforma.
- Licenciamiento completo del servicio durante la vigencia contractual.
- Administración y **soporte técnico nivel 1, 2 y 3**, bajo un esquema de **coadministración con la Entidad**.
- Soporte técnico especializado para la atención de fallas, incidentes y eventos de seguridad 7x24x365;
- El proveedor debe crear como mínimo **3 usuarios** para INMLCF;
- Aplicación de parches de seguridad, actualizaciones de firmware y hotfixes recomendados por el fabricante, sin afectar la arquitectura existente.
- Transferencia de conocimiento y acompañamiento;
- Documentación con diagramas y direccionamiento usado; entrega de informes mensuales.

Reportes y Documentación

- El proveedor deberá entregar, como mínimo:
- Debe ser capaz de generar reportes o presentar comparativos entre dos secciones distintas, resumiendo todos los cambios efectuados.

- Debe permitir crear flujos de aprobación en la solución de gestión, donde un administrador pueda crear todas las reglas, pero estas mismas solamente sean aplicadas después de la aprobación de otro administrador.
- Reportes periódicos de operación, incidentes atendidos, eventos de seguridad y estado de la plataforma.
- Documentación técnica y diagramas de alto nivel de la solución gestionada.
- Informes de afinamiento y recomendaciones de mejora en seguridad.

3.10 CONSOLA DE ANALITICA Y TELEMETRÍA CENTRALIZADA DE USO DEDICADO Y EXCLUSIVO PARA LA ENTIDAD

3.10.1 Modalidad y alta disponibilidad

La Entidad requiere contratar un **servicio dedicado de analítica, telemetría y gestión centralizada de logs**, suministrado bajo modalidad de servicio, de uso **exclusivo para el INMLCF**, desplegado en una **instancia aislada en nube privada o pública**, fortaleciendo la confidencialidad, integridad, disponibilidad y autonomía de la información.

- **Alcance Técnico Mínimo**
  - Suministro, implementación, puesta en marcha, licenciamiento, administración y soporte integral (Niveles 1, 2 y 3) bajo un modelo de **coadministración con la Entidad**.
  - Implementación de **dos (2) instancias virtuales en Alta Disponibilidad**, cada una con capacidad mínima de **100 GB diarios de ingesta de logs**.
  - Integración nativa con el ecosistema de seguridad y conectividad SD-WAN del INMLCF (NGFW, SD-WAN, Switches, AP, ZTNA, correo electrónico, servicios de Azure y dispositivos de terceros).

3.10.2 Capacidades mínimas

- **Gestión y Almacenamiento de Logs**
  - Recepción, normalización, indexación y almacenamiento seguro de logs.
  - Compatibilidad con **IPv4/IPv6**, formatos **Syslog, CEF, LEEF y JSON**.
  - **Cifrado de datos en tránsito y en reposo**.
  - Políticas de **retención configurables por tipo de log y dispositivo**.
  - Capacidad mínima: **100 GB de logs diarios** y **10 TB de almacenamiento**, con retención en línea no inferior a **60 días**.
- **Arquitectura, Disponibilidad y Escalabilidad**
  - Arquitectura escalable con roles de **colector y analizador**.
  - Soporte de **Alta Disponibilidad**, fail-over automático y clústeres activos-activo o activo-pasivo.
  - Actualizaciones de software sin interrupción mediante **rolling upgrade**.

- **Seguridad, Control y Gobierno**
  - Definición de **dominios administrativos (ADOM)** y múltiples roles de administración.
  - Autenticación robusta con **MFA**, integración con **LDAP/Active Directory o RADIUS**.
  - Auditoría completa de accesos, cambios administrativos y consultas forenses.
  - Integración con **SNMP**, API REST y servicios externos de inteligencia de amenazas.
  - Debe 100% compatible con SAML.

- **Análisis, Correlación e Investigación Forense**
  - Motor de **correlación de eventos** con reglas predefinidas y personalizadas.
  - Búsqueda forense avanzada por usuario, IP, dispositivo y atributos múltiples.
  - Detección de **Indicadores de Compromiso (IoC)**, brotes de amenazas y comportamientos anómalos.

- Visualización de cadenas de eventos y líneas de tiempo para análisis causa-efecto.

- **Gestión de Incidentes y Operación SOC**
- Creación automática de incidentes a partir de eventos correlacionados.
- Clasificación por severidad, priorización, asignación de responsables y gestión de SLA.
- Integración con plataformas de **ticketing** (Jira, ServiceDesk, Zendesk u otras).
- Soporte para marcos **MITRE ATT&CK, NIST e ISO 27001**.

- **Reportes, Dashboards y Cumplimiento**
- Dashboards personalizables en tiempo real con indicadores KPI.
- Generación y programación de reportes automáticos en **PDF, HTML, CSV, XML**.
- Plantillas de cumplimiento para **PCI DSS, NIST CSF, NIST 800-53, IEC 62443**, entre otros.
- Exportación de información a plataformas de **Business Intelligence**.

Inteligencia Artificial y Automatización

- Asistente de **IA generativa** integrado para análisis conversacional, triage y respuesta a incidentes.
- Capacidades de **machine learning**, detección de anomalías y priorización basada en riesgo.
- Automatización SOC mediante **playbooks**, con acciones de contención y respuesta.
- Gestión y visualización del consumo de tokens de IA y control por usuario.

- **Integración Security Fabric**
- Compartición de telemetría e IoC entre todos los componentes del **Security Fabric**.
- Correlación unificada de eventos entre firewall, endpoints, correo electrónico, red y nube.
- Bloqueo automático de amenazas y orquestación de respuestas.

- **Soporte, Operación y Cumplimiento**
- El proveedor será responsable, como mínimo, de:
-
- Suministrar a la entidad la topología de la solución propuesta a implementar en la plataforma tecnológica del INMLCF.
- Implementación, puesta en marcha y configuración inicial de la plataforma.
- Costos del licenciamiento completo del servicio durante la vigencia contractual, junto con los recursos de cómputo y conectividad para acceder al servicio.
- Administración y **soporte técnico nivel 1, 2 y 3**, bajo un esquema de **coadministración con la Entidad**.
- Soporte técnico especializado para la atención de fallas, incidentes y eventos de seguridad 7x24x365;
- El proveedor debe crear como mínimo **3 usuarios** para INMLCF;
- Aplicación de parches de seguridad, actualizaciones de firmware y hotfixes recomendados por el fabricante, sin afectar la arquitectura existente.
- Transferencia de conocimiento y acompañamiento;
- Documentación con diagramas y direccionamiento usado; entrega de informes mensuales.

- **Reportes y Documentación**

- El proveedor deberá entregar, como mínimo:
- Reportes periódicos de operación, incidentes atendidos, eventos de seguridad y estado de la plataforma.
- Documentación técnica y diagramas de alto nivel de la solución gestionada.
- Informes de afinamiento y recomendaciones de mejora en seguridad.

3.11 SERVICIO DE GESTIÓN DE IDENTIDAD Y ACCESO DEDICADO Y USO EXCLUSIVO PARA LA ENTIDAD

La Entidad requiere la implementación de un **servicio dedicado de gestión de identidad y autenticación robusta**, basado en la Gestión de Identidad y Acceso Dedicado y Uso exclusivo para la Entidad, el suministrado bajo la modalidad **como servicio**, garantizando **uso exclusivo**, **instancias aisladas** y **alta disponibilidad**, integradas de manera nativa con la arquitectura de seguridad y conectividad SD-WAN institucional.

3.11.1 Modalidad del servicio

- El servicio deberá ser provisto **bajo un esquema de nube privada**, con instancias virtuales dedicadas y exclusivas para la Entidad.
- El proveedor será responsable del **suministro, licenciamiento, implementación, administración, operación y soporte** del servicio durante toda la vigencia contractual.
- El modelo de operación será de **coadministración** entre el proveedor y los funcionarios designados por la Entidad.

3.11.2 Arquitectura y alta disponibilidad

- Implementación **de dos (2) instancias redundantes** de servicio **dedicado de gestión de identidad y autenticación robusta** en esquema de **Alta Disponibilidad**, soportando modos **activo-activo y/o activo-pasivo**.
- Sincronización automática de configuración entre las instancias.
- Infraestructura hiperconvergente suministrada por el proveedor, incluyendo **vCPU, memoria RAM y almacenamiento**, así como todos los componentes de software necesarios y conectividad para la correcta operación y acceso al servicio.

3.11.3 Capacidad y escalabilidad

- El servicio deberá soportar **mínimo cinco mil (5.000) usuarios activos**.
- El licenciamiento deberá ser **perpetuo e ilimitado en transferencia de dispositivos**, permitiendo la reutilización de tokens ante altas y bajas de usuarios.
- Capacidad de crecimiento incremental sin requerir cambios de hardware o licenciamiento adicional.

3.11.4 Integraciones obligatorias

- Integración nativa con:
  - Soluciones **SD-WAN** y **Zero Trust Network Access (ZTNA)** de la Entidad.
  - **Next Generation Firewall** institucional.
  - **Microsoft Entra ID** mediante **SAML** para Single Sign-On (SSO).
- Compatibilidad total con **VPN IPSec y SSL** existentes.
- Soporte como **servidor RADIUS, LDAP y SAML IdP**.

3.11.5 Autenticación y control de acceso

- En caso de ser requerido por la entidad, la solución deberá soportar la **autenticación multifactor (MFA)** con:
  - Tokens móviles y físicos.
  - OTP basados en tiempo y eventos (OATH).
  - Push de aceptación y mensajería.
- Soporte de **Single Sign-On (SSO)** para aplicaciones, estaciones Windows y portales institucionales.
- Integración nativa con **802.1X**, autenticación por **MAC address** y soporte de métodos **EAP (PEAP, EAP-TLS, EAP-TTLS, EAP-GTC)**.

- Políticas de complejidad de contraseñas, bloqueo automático por intentos fallidos y protección contra ataques de fuerza bruta.

3.11.6 Gestión de usuarios y autoservicio

- Administración centralizada de usuarios locales, de Directorio Activo, invitados y contratistas.
- Portal de **autoservicio accesible por Internet** para:
  - Restablecimiento seguro de contraseñas.
  - Registro y gestión de tokens.
  - Autoregistro de usuarios con aprobación administrativa.
- Provisión de **certificado SSL vigente** para la publicación segura del portal.

3.11.7 Autoridad certificadora

- El servicio deberá actuar como **Autoridad Certificadora (CA)**, permitiendo:
  - Emisión, administración y revocación de certificados digitales.
  - Gestión de certificados X.509.
  - Soporte de **OCSP, CRL y SCEP**.
  - Integración con CAs externas confiables.

Funcionalidades del Single Sign On:

- La solución proporcionará la capacidad de servicio SSO (Single Sign-On), con autenticación de usuario transparente (pasiva) en sistemas compatibles.
- La solución tendrá la capacidad de integrarse a un directorio activo (Windows AD) y poder ofrecer funcionalidad de SSO (Single Sign On), donde se utilizarán las mismas credenciales que un usuario utiliza para autenticarse en el dominio desde su estación de trabajo.

- La solución permitirá definir una lista de usuarios de SSO que serán excluidos, evitando así las interferencias de políticas de servicios como antivirus o secuencias de comandos a través de GPO.
- Admitirá el análisis de archivos syslog enviados desde una fuente remota, para uso del servicio SSO.
- Soportará el lenguaje de marcado de aserción de seguridad (SAML), actuando como un proveedor de identidad (IDP) que establece una relación de confianza para la autenticación segura de los usuarios que intentan acceder a un proveedor de servicios (SP).
- Soportará SSO basado en RADIUS (RSSO - RADIUS Single Sign On).

3.11.8 Administración, monitoreo y auditoría

- Interfaces de administración **GUI y CLI**, accesibles vías navegador sin software adicional.
- Gestión de perfiles de administración con segregación de funciones.
- Registro y auditoría de eventos de autenticación, cambios de configuración y gestión de usuarios.
- Envío de logs e integración con el **correlacionador de eventos** de la Entidad mediante **SNMP v2/v3 y syslog**.

3.11.9 Respaldo y continuidad

- Copias de seguridad completas y cifradas de la configuración y bases de datos.
- Programación de respaldos automáticos con almacenamiento en servidores externos mediante **FTP o SFTP**.
- Restauración integral desde la interfaz de administración.

3.11.10 Compatibilidad de plataformas

- Soporte para sistemas operativos:
  - **Windows 10 o superior**.
  - **Android**.

- **iOS (iPhone, iPad, iPod Touch)**.

3.11.11 Servicios de implementación y soporte

- El proveedor deberá incluir:
- Servicios de implementación: planeación, instalación/configuración, actualización a última versión estable, pruebas funcionales/integración, acompañamiento, entrega a satisfacción y soporte 7x24 N1/N2/N3.
- Backups completos cifrados, programación automática y almacenamiento externo FTP/SFTP;
- Soporte para Windows 10+, Android e iOS.
- Instalación, configuración y actualización a la última versión estable del fabricante.
- Pruebas funcionales y de integración.
- Acompañamiento y asesoría para la integración con el servicio de ZTNA, SD-WAN y Next Generation Firewall de la Entidad para el despliegue de Single Sign-On.
- Licenciamiento completo del servicio durante la vigencia contractual.
- Garantizar la continuidad operativa y disponibilidad del servicio.
- Documentación técnica y diagramas de alto nivel de la solución una vez finalizada la implementación.
- Informes de afinamiento y recomendaciones de mejora en seguridad.
- Transferencia de conocimiento y acompañamiento;
- Entrega del servicio a satisfacción de la Entidad.

- **Soporte y acceso**

- Soporte técnico especializado para la atención de fallas, incidentes y eventos de seguridad 7x24x365;

- Administración y **soporte técnico nivel 1, 2 y 3**, bajo un esquema de **coadministración con la Entidad**.
- El proveedor debe crear como mínimo **3 usuarios** de lectura para INMLCF.
- Aplicación de parches de seguridad, actualizaciones de firmware y hotfixes recomendados por el fabricante, sin afectar la arquitectura existente.

- **Reportes y Documentación**

- El proveedor deberá entregar, como mínimo:
- Reportes periódicos de operación, incidentes atendidos, eventos de seguridad y estado de la plataforma.
- Documentación técnica y diagramas de alto nivel de la solución gestionada.
- Informes de afinamiento y recomendaciones de mejora en seguridad.

3.12 SERVICIO DE SECURE ACCESS SERVICE EDGE (SASE)

Como parte de la Estrategia de Seguridad Digital de la Entidad, se ha determinado la contratación de un servicio de SASE (Secure Access Service Edge) en modalidad de servicio que garantice una convergencia plena entre las funciones de seguridad y conectividad, el cual deberá ofrecer una integración nativa con los servicios de SD-WAN desplegados tanto en las sedes físicas como en la arquitectura de nube en Azure, permitiendo que las políticas de seguridad, el enrutamiento inteligente y la visibilidad del tráfico se gestionen de forma unificada desde una consola única, optimizando la experiencia del usuario y asegurando una postura de defensa consistente en todo el ecosistema híbrido; para lo cual se deberán cumplir los siguientes puntos:

3.12.1 Alcance

- La Entidad requiere la implementación, puesta en marcha, afinamiento, operación, soporte y monitoreo de una solución SASE **para 1000 usuarios** con integración nativa a los equipos que hacen parte del alcance SD-WAN y la seguridad perimetral de la entidad.
- La solución de SASE debe proporcionar a la entidad un conjunto de protecciones extendiendo el perimetro corporativo para asegurar los datos desde y hacia los equipos finales y usuarios, y habilita el acceso a Internet, a aplicaciones privadas y a aplicaciones en SaaS.

3.12.2 Generalidades

- La solución SASE debe proveer Datacenter que pueden ser del Fabricante o en instalaciones de nubes públicas.
- La solución SASE debe soportar servicios al cliente en un formato de 24x7
- La solución debe proveer un servicio de asistencia para la instalación y puesta a punto.
- La solución debe estar en capacidad de aumentar en mínimo cuatro (4) dirección IP publicas adicionales a las contratadas en cualquier momento.
- La solución SASE debe proveer la funcionalidad de resolver dominios privados internos mediante el DNS interno de la Compañía
- El punto de acceso SASE debe proporcionar todas las funciones de seguridad solicitadas. No se aceptan puntos de acceso donde se tenga servicios parciales.
- La solución debe proveer encripcion en tuneles IPSEC y con valores de ancho de banda superior a 300 Mbps sin pérdida de paquetes.
- Todas las funcionalidades (AV, CASB. DLP, Ant-malware, SGW, SDWAN) deben ser del mismo fabricante para permitir una óptima integración y eliminar posibles puntos de riesgo
- La solución debe estar en capacidad de aumentar los PoPs del fabricante o de la nube publica de conexión hasta en 16 sitios adicionales.
- La solución de SASE debe incluir inspección de antivirus, IPS, Filtrado WEB, Filtrado Botnet y C&C, Inspeccion SSL, Inline CASB e inline DLP, Acceso seguro privado (NPA, SPA, o como lo denomine el fabricante, ZTNA, sandbox, gestion de vulnerabilidades, RBI, Cloud API CASB & DLP,

ZTNA sin agente, direcciones publicas dedicadas, Monitoreo de experiencia de usuario, Integracion con Servicio de SOC, servicio de respuesta forense, asistencia en las configuraciones

- La solución de SASE permite realizar segregación de roles y funciones para los administradores por cada funcionalidad.

3.12.3 Acceso Seguro a Internet (Secure Internet Access SIA)

- La solución SASE debe incluir inspección SSL
- La solución debe incluir un sistema de Anti-virus (AV) en línea incluido propio del fabricante.
- La solución debe incluir un sistema de prevención de intrusión incluido
- La solución debe incluir filtrado Web y DNS incluido
- La solución debe incluir filtrado de Botnet y prevencion de Comando y Control
- La solución debe incluir Aislamiento de browser remoto (Remote Browser Isolation RBI) del usuario final

3.12.4 Acceso Seguro a aplicaciones SaaS (Secure SaaS Access SSA)

- La solución debe incluir agente de seguridad de acceso a la nube (Cloud Access Security Broker CASB) en línea
- La solución debe incluir un sistema de prevención de perdida de datos (Data Loss Prevention DLP) en línea
- La solución debe incluir API en nube para CASB y DLP

3.12.5 Acceso Privado Seguro (Secure Private Access SPA)

- El punto de acceso de SASE debe tener la posibilidad de integrarse nativante con los equipos SD-WAN para realizar conexiones directas y comportarse como un hub adicional en la arquitectura interna de la Compañia.
- La solución debe incluir Zero Trust Network Access (ZTNA)

- La solución debe incluir ZTNA sin agente
- Se debe poder definir donde realizar la inspección de seguridad on-prem (equipos sdwan) y en nube con la misma postura de seguridad.
- Se debe tener la opción de acceder a aplicaciones locales, pero con inspección de seguridad incluida
- Se debe soportar el análisis de tráfico iniciado por el Cliente y por servidor y gestionados desde la misma consola

3.12.6 Licencias incluidas

- Se debe permitir el uso de minimo tres (3) dispositivos por usuario sin incrementar la licencia y pueden usar una combinacion de modo con agente y/o modo proxy.
- Se debe incluir minimo cuatro (4) direcciones IP publicas dedicadas

3.12.7 Seguridad para los equipos finales (Endpoint Security)

- La solución debe incluir un único agente que tenga las funciones de protección de antivirus (endpoint protection EPP), antiransonware, escaneo de vulnerabilidades, control de dispositivos USB, chequeo permanente de postura, VPN, ZTNA y SASE. No se admiten soluciones con funciones separadas o múltiples agentes o funciones que estas funciones se encuentren en la nube.
- La solución incluirá el servicio de Sandbox para evaluar riesgos en el equipo final.
- La solución incluirá el servicio de Gestión de vulnerabilidades
- El agente debe validar la postura permanentemente. No se admiten soluciones en las cuales deba realizar la desconexión y conexión para validar nuevamente la postura.
- El agente debe estar en capacidad de soportar mínimo Windows, MacOS y Linux.
- Los logs de seguridad deben cubrir los componentes principales para mejorar la detección de errores - AV, Filtrado Web, Filtrado de archivos, inspección SSL, control de aplicaciones, DLP e IPS.

3.12.8 Integración NOC / SOC

- La solución SASE debe poder generar reporte de logs, y reenviarlos a otras soluciones. Cloud Logging, Reporting & Log Forwarding
- La solución debe generar reportes de control y riesgo de las aplicaciones, uso de VPN y web y cyber-bullyng.
- La solución debe incluir el monitoreo de experiencia Digital en los equipos que tienen agente instalado.
- La solución SASE se debe integrar con el servicio de SOC-as-a-Service entregado por el mismo fabricante.
- La solución SASE debe integrarse con un servicio de Respuesta Forense para determinar riesgos en los equipos donde se instale el agente ZTNA.
- Toda la solución de seguridad debe ser del mismo fabricante de SD-WAN incluyendo la protección en nube y la protección de los equipos finales.
- Los servicios de seguridad como AV, IPS y filtrado web deben ser avalados por un laboratorio de pruebas externo.
- El control de aplicaciones en el FWaaS debe identificar aplicaciones y estar en capacidad de identificar aplicaciones y sub-conjuntos de aplicaciones dentro de una aplicación especifica.
- El firewall como servicio (FWaaS) debe estar en capacidad de aplicar inspección de contenido sobre cualquier política y protocolo. No debe estar restringido a HTTPS, DNS y FTP. Debe incluir soporte para protocolos de voz incluyendo SIP, VoIP, H.323, H.248.

3.12.9 Gestión

- El servicio de SASE debe proveer una consola unificada para la gestión y orquestación del servicio, herramientas y servicios que hacen parte de la arquitectura incluida la seguridad del usuario final y sus dispositivos finales. No se aceptan múltiples consolas para este proceso.
- La solución SASE debe permitir la integración por medio de REST API
- La solución debe proveer reportes para visualizar el comportamiento de las aplicaciones, seguridad y actividades de usuarios.

3.13 SERVICIO DE CONTROL DE ACCESO A LA RED

Como parte de la Estrategia de Seguridad Digital de la Entidad, se ha determinado la contratación de un servicio de Control de Acceso a la Red (NAC) que garantice una visibilidad y control granular sobre todos los dispositivos que se conecten a la infraestructura, el cual deberá ofrecer una integración nativamente con el servicio de SD-WAN y LAN (Switches y Access Point) desplegados específicamente para la sede San Martin, permitiendo que la autenticación, la asignación de perfiles de red y el cumplimiento de posturas de seguridad se gestionen de forma unificada para asegurar que solo los activos autorizados y saneados puedan acceder a los recursos institucionales y de nube; para lo cual se deberán cumplir los siguientes puntos:

3.13.1 Alcance

- La Entidad requiere la implementación, puesta en marcha, afinamiento, operación, soporte y monitoreo de una solución de NAC en Alta Disponibilidad Georedundante que conste de appliances virtual, los cuales deberán estar alojados en la nube privada del oferente que cuente con licenciamiento para controlar mínimo 1500 dispositivos. No se aceptarán soluciones con appliances o hardware físicos.
- El oferente será responsable de suministrar los costos de licenciamiento, recursos de cómputo y la conectividad para acceder a los servicios.

3.13.2 Generalidades

- La solución debe estar en capacidad de instalarse en Azure, HyperV, Vmware y KVM.
- La solución NAC debe incluir los siguientes bloques funcionales:
  - Visibilidad de red y perfilado de dispositivos conectados.
  - Automatización del proceso de provisión de red en función del tipo de dispositivo que se esté conectando
  - OnBoarding de nuevos dispositivos sencillo, versátil y potente.

- Endpoint Compliance: Permitiendo a la organización desplegar políticas asociadas a diferentes grupos de usuarios, verificando su cumplimiento y notificando las desviaciones, permitiendo configurar diferentes protocolos de remediación, desde acciones de aislamiento inmediatas a simples notificaciones, pasando por acciones diferidas.
- Identificación de amenazas, a través de la integración con otros elementos, y ejecución de acciones de remediación en función del evento.
- Gestión de invitados y usuarios externos: Fácil y rápida, sin necesidad de involucrar al personal de IT en el alta de nuevos usuarios externos por medio de patrocinadores o Sponsors.

- La solución NAC debe ser agnóstica respecto a los fabricantes del equipamiento de acceso, tanto cableado como inalámbrico y por tanto válida en redes hetereogéneas.
- La solución NAC debe estar integrada con los dispositivos de red y seguridad existentes, y los que se incluyan en la nueva arquitectura.
- Debe ser capaz de trabajar bien con agentes instalados en los endpoints, o bien sin agentes.
- La solución NAC no puede ser dependiente de soluciones 802.1x y RADIUS, pero debe de ser compatible.
- La solución debe contar con fuente de poder dual de mínimo 500W Hot Plug
- La solución debe tener incluidos los módulos de integración con terceros
- La solución debe integrarse con el Firewalls, SIEM, Generador de Analítica, Sandbox, EDR y Honeypots.

3.13.3 Perfilado de Dispositivos

- La solución NAC debe tener capacidad para inventariar todos los dispositivos de la red, incluyendo equipamiento que no sea PC, como impresoras, Smartphones (Iphone, Android y Windows Phone), teléfonos IP, cámaras y otros dispositivos IoT que pudieran existir (biométricos…) y dispositivos OT.
- Debe poder utilizar al menos 20 métodos diferentes para identificar el tipo de dispositivo: DHCP fingerprint, NMAP scan, Vendor OUI, ubicación, puertos abiertos o información obtenida a través de agentes.

- Debe soportar el perfilado de dispositivos interactuando con el dispositivo mediante HTTP/HTTPS, SSH/Telnet o incluso interaccionando con el dispositivo a través de scripts diseñados a medida.
- Debe incluir un servicio dinámico de identificación de dispositivos IoT que comparta la información disponible sobre el dispositivo a perfilar con un servicio en Nube, que emplee técnicas de inteligencia que ayuden a la identificación del dispositivo.
- Debe soportar el perfilado de dispositivos Windows pertenecientes al domino mediante WMI o WINRM, utilizando canales seguros y validados mediante certificado.

3.13.4 Authentication y Enforcement

- La solución debe permitir conectarse a la red corporativa solo a dispositivos autenticados/registrados, desplegando políticas de seguridad que bloqueen y aíslen dispositivos que no cumplan los criterios corporativos, enviándolos a un área de cuarentena sin necesidad de intervención por parte de los administradores de red.
- Debe ser capaz de autorizar los accesos mediante asignación dinámica de VLAN's y/o aplicando ACLs al puerto de acceso.
- Debe ser capaz de controlar escenarios en los que hay más de un equipo conectado a un puerto, asociando a cada equipo la VLAN adecuada, siempre que el equipo de acceso lo permita.
- Debe ser capaz de integrarse con los firewalls para asociar los dispositivos a reglas de seguridad concretas, en función del tipo de dispositivo.
- Debe soportar autenticación de máquina y usuarios, pudiendo autenticar un endpoint sin usar agentes.
- Debe de ser capaz de asociar al dispositivo atributos adicionales, como la ubicación, tipo de dispositivo, fabricante. Además de los atributos del usuario conectado.
- Debe soportar opciones de autenticación flexibles, incluyendo 802.1X, autenticación WEB y autenticación MAC.
- Para despliegues 802.1X, debe poder actuar como Radius Proxy y como Radius local (TTLS/PAP, l TTLS/MSCHAPv2, PEAP/MSCHAPv2, TLS)

- Debe soportar integración LDAP y Microsoft Active Directory, sin necesitar ningún componente adicional, para desplegar políticas en función de su pertenencia a ciertos grupos.
- Debe soportar RADIUS Identity store.
- Debe soportar la detección y perfilamiento de sistemas operativos chrome
- Integración de MDM incluida
- Debe soportar enforcement por medio de SSH/SNMP

3.13.5 Requisitos de Endpoint Compliance y Remediación

- La solución debe soportar inspección de los dispositivos tanto basada en agente (persistente y disoluble) como sin agente.
- La solución NAC debe ser capaz de realizar, al menos, las siguientes comprobaciones: service packs, nivel de parcheo, que haya instalado las actualizaciones críticas, Antivirus y AntiSpyware, servicios y procesos, certificados, existencia de archivos y cualquier entrada del registro de Windows.
- Debe contar con un Motor de correlación de eventos.
- La solución debe proporcionar un rol de cuarenta que se interactúe con los Sistemas de parcheo. De esta manera, los dispositivos corporativos que no cumplan los requisitos serán enviados a un portal cautivo de "auto-remediación": Los equipos que no sean compliant debe de ser enviados a cuarentena dinámicamente, y o bien se le proporcionan instrucciones para la remediación o se ejecuta la remediación automática a través de sistemas como BigFix.

3.13.6 Gestión de Invitados

- El Sistema de control de acceso debe proporcionar una plataforma flexible y eficiente de gestión de usuarios no corporativos, que permita manejar el acceso de aquellos usuarios con un acceso transitorio (típicamente invitados) o con un acceso más estable (contratistas externos).
- Debe permitir definir perfiles limitados que solo tengan acceso a la gestión de cuentas de invitados.

- Debe permitir altas masivas (p.e. para conferencias), autoregistros, registros esponsorizados o dados de alta por un administrador.
- Debe permitir autenticaciones por medio de redes Sociales.
- Debe permitir la opción de Aceptar invitados por medio de patrocinadores o Sponsors.
- Debe ser flexible y permitir la definición de diferentes perfiles, como invitados de corta /larga estancia, asistentes a conferencias o auto-registrados.

3.13.7 Gestión y Reporte

- El sistema de control de acceso almacena información crucial sobre la red, cuántos elementos hay conectados y sus características, cuántos cumplen la política de seguridad de la empresa así como los eventos de seguridad que se puedan haber producido. También almacena información sobre eventos en la red (cambios en los puertos, conexiones, etc.) que pueden ser de gran utilidad para realizar investigaciones después de que se produzca una investigación.
- Debe ofrecer una consola de monitorización, reporting y troubleshooting que ayude a los administradores y operadores de helpdesk.
- La consola debe ser accesible a través de una GUI Web, sin necesidad de aplicaciones específicas.
- Debe permitir obtener, al menos, la siguiente información:
    - Eventos de conexión a lo largo del tiempo.
    - Cambios en los puertos.
    - Eventos de seguridad detectados por la plataforma a lo largo del tiempo (por ejemplo, fingerprints que cambian, intentos de impersonación…).
    - Eventos de seguridad recibidos de otras plataformas, y las acciones tomadas
    - Resultado de los escaneos de compliance (fallados, pasados)
    - Histórico de dispositivos conectados, última conexión…)
- Debe incluir plantillas de reportes, ejecutables bajo demanda o programados).
- Debe permitir customizar los reportes.
- Debe de incluir plantillas de despliegue de políticas.

- Debe de permitir la opción de usar un Sistema de reporte y monitorización dedicado.

3.14 SERVICIOS DE PROTECCIÓN, RENDIMIENTO Y SEGURIDAD PARA APLICACIONES WEB.

El INMLCF requiere la contratación de una solución integral de seguridad y rendimiento para aplicaciones web basada en una red global de borde (Edge) en modalidad de servicio, con el fin de garantizar la disponibilidad, integridad y rendimiento de sus activos digitales. El servicio debe integrar, bajo una arquitectura unificada, capacidades de mitigación de ataques de denegación de servicio (DDoS) de capa 7 y 4, firewall de aplicaciones web (WAF), red de entrega de contenido (CDN).

3.14.1 Especificaciones Técnicas del Servicio

- La plataforma propuesta por el oferente debe contar con una arquitectura de Red Anycast "Every Service, Every Location" con la capacidad de ejecutar el 100% de los servicios (WAF, AntiDDoS, CDN, Load Balancing, entre otros.) en cada uno de sus puntos de presencia (PoP) evitando únicos puntos de falla y cuellos de botella geográficos
- La plataforma propuesta por el oferente debe contar con más 335 centros de datos (PoP) distribuidos a nivel global.
- La solución propuesta debe contar con la capacidad de mitigar ataques volumétricos y de aplicación en el punto de entrada. Con una capacidad de +477 Tbps en el Borde con el fin de absorber ataques masivos sin degradar la experiencia del usuario final.
- La solución propuesta deberá estar a menos de 50ms de casi cualquier ciudadano con acceso a Internet. Esto es necesario para procesos de identificación y votación donde la velocidad de carga impacta directamente en la experiencia y confianza del ciudadano.
- IA en el Borde (Future-Proofing): La solución deberá con GPUs instaladas en 210 ciudades para inferencia de IA en el borde.

- La solución técnica propuesta deberá basarse en una arquitectura de desarrollo nativo y unificado, garantizando que la totalidad de los servicios de seguridad y rendimiento operen bajo una misma plataforma lógica sin fragmentaciones derivadas de adquisiciones de terceros. La plataforma debe permitir la integración automatizada entre sus módulos; específicamente, los datos generados por el componente de protección API deberán integrarse de forma directa en las reglas del Firewall de Aplicaciones Web (WAF) sin requerir exportaciones manuales de datos o servicios profesionales adicionales para la correlación de eventos. El oferente debe asegurar que esta gestión centralizada permita administrar y correlacionar amenazas en tiempo real desde una consola única, optimizando la eficiencia operativa y eliminando la complejidad técnica de gestionar múltiples interfaces inconexas.

- Visibilidad Global de Amenazas de Día Zero: la solución propuesta deberá identificar patrones de ataque antes de que se conviertan en amenazas locales.
- La solución propuesta deberá ser 100% en nube, permitiendo reducir el tiempo de despliegue de políticas de minutos a segundos.

- La solución propuesta deberá contar con una capacidad de red masiva de +477 Tbps e interconexión con +13,000 redes a nivel mundial.

- El oferente deberá presentar una solución que haya mitigado automáticamente ataques con volumetría de 31.4 Tbps y 14.1 mil millones de paquetes por segundo (pps) en el borde, asegurando que el tráfico malicioso nunca llegue a la infraestructura de la entidad.

- La solución propuesta deberá estar a menos de 50 ms del 95% de la población conectada globalmente, gestionando 85 millones de consultas DNS por segundo (7.4 trillones al día) a nivel global, garantizando una resolución instantánea y alta disponibilidad para los portales de trámites y resultados electorales de la entidad.

- La solución propuesta deberá centralizar la seguridad y el rendimiento en un único Dashboard nativo. Esta consola unificada debe permitir que el equipo de la entidad administre y correlacione amenazas en tiempo real sin saltar entre múltiples plataformas, incrementando la eficiencia operativa en un 29% y eliminando errores por fatiga de herramientas inconexas.

- La solución deberá integrarse con el SIEM de la entidad a través del aprovisionamiento de un bucket de S3 en AZURE, el cual deberá ser suministrados, administrados y soportado por el oferente.
- La solución debe integrar capacidades de Gestión de Bots sustentadas en una red global con visibilidad de amenazas en tiempo real. El sistema debe contar con el respaldo de una infraestructura que procese un volumen masivo de tráfico global, permitiendo el bloqueo proactivo de un promedio de 230 mil millones de amenazas diarias. Asimismo, la plataforma debe garantizar la mitigación de ataques dirigidos a aplicaciones vía HTTPS con una capacidad de respuesta de hasta 205 millones de solicitudes por segundo (Mrps) sin degradar el rendimiento de los servicios. Esta operatividad debe estar soportada por una arquitectura de alta disponibilidad capaz de procesar un promedio de 93 millones de peticiones por segundo en el borde de la red.

- La solución debe proporcionar una capa de seguridad específica para proteger interfaces de programación (APIs) contra ataques dirigidos.
- La solución deberá utilizar inteligencia distribuida para identificar y mitigar tráfico automatizado malicioso.
- La solución deberá supervisar la ejecución de scripts en el navegador del usuario para detectar ataques de skimming o inyecciones de código de terceros.
- La solución debe ofrecer protección integral contra vulnerabilidades web.
- La solución debe permitir extender la protección de protocolos que no son HTTP/S (como TCP o UDP).

- La solución deberá integrar un motor de enrutamiento inteligente que identifique y evite en tiempo real las congestiones de la red pública de Internet, seleccionando dinámicamente las rutas más rápidas y confiables a través de la infraestructura global del fabricante. Este componente debe optimizar la entrega de activos digitales mediante el uso de telemetría de red avanzada, garantizando una reducción significativa en la latencia y una mejora en la velocidad de carga de las aplicaciones para el usuario final.

- La solución deberá integrar una funcionalidad de balanceo de carga global que permita la distribución inteligente del tráfico entre múltiples centros de datos o servidores finales (endpoints) para garantizar la continuidad del negocio y la alta disponibilidad de los servicios. Este componente debe ser capaz realizar comprobaciones de estado constantes para redirigir el tráfico automáticamente hacia la infraestructura más cercana o disponible. Al operar de forma nativa en la red global de borde, la solución debe eliminar los puntos únicos de falla y evitar cuellos de botella geográficos, asegurando que las peticiones de los ciudadanos se resuelvan de manera instantánea y eficiente.

- La plataforma deberá garantizar compatibilidad nativa y simultánea para protocolos IPv4 e IPv6 en la totalidad de los componentes y servicios contratados. La red de borde debe realizar la terminación y traducción de tráfico de forma transparente, asegurando que las funciones de seguridad (WAF, DDoS, Bot Management), rendimiento (CDN, Enrutamiento Inteligente) y conectividad (DDoS L4) operen sin restricciones bajo ambos estándares de direccionamiento.

3.14.2 Generalidades

- El oferente seleccionado será el responsable integral de la implementación, configuración, administración y soporte técnico de la totalidad de la solución contratada. Esta responsabilidad abarca la puesta en marcha de todos los componentes de seguridad y rendimiento (WAF, DDoS, CDN, entre otros), garantizando que la transición operativa se realice sin interrupciones en los servicios digitales de la Entidad.

- El oferente deberá acreditar la calidad de Partner Nivel Plus (Tier 1) o su equivalente más alto, vigente a la fecha de presentación de la oferta.

- El proponente deberá demostrar una relación comercial directa con el fabricante de la solución propuesta, sin intermediarios. No se aceptarán ofertas bajo la modalidad de uniones temporales o consorcios que no cuenten con la certificación directa de nivel superior emitida por el fabricante.
- Se deberá adjuntar una certificación emitida por el fabricante donde se valide el nivel de alianza solicitado y se garantice el respaldo técnico de segundo y tercer nivel para la Entidad durante toda la vigencia del contrato.

4. IPV6

El presente capítulo consolida y depura los requerimientos técnicos **derivados íntegramente del anexo "ANEXO IPV6"** y se incorpora como condiciones obligatorias para la continuidad, estabilidad y sostenibilidad operativa del protocolo IPv6 en coexistencia con IPv4 (Dual Stack) en el INMLCF.

4.1 Contexto y estado actual de la infraestructura

El Instituto Nacional de Medicina Legal y Ciencias Forenses (INMLCF) cuenta con una infraestructura de red implementada y en operación bajo el esquema de doble pila (Dual Stack IPv4/IPv6), aplicada de forma integral sobre los componentes institucionales, incluyendo:

- Infraestructura de red WAN y LAN
- Plataformas de seguridad
- Infraestructura tecnológica
- Servidores y Servicios misionales y de soporte (Infraestructura local y la nube de Azure).

En consecuencia, la Entidad requiere garantizar la continuidad, estabilidad y sostenibilidad operativa del protocolo IPv6, en coexistencia con IPv4, como parte fundamental de su arquitectura tecnológica

vigente.

4.2 Compatibilidad obligatoria IPv4 / IPv6 (Dual Stack)

El Proponente/Contratista deberá garantizar y mantener de manera ininterrumpida la adopción simultánea de IPv6 e IPv4 en todos los componentes y soluciones que hagan parte del alcance contractual.

Como mínimo, deberá asegurar que:

- Todos los servicios operen de forma nativa bajo ambos protocolos (IPv4 e IPv6).
- La coexistencia IPv4/IPv6 se mantenga sin afectación a la disponibilidad, desempeño o seguridad de los servicios.
- No se requieran cambios estructurales ni disruptivos sobre la infraestructura Dual Stack ya operativa del INMLCF.

4.3 Gestión y preservación del direccionamiento IP

El Proponente/Contratista será responsable de:

- Mantener en condiciones óptimas de funcionamiento los esquemas de direccionamiento IPv4 e IPv6 implementados en la Entidad.
- Conservar el direccionamiento otorgado.
- Un (1) prefijo IPv6 /44 y el Sistema Autónomo, ambos registrados a nombre de la entidad.
- Organización: INSTITUTO DE MEDICINA LEGAL Y CIENCIAS FORENSES
- Preservar las configuraciones de red que respaldan la coexistencia de ambos protocolos, garantizando la integridad de las configuraciones actuales del Sistema Autónomo asignado a la Entidad.
- Garantizar que cualquier nuevo servicio, modificación, ampliación o integración cumpla con los rangos, políticas y estándares de direccionamiento IPv6 establecidos por el INMLCF, los cuales son recomendación directa del MinTIC

4.4 Integración de nuevos componentes, sistemas o servicios

Cualquier nuevo componente, sistema o servicio que sea propuesto, suministrado o integrado durante la vigencia del contrato deberá cumplir obligatoriamente con las siguientes condiciones técnicas:

- Ser compatible de forma nativa con IPv4.
- Integrarse plenamente a la infraestructura Dual Stack existente.
- Adaptarse a las políticas, estándares y esquemas de direccionamiento IPv4/IPv6 ya establecidos por el INMLCF.
- No generar afectaciones a la operación actual ni requerir reprocesos sobre la infraestructura existente.

4.5 Equivalencia de rendimiento, seguridad y gestión

El Proponente/Contratista deberá garantizar que las funcionalidades de red bajo IPv6 cuenten con el mismo nivel de calidad que las ofrecidas bajo IPv4, asegurando como mínimo:

- Igual nivel de rendimiento y estabilidad.
- Mecanismos de seguridad equivalentes.
- Capacidades de gestión, monitoreo y operación consistentes entre ambos protocolos.
- Continuidad del servicio bajo escenarios de coexistencia IPv4/IPv6.

4.6 Principio de continuidad del servicio

La operación y mantenimiento de IPv6 deberá ejecutarse bajo el principio de continuidad del servicio, por lo cual:

- No se permitirán cambios que impliquen interrupciones no controladas.
- No se aceptarán soluciones que requieran migraciones disruptivas.
- La infraestructura Dual Stack existente deberá mantenerse operativa durante toda la vigencia contractual.

4.7 Carácter obligatorio y aceptación

- Cumplimiento obligatorio: Todos los requerimientos establecidos en este capítulo son de cumplimiento obligatorio.
- No aceptación por incumplimiento: La inobservancia de cualquiera de las condiciones descritas dará lugar a la no aceptación de la solución propuesta, sin perjuicio de las demás consecuencias contractuales aplicables conforme al Pliego de Condiciones.

4.8 Verificación y evidencias de cumplimiento

Para efectos de recepción y aceptación, la Entidad podrá requerir evidencias documentales y/o pruebas de operación que demuestren:

- Operación Dual Stack (IPv4/IPv6) nativa en los servicios incluidos en alcance.
- Preservación de esquemas de direccionamiento y configuraciones existentes, y que cualquier ajuste respeta políticas definidas por la Entidad.
- Integración de nuevos componentes sin afectación del entorno actual y sin migraciones disruptivas.

5. SERIVIOS WIFI MOVILES A NIVEL NACIONAL

SOSTENIBILIDAD DEL SERVICIO INTEGRAL DE MOVILIDAD: 50 SERVICIOS WIFI MOVILES A NIVEL NACIONAL

Contratar la sostenibilidad, operación y administración de una solución integral de movilidad para cincuenta (50) servicios WiFi-móviles que permitan conexión directa, WiFi administrable y distribución de conectividad móvil 4G LTE o superior, bajo un esquema de contingencia a nivel nacional.

5.1 El oferente deberá suministrar, habilitar y operar como mínimo:

- Cincuenta (50) servicios WiFi-móviles a nivel nacional, que permitan conexión directa y WiFi administrable.

5.2 El Contratista deberá suministrar y garantizar, como mínimo:

- Cincuenta (50) servicios WiFi móviles con capacidad de conexión directa y WiFi administrable.
- Debe prestar el servicio mediante una solución integral de movilidad la cual incluye 50 modems, con los planes solicitados así: 20 sim card de TIGO, 15 sim card de Claro, 15 sim card de Movistar.
- Conectividad móvil 4G LTE o superior, operativa en cualquier ubicación con cobertura del servicio móvil, para fines de contingencia institucional.
- Capacidad mínima de navegación de 100 GB (por servicio/línea, conforme al esquema contratado), disponible “en cualquier lugar con cobertura de red móvil 4G o superior”.
- Cobertura de conectividad en todo el territorio nacional, incluyendo Isla de San Andrés y Providencia.
- Mecanismo de recarga de datos cuando se agote la capacidad incluida, para garantizar continuidad del servicio.
- Provisión de una plataforma de monitoreo para medir datos consumidos por cada línea/servicio (al menos a través de la plataforma del operador que oferta el servicio).
- Disponibilidad de un Centro de Control que permita la autogestión de los servicios móviles e incluya, como mínimo, los módulos indicados en este Anexo.

5.3 Requerimientos mínimos funcionales

5.3.1 Funcionalidad de punto de acceso WiFi (movilidad)

El servicio debe permitir establecer una red inalámbrica tipo punto de acceso WiFi utilizable en cualquier lugar, habilitando conectividad para más de un dispositivo de manera simultánea, destacando movilidad y conectividad para atender contingencias por indisponibilidad del servicio principal.

5.3.2 Capacidad mínima y continuidad por recargas

a) Cada servicio debe disponer de una capacidad mínima de 100 GB de navegación según el esquema contratado.

b) Si se consumen los 100 GB, la Entidad debe contar con la posibilidad de recargar datos al dispositivo/servicio para garantizar la prestación continua.

c) La recarga será facturada mes a mes y solo podrá ser solicitada por personal autorizado por la Entidad

5.4 Requerimientos mínimos de monitoreo, autogestión y plataforma (Centro de Control)

5.4.1 Plataforma de monitoreo de consumo

El Contratista debe proporcionar una plataforma que permita medir la cantidad de datos utilizados por cada línea (al menos mediante la plataforma propietaria del operador que oferta el servicio).

5.4.2 Centro de Control para autogestión

El Centro de Control deberá permitir realizar la autogestión de los servicios móviles y deberá contar, como mínimo, con los siguientes módulos:

Dispositivos

- Facturación
- Administración
- Automatización
- Base de conocimientos
- Estadísticas

5.5 Requerimientos mínimos de reportes

El Contratista deberá entregar reportes mensuales asociados al servicio, incluyendo (como mínimo) reporte de usabilidad.

Adicionalmente, se deberán incluir reportes como páginas visitadas, entre otros, en la medida de lo posible según capacidades del servicio y del operador.

5.6 Requerimientos mínimos de equipos y SIM

Los equipos y las SIM Cards que formen parte del servicio deben ser nuevos.

5.7 Requerimientos mínimos técnicos del equipo (router WiFi 4G/LTE o superior) – neutrales (sin marca)

Este apartado define mínimos de compatibilidad y capacidad. Si el Contratista suministra equipos o si la Entidad aporta equipos, deberán cumplir los mínimos siguientes (o equivalentes/superiores

5.7.1 Conectividad móvil (WWAN)

- Soporte de **4G LTE** (mínimo) y **3G**.
- Categoría LTE **Cat 4 o superior**.

5.7.2 Conectividad WiFi (WLAN)

- WiFi **802.11 b/g/n**, banda **2.4 GHz**
- Capacidad WiFi de referencia: **2x2 MIMO** y desempeño equivalente a **300 Mbps** (o superior).
- Soporte de **mínimo 32 usuarios** simultáneos.

5.7.3 Interfaces mínimas

- Al menos **1 puerto Ethernet RJ45** (WAN/LAN).
- **Ranura para SIM**.
- Conector para **antena externa** (o equivalente).
- Botones/funciones mínimas: **WPS** y **Restablecer**.

5.7.4 Requisito adicional cuando el dispositivo soporte voz (si aplica)

- En caso de ser dispositivo de voz, deberá soportar **VoLTE**.

5.8 Compatibilidad mínima con la red del operador (cuando la Entidad aporte equipos o adquiera con terceros)

Si la Entidad dispone de equipos propios o adquiridos con terceros, para asegurar compatibilidad con la red del operador, el equipo deberá cumplir como mínimo:

Soporte de bandas **B2, B4 y B28**

- Soporte de tecnologías **3G y 4G**.
- Si es de voz: soporte **VoLTE**.
- Contar con **homologación ante la Comisión de Regulación de Comunicaciones (CRC)**.

5.9 Requerimiento asociado a SD-WAN (cuando aplique como canal secundario)

Para dar cumplimiento al requerimiento de canal secundario en un esquema pasivo de **SD-WAN**, se contempla un servicio móvil LTE a nivel nacional por sede solicitada, como contingencia.

Importante: La cantidad de sedes y dimensionamiento por sede se deberá ajustar al anexo de sedes del proceso, manteniendo el cumplimiento del canal secundario.

5.10 Condición de cierre (equipos en modalidad de servicio)

Cuando los equipos móviles se entreguen en modalidad de servicio, al finalizar el contrato deberá existir la **opción** para que la Entidad los adquiera conforme a las condiciones pactadas (según el modelo contratado).

Nota de implementación: Si adicionalmente se requiere atender un esquema de **canal secundario (pasivo) para SD-WAN**, el oferente deberá incluir servicios móviles LTE por sede según el anexo de sedes, como parte de la contingencia.

Se detalla para la conexión de datos con salida a internet con servicio 4G LTE para permitir servicio Wifi en sitio:

SERVICIO	CANTIDAD	PROPUESTA TIGO
Conectividad Gestionada	50 líneas	Individual Controlado 100 GB - Planes móviles con MIFI
Equipos MIFI (Servicio)	50	MODEM con las especificaciones descritas o superiores

SDWAN

Para dar cumplimiento al requerimiento de canal secundario en un esquema pasivo de SDWAN, se contempla en cada una de las sedes solicitadas un servicio móvil LTE a nivel nacional.

SERVICIO	CANTIDAD	PROPUESTA TIGO
Conectividad Gestionada	2 bolsas	Bolsa Fija 5 TB - Planes móviles para SDWAN
Equipos Router	95	LTE o similar

Nota: en todo caso, el anterior alcance se circunscribe únicamente a lo ofertado en el presente documento

6. REQUERIMIENTOS DEL PERIODO DE TRANSICIÓN.

El presente Anexo Técnico tiene por objeto establecer las **condiciones técnicas, operativas y obligatorias** que deberá cumplir el **PROVEEDOR** para la ejecución del **período de transición de los servicios de conectividad, red LAN y ciberseguridad**, garantizando la continuidad, estabilidad y disponibilidad de los servicios del INMLCF.

Alcance del Período de Transición

El PROVEEDOR deberá planear, ejecutar y culminar el **período de transición de los servicios de conectividad, wan, sdwan, LAN(**switch core, switch acceso, solución wi-fi**), IPV6 y ciberseguridad**, asegurando que dichos servicios se encuentren **plenamente implementados, operativos y funcionando de manera estable a más tardar el primero (1) de agosto de 2026**.

Para la conectividad hacia azure el proveedor deberá establecer un cronograma de implementación en conjunto con la entidad entendiendo que el INMLF realizará la migración a azure y deberá estar alienado a las actividades de azure.

Para los servicios de SECURE ACCESS SERVICE EDGE (SASE) y CONTROL DE ACCESO A LA RED NAC

El proveedor deberá establecer un cronograma de implementación en conjunto con la entidad

entendiendo que el INMLF realizará la migración a Azure y deberá estar alienado a las actividades de azure.

El período de transición comprenderá, como mínimo, las actividades de planeación, coexistencia de plataformas, migración tecnológica, pruebas técnicas, validaciones operativas, ajustes de configuración, puesta en producción y estabilización de los servicios.

6.1 Condiciones Técnicas Obligatorias

Durante el período de transición, el PROVEEDOR deberá garantizar, bajo su exclusiva responsabilidad, el cumplimiento de las siguientes condiciones técnicas obligatorias:

a) **Continuidad del servicio:**

No se deberá generar **ningún tipo de indisponibilidad, interrupción, degradación o afectación** en la prestación de los servicios actualmente en operación en la Entidad.

b) **Operación ininterrumpida:**

Los servicios deberán mantenerse activos, estables y disponibles durante todo el proceso de transición, conservando los niveles de calidad, desempeño, seguridad y disponibilidad definidos contractualmente.

c) **Transición controlada:**

Las actividades de migración y coexistencia deberán ejecutarse de forma progresiva, controlada y coordinada con la Entidad, minimizando riesgos técnicos y operativos.

d) **Gestión de riesgos y contingencias:**

El PROVEEDOR deberá implementar las medidas técnicas, operativas y de contingencia necesarias para prevenir incidentes y garantizar la continuidad del servicio durante toda la transición.

6.2 Fecha Límite de Entrada en Operación

El PROVEEDOR deberá garantizar que, como resultado del período de transición, los servicios de conectividad, LAN y ciberseguridad se encuentren **completamente operativos y en producción a más tardar el primero (1) de julio de 2026**, sin excepciones.

6.3 CONDICIÓN ECONÓMICA DEL PERÍODO DE TRANSICIÓN

- Todas las actividades asociadas a la transición deberán ser asumidas íntegramente por el PROVEEDOR.
- Las actividades asociadas a la planeación, coexistencia de plataformas, migración tecnológica, pruebas, acompañamiento, ajustes de configuración, puesta en producción y estabilización de los servicios deberán ser asumidas por el PROVEEDOR, sin generar cobros adicionales distintos a los expresamente autorizados en el contrato.
- Una vez cada servicio de conectividad sea instalado, entregado y se encuentre en operación efectiva, el PROVEEDOR deberá reflejar el costo correspondiente a la instalación de dicho servicio en la factura del mes en el cual se formalice su entrada en operación, de conformidad con las condiciones económicas y tarifas establecidas contractualmente.
- No se reconocerán costos adicionales por planeación, migración, coexistencia de plataformas, pruebas, acompañamiento, soporte, estabilización ni ajustes técnicos.

6.4 Carácter Obligatorio y Esencial

Las condiciones establecidas en el presente Anexo Técnico

Las condiciones establecidas en el presente Anexo Técnico son de **cumplimiento obligatorio** y hacen parte integral del contrato.

El incumplimiento de cualquiera de las obligaciones aquí descritas, en especial:

- La generación de indisponibilidad del servicio,
- El incumplimiento de la fecha límite establecida,
- O la imposición de costos a la Entidad,

Será considerado **incumplimiento grave**, dando lugar a la aplicación de penalidades, medidas correctivas y demás acciones contractuales a que haya lugar, conforme a lo establecido en el contrato y en el Pliego

de Condiciones.

7. ACUERDOS DE NIVELES DE SERVICIO (ANS/SLA)

El PROVEEDOR deberá definir, documentar y garantizar los Acuerdos de Niveles de Servicio (ANS/SLA) aplicables a la Solución Integral de Telecomunicaciones, asegurando continuidad operativa, disponibilidad, desempeño, seguridad, trazabilidad y cumplimiento contractual, conforme a los anexos técnicos del proceso y a las condiciones exigibles a una Para la entidad.

7.1. Alcance y componentes cubiertos

Los ANS/SLA aquí definidos aplican a todos los componentes incluidos en el alcance contractual, entre otros: conectividad (Internet/underlay/backup), SD-WAN y su orquestación, red LAN (core y acceso), WLAN, servicios administrados, ciberseguridad (SOC/RSOC, SIEM, AntiDDoS, ZTNA, correo, WAF y demás), continuidad IPv6 (dual stack), servicios WiFi-móviles y el período de transición, incluyendo la mesa de servicios y los canales de atención.

7.2. Principios de medición y gobierno del SLA

a) Medición: los indicadores deberán ser medidos de extremo a extremo y por componente (enlace, CPE, plataformas y servicios), con registros auditables y trazabilidad de eventos.

b) Ventanas de mantenimiento: deberán ser programadas y notificadas como mínimo con 5 días de antelación a la supervisión del contrato, sin afectar la continuidad del negocio; cuando impliquen indisponibilidad, deberán contar con plan de trabajo, reversa (rollback) y aprobación de la Entidad.

c) Exclusiones: solo se considerarán exclusiones por fuerza mayor o causas atribuibles demostrablemente a la Entidad; en todo caso, deberán documentarse en ticket y acta de incidente.

d) Reportes: el PROVEEDOR deberá entregar reportes mensuales de cumplimiento de SLA y reportes de incidentes críticos cuando la Entidad lo requiera, incluyendo causa raíz (RCA), acciones correctivas y preventivas.

7.3. Mesa de servicios, severidad y escalamiento

El PROVEEDOR deberá operar una mesa de servicios con atención 7x24x365 para la recepción y gestión de incidentes, solicitudes y cambios, con clasificación por severidad (Crítica, Alta, Media y Baja), tiempos de respuesta y resolución definidos contractualmente, y niveles de escalamiento (N1/N2/N3 y fabricante) hasta la normalización del servicio.

El esquema de escalamiento deberá incluir contactos, horarios, canales, tiempos máximos por nivel y el procedimiento de comunicación a la Entidad, manteniendo evidencias en el sistema de tickets.

7.4. ANS/SLA específicos por componente

7.4.1 Conectividad (Internet, enlaces principales y de respaldo)

- **Rehúso obligatorio 1:1:** Para todos los canales principales de Internet y para los enlaces de respaldo (backup) se deberá aplicar rehúso 1:1 (sin sobresuscripción) y simetría, garantizando que el ancho de banda contratado corresponda al ancho de banda efectivamente disponible para la Entidad, tanto en sentido de subida como de bajada.
- **Disponibilidad y calidad:** El PROVEEDOR deberá garantizar la disponibilidad, latencia, jitter y pérdida de paquetes conforme a los valores definidos en el Anexo de Conectividad y a los ANS establecidos para cada tipo de sede. La medición deberá sustentarse con herramientas de monitoreo y evidencias verificables.
- **Atención de fallas:** Los tiempos de atención, aislamiento, contingencia y restablecimiento deberán cumplir los ANS definidos. Para sedes con doble enlace, el failover deberá ser automático y sin intervención manual, manteniendo continuidad del servicio.
- **Gestión de capacidad:** El PROVEEDOR deberá realizar monitoreo proactivo de utilización y tendencias, y proponer ajustes para prevenir degradaciones; cualquier cambio de capacidad deberá tramitarse conforme al procedimiento de control contractual.
- Elaborar informe dirigido a la Supervisión para la entrega de la instalación de la conectividad, el cual debe contener los documentos que se enumeran a continuación:

- ARCHIVO DE EXCEL donde se relacione la siguiente información:
- Nombre sede

- Tipo de Servicio: Dedicado (1:1),
- Tecnología última milla:
- Terrestre: Fibra Óptica: Satelital LEO: Satelital GEO
- Inalámbrica: Radio
- Ancho de banda instalado
- Datos de contacto de quien recibió la instalación (nombre, teléfono fijo, celular, cuenta de correo y cargo)
- Número total de Puntos de acceso inalámbrico instalados (Si Aplica)
- Georreferenciación del sitio donde se instala el servicio.
- ACTA DE ENTREGA: Documento debidamente diligenciado y firmado por las partes (representante del Comitente vendedor y representante del INMLCF que en este caso es el supervisor del contrato.
- REGISTRO FOTOGRÁFICO DIGITAL: Donde se aprecie las condiciones en que fue ejecutada la instalación, las fotografías a enviar son:
- Entrada de la sede donde se detalle fachada, nombre, dirección.
- Recorrido del cableado para la instalación de los equipos de comunicaciones instalados por el Comitente vendedor
- Sitio de instalación de los equipos de comunicaciones
- Cada uno de los elementos suministrados e instalados, incluyendo las Antenas de la solución, si aplica
- Obras civiles (si las hubiere)
- Fotografía en que se evidencie acceso a los servicios.
- PRUEBAS DE VERIFICACIÓN DE LOS SERVICIOS: las pruebas que se deben realizar y enviar en el informe son las siguientes:
- Verificación de ingreso de cada uno de los computadores a la página https://medicinalegal.gov.co/ a la página del Proveedor de Redes y Servicios de Telecomunicaciones – PRST y por lo menos dos páginas internacionales.
- Reporte de tráfico de la sede instalada.

- ACTAS DIGITALIZADAS: El Comitente vendedor entregará en medio magnético el acta establecida en el numeral 2 de este título y todas aquellas actas y comunicaciones que se hayan generado en el desarrollo de su labor de instalación.

-

7.4.2 SD-WAN / Orquestación / Gestión centralizada

Aplican los ANS establecidos para una Para la entidad: operación 7x24x365, soporte N1/N2/N3, gestión de cambios con trazabilidad, continuidad de la plataforma de administración, monitoreo proactivo y reportes periódicos. Los tiempos de atención y solución se regirán por las tablas de ANS definidas en los anexos técnicos.

7.4.3 Red LAN (Core, Acceso, NAC/SD-Branch) y WLAN

Aplican los ANS establecidos para una Para la entidad: alta disponibilidad de componentes críticos (Core), soporte en sitio cuando aplique, reposición/RMA, y continuidad de operación. Los incidentes que afecten servicios misionales deberán tratarse con prioridad acorde a severidad, garantizando restablecimiento dentro de los tiempos comprometidos.

7.4.4 Ciberseguridad (SOC/RSOC, SIEM, AntiDDoS, ZTNA, Correo, WAF/SASE y demás servicios)

Aplican los ANS establecidos para una Para la entidad, incluyendo: monitoreo 7x24x365, gestión de incidentes por severidad, notificación y escalamiento inmediato en eventos críticos, retención y disponibilidad de logs, entrega de reportes mensuales y de RCA, y cumplimiento de lineamientos de seguridad, auditoría y confidencialidad institucionales. Los tiempos de contención, mitigación y respuesta deberán alinearse con los ANS definidos en los anexos de cada servicio.

7.4.5 Continuidad IPv6 (Dual Stack)

Aplican los ANS establecidos para una Para la entidad: continuidad del esquema Dual Stack sin afectación

a la operación, mantenimiento preventivo y correctivo, soporte 7x24x365 cuando el incidente afecte servicios críticos, y verificación de que cualquier integración o cambio preserve las políticas de direccionamiento y seguridad definidas por la Entidad.

7.4.6 Servicios WiFi móviles

Aplican los ANS establecidos para una Para la entidad: disponibilidad del servicio, soporte y reposición de equipos/SIM cuando aplique, gestión de recargas autorizadas, plataforma de monitoreo y reportes mensuales. Los tiempos de atención y solución deberán regirse por los ANS contractuales.

7.4. Período de transición

Durante el período de transición se aplicarán los ANS más estrictos definidos para continuidad del servicio para la entidad, con obligación de no generar indisponibilidades, ejecución sin costo para la Entidad, coexistencia controlada y planes de reversa. Cualquier afectación deberá ser tratada como incidente de alta criticidad y gestionarse con prioridad máxima.

- **Penalidades, créditos de servicio y mejora continua**

El incumplimiento de los ANS/SLA dará lugar a la aplicación de las penalidades, descuentos y demás medidas contractuales a que haya lugar, según el contrato y el pliego de condiciones.

El PROVEEDOR deberá proponer y ejecutar planes de mejora continua cuando se presenten tendencias de degradación o incumplimientos repetitivos, incluyendo acciones preventivas y de fortalecimiento de capacidad.

La Entidad podrá auditar en cualquier momento la medición de los indicadores, los tickets, bitácoras, logs y reportes asociados al cumplimiento del SLA. El PROVEEDOR deberá conservar evidencias verificables

durante toda la vigencia contractual y el periodo que establezca la normativa aplicable.

A manera de conclusión, se establece que el Instituto Nacional de Medicina Legal y Ciencias Forenses requiere la ejecución integral del objeto contractual dentro de un plazo de ejecución de hasta CINCO (5) MESES, contados a partir del cumplimiento de los requisitos de perfeccionamiento y legalización del contrato, sin que en ningún caso dicho plazo exceda el treinta y uno (31) de diciembre de 2026. Este término permitirá garantizar la adecuada implementación, transición, puesta en operación y estabilización de la Solución Integral de Telecomunicaciones, asegurando la continuidad de los servicios, el cumplimiento de los niveles de servicio pactados y la correcta ejecución técnica y operativa de las obligaciones contractuales.

SONIA PATRICIA CASTAÑEDA NEIRA
Profesional Especializado
Coordinadora Grupo Nacional de Tecnologías de Información y Desarrollo

	Nombre, apellido y cargo	Firma	Fecha
Proyectó	Pablo Emilio Martínez Salcedo Profesional Universitario – GNTID Leidy Carolina Morales Bermúdez Profesional Especializado - GNTID		04/05/2026
Revisó	Sonia Patricia Castañeda Neira – Coordinadora GNTID.		
Aprobó	Sonia Patricia Castañeda Neira – Coordinadora GNTID.		
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes, bajo nuestra responsabilidad, lo presentamos para la firma.			