CONVOCATORIA

Solicitud de Expresión de interés

REF.: LGMDE-005/2026-HNES

Contratación: SERVICIO DE SUMINISTRO, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN OPERACIÓN DE LA INFRAESTRUCTURA DE RED, CONECTIVIDAD INALÁMBRICA Y SEGURIDAD PERIMETRAL PARA EL PROGRAMA DOCTORSV.

Fuente De Financiamiento: Fondo General-Telemedicina

El Hospital Nacional El Salvador convoca a personas naturales y jurídicas, nacionales y extranjeras que a participar en el presente proceso de contratación LGMDE-005/2026-HNES, que tiene por objeto la adquisición de los productos siguientes:

ítem	Código SINAB	Código ONU	Denominación del bien o servicio	Cantidad
1	81209008	72151605	SERVICIO DE INSTALACION Y CERTIFICACION DE CABLEADO ESTRUCTURADO PARA VOZ Y DATOS	1
2	83121703	83121703	SERVICIO DE INSTALACION DE RED DE AREA LOCAL (LAN)	1

Condiciones Generales y Particulares de la Solicitud de Expresión de Interés:

Descargar Documento de Solicitud de Expresión de Interés en el enlace siguiente https://hnes.gob.sv/servicios/documentos-procesos-de-compra/

Para expresar interés en participar:

Enviar su propuesta a los correos electrónico: karen.valles@salud.gob.sv, karla.guzman@salud.gob.sv indicando en el asunto el nombre de la contratación y el proyecto.

El periodo para enviar expresiones de interés cerrará a las 15:00 horas del 7 de septiembre de 2026, Zona horaria de El Salvador (GMT-6). Las propuestas deberán incluir el formulario de identificación de proveedor (Anexo 1).

Distrito de San Salvador, San Salvador Centro, 1 de septiembre de 2026

SOLICITUD DE EXPRESIÓN DE INTERES

REF.: LGMDE-005/2026-HNES

Contratación: SERVICIO DE SUMINISTRO, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN OPERACIÓN DE LA INFRAESTRUCTURA DE RED, CONECTIVIDAD INALÁMBRICA Y SEGURIDAD PERIMETRAL PARA EL PROGRAMA DOCTORSV.

Fuente De Financiamiento: Fondo General-Telemedicina

El Hospital Nacional El Salvador (HNES) invita a personas naturales y jurídicas, nacionales o extranjeras a participar en el proceso de Solicitud de Expresión de Interés (SEI) que se regirá bajo las condiciones siguientes:

I. CONDICIONES GENERALES DEL PROCESO ADMINISTRATIVO DE CONTRATACIÓN.

A. NATURALEZA Y NORMATIVA APLICABLE.

La presente SEI se regirá de conformidad a lo previsto en la Ley General para la Modernización Digital del Estado y el Lineamiento para la Ejecución del Procedimiento Administrativo establecido en la Ley General para la Modernización Digital del Estado.

La presente SEI consistirá en una convocatoria pública a proveedores nacionales y extranjeros, domiciliados o no, para que presenten su manifestación de interés a través de una propuesta técnica y económica, que será evaluada bajo criterios de selección claros y precisos, basados en la metodología de análisis de calidad-costo. En ese sentido, el presente procedimiento no requiere la presentación de documentación legales ni financieros.

La normativa aplicable podrá ser consultada en la siguiente dirección web: https://portal.modernizacion.gob.sv/#/home.

B. FASES DEL PROCESO ADMINISTRATIVO

En cumplimiento a lo establecido en el numeral 4 "Procedimiento en caso de financiamiento por donación o contratos de préstamos, para la adquisición a través de Licitación Pública Internacional", del romano VIII "Procedimiento Administrativo" del Lineamiento para la Ejecución del Procedimiento Administrativo establecido en la Ley General para la Modernización Digital del Estado, esta Solicitud de Expresión de Interés se realizará la manera siguiente:

1. Publicación del Solicitud de Expresión de Interés: la convocatoria se realizará en medios de comunicación nacionales e internacionales, de manera enunciativa y no limitativa, por medio de prensa escrita y los canales de sus redes sociales oficiales. El documento podrá ser descargado desde la página web oficial del HNES o ingresando al enlace siguiente https://hes.gob.sv/servicios/documentos-procesos-de-compra/, a partir del mismo día de la publicación de su convocatoria.

2. Período de consultas, respuestas y adendas: para consultas deberá remitirlas por escrito, en físico en las instalaciones de la Unidad de Informática y Telecomunicaciones del Hospital Nacional El Salvador, ubicadas en Avenida De La Revolución #222, distrito de San Salvador, San Salvador Centro, San Salvador, El Salvador, C.A. o por correo electrónico a la dirección karen.valles@salud.gob.sv, karla.guzman@salud.gob.sv a más tardar las diez (10:00) horas, Zona horaria de El Salvador (GMT-6), del 7 de septiembre del corriente año. El HNES podrá responder las consultas y realizar adendas al presente documento hasta antes de la hora y fecha establecida para la recepción de propuestas.

3. Recepción de propuestas: será hasta las 15:00 horas, zona horaria de El Salvador (GMT-6), del día 7 de septiembre del corriente año.

4. Evaluación de propuestas: el HNES evaluará las propuestas en un período máximo de cinco (5) días hábiles a partir del siguiente a la fecha de recepción.

5. Plazo de inconformidades: En caso de recibir más de una expresión de interés, los proponentes podrán presentar su escrito de inconformidad de los resultados dentro de dos (2) días hábiles contados a partir del siguiente a la notificación de los mismos.

6. Notificaciones: el HNES notificará a los proponentes el resultado de la evaluación, la admisión y resolución de escrito de inconformidad, cuando aplique, hasta en un plazo máximo de dos (2) días hábiles posteriores la emisión del respectivo acto.

C. SUPLETORIEDAD.

Cualquier aspecto de índole legal, jurisdiccional, administrativo o técnico que no se encuentre regulado en el presente documento será convenido en la respectiva orden de pedido, cuando sea procedente.

D. RESULTADO DE LA EVALUACIÓN.

Una vez evaluadas las propuestas derivadas de la presente Solicitud de Expresión de Interés y habiendo sido finalizado y aprobado el informe respectivo sin que se hubiese recibido escrito de inconformidad o que este haya sido resuelto, el HNES podrá iniciar un procedimiento de contratación bajo la Ley de Compras Públicas y/o Ley de Bolsas de Productos y Servicios, pudiendo generar las invitaciones y/o incluir los proveedores que cumplieron los requisitos técnicos en las listas cortas, según aplique.

En caso de que, la propuesta más favorable provenga de alguno de los sujetos intervinientes en el Convenio de Alianza Estratégica para la Modernización Digital del Estado o que esta sea la única propuesta y haya cumplido con los criterios de evaluación establecidos, el HNES podrá emitir orden de pedido, de conformidad a los establecido en la ley.

El resultado de la evaluación que hace referencia este apartado será notificado a todos los proponentes.

II. CONDICIONES PARTICULARES DEL PROCESO ADMINISTRATIVO DE CONTRATACIÓN.

SERVICIO DE SUMINISTRO, INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN OPERACIÓN DE LA INFRAESTRUCTURA DE RED, CONECTIVIDAD INALÁMBRICA Y SEGURIDAD PERIMETRAL PARA EL PROGRAMA DOCTORSV

TÉRMINOS DE REFERENCIA

1. ANTECEDENTES

El Gobierno de El Salvador, en aras de modernizar el sistema de atención en salud y disminuir la brecha de atención existente, ha desarrollado un sistema de telemedicina a nivel nacional que permitirá dar solución a diversos problemas actuales del sistema de salud público salvadoreño. Así, bajo una mirada integral, el Gobierno prevé disminuir las brechas de acceso igualitario y garantizar la sostenibilidad del sistema de salud, mediante la implementación de una plataforma tecnológica que permita la prestación de servicios de telemedicina, así como el fortalecimiento del capital humano en salud a través de la incorporación de herramientas digitales, la formación continua y especializada, y la modernización de los procesos de atención.

Como parte de esta estrategia, se impulsó una primera etapa orientada a la implementación de un sistema de telemedicina en El Salvador. En el marco de su ejecución, el 13 de noviembre de 2025 fue lanzada la aplicación DoctorSV mediante una estrategia de incorporación progresiva por rangos etarios. Gracias a los beneficios y facilidades que ofrece, la aplicación logró una amplia aceptación y una rápida adopción entre la población.

Posteriormente, se dio continuidad al desarrollo del Programa DoctorSV mediante una segunda fase, orientada a garantizar su continuidad y sostenibilidad a través del fortalecimiento de su plataforma tecnológica, la consolidación de la red de servicios y la incorporación de capacidades tecnológicas que permitan ampliar la cobertura, mejorar la calidad de la atención y fortalecer el sistema de salud público salvadoreño.

Esta nueva etapa del Programa DoctorSV contempla el fortalecimiento de la infraestructura tecnológica que soporta la operación de la plataforma, incorporando componentes de conectividad, redes de datos, comunicaciones inalámbricas y seguridad perimetral que permitan garantizar la disponibilidad, continuidad operativa, seguridad de la información y escalabilidad de los servicios digitales prestados a la población. Asimismo, busca establecer una infraestructura moderna, resiliente y de alto desempeño que permita soportar el crecimiento sostenido de usuarios, el intercambio seguro de información clínica y la incorporación de nuevas funcionalidades basadas en tecnologías emergentes.

En ese contexto, el crecimiento sostenido en la utilización de DoctorSV ha incrementado la demanda sobre la infraestructura tecnológica que soporta la operación del programa, haciendo necesario fortalecer la capacidad de conectividad, disponibilidad y seguridad de las redes institucionales. La implementación de una infraestructura de comunicaciones moderna constituye un elemento

estratégico para garantizar la continuidad de los servicios de telemedicina, la integración de las diferentes sedes operativas y el funcionamiento eficiente de los componentes tecnológicos que conforman el ecosistema DoctorSV.

En ese sentido, el presente proceso de contratación tiene como finalidad el suministro, instalación, configuración y puesta en operación de la infraestructura de red, conectividad inalámbrica y seguridad perimetral para el Programa DoctorSV, mediante la adquisición e implementación de equipos de red, plataformas de conectividad inalámbrica, soluciones de switching, protección inalámbrica, firewalls de nueva generación y demás componentes necesarios para fortalecer la infraestructura tecnológica que soporta la operación del programa.

El presente proceso de contratación contribuye al fortalecimiento de la infraestructura digital y tecnológica de DoctorSV, necesaria para garantizar la continuidad, disponibilidad, seguridad y crecimiento del Programa, así como la prestación oportuna y confiable de los servicios de telemedicina a la población salvadoreña.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Implementar una infraestructura tecnológica de red, conectividad inalámbrica y seguridad perimetral para el Programa DoctorSV, mediante el suministro, instalación, configuración y puesta en operación de equipos y soluciones especializadas que garanticen la disponibilidad, seguridad, continuidad operativa y escalabilidad de los servicios de telemedicina, fortaleciendo la infraestructura digital que soporta la prestación de servicios de salud a la población.

2.2 OBJETIVOS ESPECÍFICOS

1. Fortalecer la infraestructura de comunicaciones del Programa DoctorSV mediante la implementación de una plataforma de conectividad inalámbrica, switching empresarial y seguridad perimetral que permita soportar la operación de los diferentes componentes tecnológicos del programa con altos niveles de disponibilidad, rendimiento y confiabilidad.

2. Garantizar la protección, integridad y disponibilidad de la información y de los servicios tecnológicos del Programa DoctorSV mediante la incorporación de soluciones de ciberseguridad, monitoreo, administración centralizada y mecanismos de control que permitan reducir riesgos y asegurar la continuidad de la operación.

3. Implementar una infraestructura de red moderna, escalable y administrable que facilite el crecimiento del Programa DoctorSV, permita la incorporación de nuevas sedes y servicios, y proporcione una plataforma tecnológica robusta para la evolución de los servicios digitales y de telemedicina del sistema nacional de salud.

3. ALCANCE DEL SERVICIO

El presente proceso de contratación comprende el suministro, instalación, configuración, integración, pruebas y puesta en operación de la infraestructura de red, conectividad inalámbrica y seguridad perimetral requerida para fortalecer la plataforma tecnológica del Programa DoctorSV, de conformidad con las especificaciones técnicas establecidas en los presentes Términos de Referencia. La solución deberá incorporar todos los equipos, licencias, accesorios y componentes necesarios para garantizar su correcto funcionamiento e integración con la infraestructura tecnológica institucional.

Asimismo, el alcance incluye la implementación de soluciones de conectividad inalámbrica, switching, protección inalámbrica y seguridad perimetral, así como la configuración de los servicios asociados, la realización de pruebas funcionales, la entrega de la documentación técnica correspondiente y la transferencia de conocimiento al personal designado por la institución, con el propósito de asegurar la adecuada administración, operación y mantenimiento de la infraestructura implementada.

La solución deberá garantizar altos niveles de disponibilidad, rendimiento, escalabilidad, continuidad operativa y seguridad de la información, permitiendo soportar el crecimiento del Programa DoctorSV, fortalecer la conectividad entre sus componentes tecnológicos y proporcionar una infraestructura robusta que contribuya a la prestación continua, segura y eficiente de los servicios de telemedicina a la población salvadoreña.

4. ESPECIFICACIONES TÉCNICAS:

A. ESPECIFICACIONES TECNICAS DEL SUMINISTRO

El servicio requerido consiste en:

ítem	Código SINAB	Código ONU	Denominación del bien o servicio	Cantidad
1	81209008	72151605	SERVICIO DE INSTALACION Y CERTIFICACION DE CABLEADO ESTRUCTURADO PARA VOZ Y DATOS	1

Características Técnicas	**PLATAFORMA WIFI** **1.1 Solución de Access Point para la red inalámbrica** ○ **Cantidad: 30 para el segundo nivel** ○ **Cantidad: 20 para el tercer nivel** **1.1.1 Generalidades** • La solución debe encontrarse en el cuadrante de Gartner Wired/Wireless LAN Access Infrastructure en su más reciente edición • La solución debe soportar el estándar IEEE 802.11be (Wi-Fi 7) • La solución debe soportar WPA3 Wi-Fi • La solución debe soportar procesos de visibilidad mediante procesos de ML/AI

	(Machine learning and artificial intelligence) • Debe soportar e incluir administración desde la nube mediante plataforma de gestión centralizada del fabricante • Debe soportar administrarse desde una implementación On-Premises sin requerir cambios de hardware en los puntos de acceso. • Debe permitir generación de contraseñas dinámicas a usuarios invitados y enviarlas por email o mensaje de texto o un medio similar • Toda la solución ofertada debe ser monomarca (con la controladora/sistema de gestión) incluyendo los accesorios de conectividad • Cada Access Point debe soportar al menos 1536 clientes en todos los radios asociados por equipo. • Cada Access Point debe permitir al menos 48 SSID, distribuidos entre los radios inalámbricos. • Debe contar con un sensor dedicado de triple frecuencia para monitoreo permanente del espectro inalámbrico, análisis de interferencias, detección de dispositivos no autorizados y funciones de seguridad, sin utilizar los radios de servicio destinados al tráfico de usuarios. • Se debe de incluir kit de montaje de equipos. • La solución debe estar en capacidad de validar el estado de la red mediante herramientas de monitoreo en tiempo real e histórico, proporcionando visibilidad de clientes, dispositivos y eventos de conectividad. • La solución debe permitir la identificación y resolución proactiva de incidentes mediante herramientas de diagnóstico integradas. • La solución debe operar en arquitectura de Nube que garantice disponibilidades superiores al 99.995% • La solución debe permitir el monitoreo y administración centralizada de puntos de acceso, switches y dispositivos de red desde una única plataforma de gestión. • La solución debe contar con herramientas de localización con características como: Detectar la ubicación de un dispositivo Rastreo de la ubicación de un dispositivo Conteo de dispositivos por ubicación • Debe soportar funcionalidades de acceso para usuarios invitados (Guest Access). • Debe soportar servicios de autenticación mediante servidor RADIUS o proxy RADIUS. • Debe soportar funcionalidades de servidor DHCP. • Debe proporcionar una vista centralizada de todos los objetos de configuración de la red. • Debe permitir la programación de actualizaciones de firmware. • Capacidad para editar en masa las propiedades de los dispositivos • Posibilidad de programar la actualización del firmware. • Debe proporcionar acceso remoto a la interfaz de línea de comandos (CLI) de los dispositivos administrados. • Debe soportar integración con Microsoft Active Directory y servicios LDAP. • Debe soportar IPv4 e IPv6. • Debe permitir la configuración de servidores Syslog y SNMP. • Debe soportar aprovisionamiento automático (Auto-Provisioning). • Debe soportar auditoría de configuraciones, respaldo, restauración, importación y exportación de configuraciones. • Debe soportar generación de reportes históricos relacionados con eventos de seguridad inalámbrica y sistemas de prevención de intrusiones inalámbricas (WIPS). • Debe incorporar Trusted Platform Module (TPM) para protección criptográfica basada en hardware y almacenamiento seguro de credenciales.

- Debe soportar tecnologías IoT integradas mediante Bluetooth Low Energy (BLE), Zigbee y Thread.
- Debe soportar funcionalidades Zero Trust Network Access (ZTNA) e integración con arquitecturas de acceso seguro.

1.1.2 Especificación de radios

La solución debe soportar como mínimo siguiente:

• Debe soportar operación en las bandas de frecuencia:

2.4 GHz a 2.5 GHz.

5.150 GHz a 5.850 GHz.

5.925 GHz a 7.125 GHz.

• Modos de operación inalámbrica compatibles:

Debe soportar IEEE 802.11a en banda de 5 GHz utilizando modulación OFDM.

Debe soportar IEEE 802.11b en banda de 2.4 GHz utilizando modulación DSSS.

Debe soportar IEEE 802.11g en banda de 2.4 GHz utilizando modulación OFDM.

Debe soportar IEEE 802.11n en bandas de 2.4 GHz y 5 GHz.

Debe soportar IEEE 802.11ac en banda de 5 GHz.

Debe soportar IEEE 802.11ax en bandas de 2.4 GHz, 5 GHz y 6 GHz utilizando acceso múltiple por división de frecuencia ortogonal (OFDMA).

Debe soportar IEEE 802.11be (Wi-Fi 7) en bandas de 2.4 GHz, 5 GHz y 6 GHz.

•La solución deberá soportar las siguientes tecnologías de modulación:

Debe soportar tecnologías de modulación y codificación definidas por los estándares IEEE 802.11a/b/g/n/ac/ax/be.

802.11 Legacy a/b/g

Soportar tecnologías de modulación DSSS y OFDM para los estándares IEEE 802.11a/b/g, permitiendo velocidades de transmisión desde 1 Mbps hasta 54 Mbps.

Debe soportar modulación 4096-QAM (4K-QAM) para maximizar el rendimiento inalámbrico en entornos Wi-Fi 7.

•La solución deberá soportar los siguientes estándares y funcionalidades inalámbricas:

Debe soportar MU-MIMO.

Debe soportar Beamforming (TxBF).

Debe soportar FCC CFR 47 part 15 Class B (USA)

Debe soportar ICES-003 Class B (Canada)

Debe soportar EN 55032 Class B

Debe soportar EN 55035

Debe soportar EN 55011

Debe soportar EN 60601-1-2

Debe soportar EN 61000-3-2: (Harmonics)

Debe soportar EN 61000-3-3 (Flicker)

Debe soportar 2014/30/EU EMC Directive

Debe soportar CISPR 32 Class B (International Emissions)

Debe soportar CISPR 11

Debe soportar AS/NZS CISPR32

Debe soportar CISPR 35 (International Immunity)

•La solución deberá incorporar un punto de acceso con arquitectura de doble radio programable, permitiendo la operación simultánea en bandas de 2.4 GHz y 5 GHz o en modo dual 5 GHz.

•Los radios deberán soportar los estándares IEEE 802.11a/b/g/n/ac/ax con tecnología 4x4:4 MIMO

•Canales de hasta 160 MHz y modulación 1024-QAM para maximizar el rendimiento inalámbrico.

•Deberá incluir un radio Bluetooth integrado para servicios IoT, localización y

•Debe soportar CCF (Cellular Coexistance Filter)

1.1.3 Interfaces

La solución debe contar con mínimo:

- 2 puertos Ethernet RJ45 integrados.
- 1 interfaz Ethernet Multigigabit con velocidades de 100/1000/2500/5000/10000 Mbps con detección automática de velocidad.
- 1 interfaz Ethernet Multigigabit con velocidades de 100/1000/2500/5000 Mbps con detección automática de velocidad.
- Debe soportar alimentación PoE mediante la interfaz Ethernet principal.
- Debe soportar alimentación PoE mediante la interfaz Ethernet secundaria.
- Debe soportar funcionalidad PoE Failover para garantizar continuidad operativa ante fallas de alimentación.
- Debe soportar funcionalidad PSE (PoE Out) a través de la segunda interfaz Ethernet.
- Debe soportar IEEE 802.3az Energy Efficient Ethernet (EEE).
- Debe contar con un puerto USB 2.0 Tipo A.
- El puerto USB deberá proporcionar alimentación de 5V / 500 mA cuando opere mediante IEEE 802.3at.
- El puerto USB deberá proporcionar alimentación de 5V / 1000 mA cuando opere mediante IEEE 802.3bt.

1.1.4 Especificaciones de corriente

- Debe soportar alimentación mediante Power over Ethernet (PoE).
- Debe ser compatible con el estándar IEEE 802.3at PoE.
- Debe ser compatible con el estándar IEEE 802.3bt PoE.
- Debe soportar alimentación mediante fuente de corriente continua (DC) de 12V / 3A.
- Debe priorizar la alimentación mediante corriente continua (DC) cuando existan simultáneamente fuentes de alimentación DC y PoE.
- Debe presentar un consumo típico de 21 W y un consumo máximo de 25.5 W cuando opere mediante IEEE 802.3at PoE sin utilizar PoE Out ni puerto USB.
- Debe presentar un consumo típico de 28 W cuando opere mediante IEEE 802.3bt

PoE.

- Debe presentar un consumo máximo de 33.6 W cuando opere mediante IEEE 802.3bt PoE sin utilización del puerto USB.

1.1.5 Antenas

La solución debe contar como mínimo con las siguientes antenas:

- Cuatro (4) antenas dual band para operación en las bandas de 2.4 GHz y 5 GHz.
- Cuatro (4) antenas dedicadas para operación en la banda de 6 GHz.
- Dos (2) antenas dedicadas para el sensor de monitoreo en bandas de 5 GHz y 6 GHz.
- Tres (3) antenas dedicadas para servicios IoT.
- Debe incorporar antenas dedicadas para el sensor de monitoreo de espectro inalámbrico.
- Debe incorporar antenas dedicadas para servicios IoT mediante Bluetooth Low Energy (BLE), Zigbee y Thread.
- Debe permitir la operación simultánea de radios de datos, sensor de seguridad y radios IoT sin degradar el desempeño de la red inalámbrica.

1.1.6 Ganancia

La solución debe contar con una ganancia mínima de antena de:

- 2.4 GHz: 3.2 dBi.
- 5 GHz: 5.1 dBi.
- 6 GHz: 6.0 dBi.
- Radios IoT (Bluetooth, Zigbee y Thread): 4.2 dBi.

Debe soportar operación simultánea en bandas de 2.4 GHz, 5 GHz y 6 GHz mediante antenas integradas de alto desempeño.

1.1.7 Cumplimiento de normativa

Los equipos ofertados deben cumplir con al menos una norma de cuidado del medio ambiente y/o manejo eficiente de energía.

Debe cumplir con las siguientes normativas ambientales:

- EU RoHS 2011/65/EU y sus enmiendas (EU) 2015/863.
- EU WEEE 2012/19/EU.
- EU REACH Regulation (EC) No. 1907/2006.
- EU SCIP Waste Framework Directive.
- China RoHS 2.
- Taiwan RoHS CNS 15663.

El oferente deberá adjuntar ficha técnica oficial del fabricante donde se evidencie el cumplimiento de las normativas ambientales ofertadas.

Cumplimiento Wi-Fi Alliance:

- Debe contar con certificación Wi-Fi CERTIFIED™ 7.
- Debe contar con certificación Wi-Fi CERTIFIED™ 6 Release 2.
- Debe contar con certificación Wi-Fi CERTIFIED™ para los estándares IEEE 802.11a/b/g/n/ac.
- Debe soportar Wi-Fi Enhanced Open™.

- Debe soportar WMM® (Wi-Fi Multimedia).
- Debe soportar Wi-Fi Agile Multiband™.
- Debe soportar Protected Management Frames (PMF).
- Debe soportar WPA™ Enterprise y Personal.
- Debe soportar WPA2™ Enterprise y Personal.
- Debe soportar WPA3™ Enterprise y Personal.

Cumplimiento de seguridad eléctrica:

- Debe cumplir con UL/CUL 62368-1.
- Debe cumplir con certificación CB IEC 62368-1.

Cumplimiento EMC y regulatorio:

- Debe cumplir con FCC CFR 47 Part 15 Class B.
- Debe cumplir con ICES-003 Class B.
- Debe cumplir con EN 55032 Class B.
- Debe cumplir con EN 55035.
- Debe cumplir con la Directiva EMC 2014/30/EU.

Debe cumplir con la Directiva RED 2014/53/EU.

1.1.8 Temperatura de operación

Al menos en los rangos de 0 a 50°C

1.1.9 Carta del fabricante

Se debe de presentar carta del fabricante donde se indique que son proveedores autorizados y con el nivel Diamond en su plan de canales para proveer, instalar y soportas las soluciones tecnologías de dicho fabricante.

1.1.10 Certificaciones tecnicas

El proveedor deberá presentar 2 ingenieros certificados en la solución para la instalación de los equipos, deberá demostrar experiencia en tecnologías FABRIC.

El proveedor deberá ser certificado por la CWNP y deberá presentar 2 certificaciones de sus ingenieros de CWNA, deberá realizar sitesurvey para validación de cobertura, rendimiento, mitigación de interferencias, y dejar la solución funcionando en optimas condición para garantizar la conectividad.

1.1.11 Plazo del servicio y lugar de entrega

El tiempo de entrega de equipos e instalación de los equipos debe de ser en un máximo de 5 días calendario en las instalaciones de DoctorSV.

1.1.12 Garantía de equipos

Se requiren 3 años de garantía

1.2 Solución de protección inalambrica RF

Cantidad: 3 sensores WIPS para el segundo nivel

Cantidad: 5 sensores WIPS para el tercer nivel

1.2.1 Tipo de solución

La solución deberá ser una plataforma dedicada de Wireless Intrusion Prevention System, WIPS, orientada a la protección, monitoreo, detección, prevención y cumplimiento de seguridad en redes WLAN empresariales.

1.2.2 Arquitectura dedicada WIPS

La solución deberá operar mediante sensores inalámbricos dedicados de tiempo completo para monitoreo del espectro y del tráfico inalámbrico, sin depender exclusivamente de puntos de acceso en modo compartido o radio-share.

1.2.3 Producto de referencia

Se tomará como referencia funcional y técnica una solución tipo WIPS dedicado o equivalente superior, debiendo cumplir como mínimo con las capacidades descritas en estos términos de referencia.

1.2.4 Operación 24x7x365

La solución deberá monitorear de forma continua el ambiente inalámbrico las 24 horas del día, los 7 días de la semana, durante todo el año, para identificar amenazas, ataques, dispositivos no autorizados y violaciones de política.

1.2.5 Componentes de la solución

La solución deberá estar compuesta, como mínimo, por sensores inalámbricos dedicados y una plataforma central de seguridad tipo appliance físico, appliance virtual o plataforma equivalente de gestión centralizada.

1.2.6 Sensores dedicados

Los sensores deberán poder operar en modo dedicado full-time para escaneo permanente del aire, detección de amenazas, captura de tráfico, análisis de eventos y localización de dispositivos sospechosos o no autorizados.

1.2.7 No afectación del servicio WLAN

La función WIPS dedicada no deberá degradar el servicio de datos de los usuarios WLAN, por lo que el monitoreo de seguridad deberá realizarse mediante sensores dedicados o radios dedicados al monitoreo.

1.2.8 Modalidad de radio dedicado

En caso de utilizar puntos de acceso de doble o triple radio, la solución deberá permitir dedicar al menos un radio exclusivamente a funciones WIPS, manteniendo los radios restantes para acceso de clientes WLAN.

1.2.9 Bandas de operación

La solución deberá soportar detección y monitoreo de amenazas en bandas de 2.4 GHz, 5 GHz y, cuando aplique, 6 GHz, incluyendo identificación de dispositivos, clientes, puntos de acceso y rogues en dichas bandas.

1.2.10 Estándares inalámbricos soportados

Los sensores deberán soportar monitoreo de redes y dispositivos compatibles con estándares IEEE 802.11a/b/g/n/ac/ax o superiores disponibles al momento de la implementación.

1.2.11 Detección de amenazas inalámbricas

La solución deberá incluir una biblioteca amplia y actualizable de amenazas inalámbricas, capaz de identificar ataques conocidos, comportamientos anómalos, vulnerabilidades, dispositivos no autorizados y actividad sospechosa.

1.2.12 Detección en tiempo real

La plataforma deberá detectar amenazas y eventos de seguridad inalámbrica en tiempo real, generando alarmas y notificaciones inmediatas al personal autorizado.

1.2.13 Detección de amenazas día cero

La solución deberá analizar actividad actual contra información histórica y patrones de comportamiento para detectar amenazas existentes, amenazas emergentes y comportamientos anómalos asociados a posibles ataques día cero.

1.2.14 Correlación centralizada

La plataforma deberá agregar y correlacionar información proveniente de múltiples sensores para mejorar la precisión de detección, reducir falsos positivos y consolidar eventos relacionados.

1.2.15 Reducción de falsos positivos

La solución deberá contar con mecanismos de detección contextual, correlación multidimensional y análisis histórico para minimizar alarmas falsas y priorizar eventos reales de riesgo.

1.2.16 Detección de rogue AP

La solución deberá detectar puntos de acceso no autorizados, diferenciando entre dispositivos vecinos, dispositivos externos y verdaderos rogue AP conectados a la red cableada de la organización.

1.2.17 Detección de rogue clients

La solución deberá detectar clientes inalámbricos no autorizados, sospechosos o asociados a dispositivos rogue, incluyendo clientes que operen en ambientes con mecanismos de protección de administración de tramas.

1.2.18 Mitigación automática de rogues

La solución deberá permitir la contención o terminación automática de dispositivos rogue mediante técnicas inalámbricas de air-termination, bloqueo por ACL, identificación del puerto de switch asociado o mecanismo equivalente.

1.2.19 Respuesta basada en políticas

La plataforma deberá permitir definir políticas de seguridad inalámbrica y asociar acciones automáticas ante violaciones, tales como notificación, generación de alarma, syslog, SNMP trap, captura remota de paquetes o análisis de espectro.

1.2.20 Gestión de políticas

La solución deberá incluir una consola central para creación, administración, aplicación y auditoría de políticas de seguridad WIPS por sitio, grupo, edificio, piso, zona, SSID, dispositivo o criterio equivalente.

1.2.21 Localización de rogues

La solución deberá permitir localizar puntos de acceso y clientes rogue sobre planos de piso o mapas de ubicación, facilitando su identificación física y desconexión por parte del personal de TI o seguridad.

1.2.22 Consola centralizada

La solución deberá proveer una consola gráfica centralizada para monitoreo, administración, correlación de eventos, visualización de alarmas, reportes, análisis forense, configuración de sensores y gestión de políticas.

1.2.23 Escalabilidad

La arquitectura deberá ser escalable para soportar múltiples sensores, múltiples sitios, crecimiento de dispositivos inalámbricos, alta densidad de clientes e incremento de dispositivos IoT, manteniendo una gestión centralizada.

1.2.24 Procesamiento distribuido

La solución deberá permitir que parte del análisis de paquetes sea realizado en los sensores, enviando a la plataforma central únicamente la información de seguridad necesaria para optimizar el consumo de ancho de banda.

1.2.25 Implementación multisede

La solución deberá soportar despliegues centralizados o distribuidos en múltiples sedes, con comunicación segura entre sensores remotos y la plataforma central a través de LAN, WAN o VPN.

1.2.26 Appliance virtual

La solución deberá soportar despliegue como appliance virtual sobre plataforma de virtualización empresarial, o appliance físico equivalente, según la arquitectura propuesta por el fabricante.

1.2.27 Alta disponibilidad

La solución deberá permitir una arquitectura resiliente o de alta disponibilidad para la plataforma de gestión y análisis WIPS, evitando puntos únicos de falla en ambientes críticos.

1.2.28 Plug and play

La solución deberá permitir incorporación simplificada de sensores, descubrimiento, registro y puesta en operación rápida, reduciendo tiempos de implementación y configuración inicial.

1.2.29 Forense inalámbrico

La solución deberá incluir capacidades de análisis forense inalámbrico para investigar eventos pasados, revisar actividad histórica de dispositivos, asociaciones, tráfico, roaming, canales y comportamiento durante intervalos específicos.

1.2.30 Retención de datos forenses

La solución deberá almacenar información histórica granular por dispositivo inalámbrico identificado, permitiendo análisis posterior de incidentes, auditorías, cumplimiento y solución de problemas.

1.2.31 Análisis histórico por dispositivo

La solución deberá permitir consultar la actividad de un dispositivo sospechoso durante periodos prolongados, incluyendo detalle por intervalos de tiempo, asociaciones, tráfico, ubicación, canal, señal y eventos relevantes.

1.2.32 Evidencia para auditoría

La plataforma deberá generar evidencia técnica de incidentes, ventanas de exposición, actividad de clientes, tráfico intercambiado, asociaciones a AP, destinos de comunicación y horarios de ocurrencia.

1.2.33 Reportería

La solución deberá incluir reportes predefinidos de seguridad, infraestructura, inventario, cumplimiento, amenazas, rogues, políticas y estado de sensores.

1.2.34 Reportes personalizados

La solución deberá permitir crear reportes personalizados seleccionando campos de la base de datos o repositorio de eventos, con posibilidad de reutilización futura.

1.2.35 Cumplimiento normativo

La solución deberá facilitar el cumplimiento y generación de evidencia para marcos regulatorios o de buenas prácticas tales como PCI DSS, HIPAA, GLBA, SOX u otros aplicables a la entidad contratante.

1.2.36 Evaluación de vulnerabilidades inalámbricas

La solución deberá incluir o soportar un módulo de evaluación de vulnerabilidades inalámbricas que permita realizar pruebas remotas desde la perspectiva de un atacante inalámbrico.

1.2.37 Pruebas automáticas y bajo demanda

El módulo de evaluación de vulnerabilidades deberá permitir ejecutar pruebas

programadas automáticamente o bajo demanda, sin requerir desplazamiento físico recurrente a cada sede.

1.2.38 Pruebas de penetración inalámbrica remota

La solución deberá permitir que los sensores ejecuten pruebas controladas de seguridad inalámbrica para identificar configuraciones débiles, accesos indebidos, rutas de entrada no autorizadas o exposición hacia activos cableados.

1.2.39 Validación de políticas de red

La solución deberá permitir validar políticas de firewall, switching, segmentación y acceso desde la perspectiva inalámbrica, identificando posibles caminos no autorizados hacia la red cableada.

1.2.40 Listas negras y control de objetivos

La solución deberá permitir definir listas negras, listas permitidas o criterios equivalentes para evaluar redes, dispositivos, destinos o activos que deban ser bloqueados, monitoreados o protegidos.

1.2.41 Análisis de espectro

La solución deberá incluir capacidades de análisis de espectro para identificar, clasificar y alertar sobre fuentes de interferencia que afecten la red WLAN, usando sensores o infraestructura compatible.

1.2.42 Identificación de interferencias

La solución deberá detectar fuentes de interferencia tales como dispositivos no Wi-Fi, cámaras inalámbricas, teléfonos inalámbricos, microondas u otros elementos que operen en bandas no licenciadas y afecten el desempeño WLAN.

1.2.43 Visualización de espectro

La solución deberá proveer visualizaciones gráficas o espectrogramas en tiempo real para análisis de interferencia, uso de canal, actividad de radiofrecuencia y solución de problemas inalámbricos.

1.2.44 Captura remota de paquetes

La solución deberá permitir convertir un sensor en sniffer remoto para capturar tramas de capa 2 observadas en el aire, con capacidad de análisis desde la consola central.

1.2.45 Exportación PCAP

La solución deberá permitir guardar o exportar capturas de paquetes en formato PCAP o equivalente compatible con herramientas externas de análisis como Wireshark.

1.2.46 Captura simultánea

La solución deberá soportar captura remota simultánea en múltiples sensores, conforme a las capacidades del fabricante, para análisis coordinado de incidentes distribuidos.

1.2.47 Visualizaciones en vivo

La plataforma deberá incluir vistas gráficas de análisis en tiempo real para datos, dispositivos, conexiones, tramas, alarmas, clientes, AP, rogues y eventos de seguridad.

1.2.48 Notificaciones

La solución deberá generar notificaciones automáticas ante eventos críticos mediante correo electrónico, consola, syslog, SNMP trap, integración SIEM o mecanismos equivalentes.

1.2.49 Integración con syslog

La solución deberá soportar envío de eventos y alarmas mediante syslog hacia plataformas externas de monitoreo, correlación o SIEM.

1.2.50 Integración SNMP

La solución deberá soportar generación de traps SNMP o integración equivalente para monitoreo por herramientas de gestión de red.

1.2.51 Alarmas accionables

Cada alarma deberá incluir información suficiente para permitir respuesta operativa, incluyendo tipo de amenaza, severidad, dispositivo involucrado, ubicación, tiempo, sensor que detectó el evento y acción recomendada o ejecutada.

1.2.52 Seguridad WPA3

La solución deberá detectar dispositivos y comportamientos asociados a redes con seguridad WPA3, incluyendo mecanismos basados en SAE o estándares equivalentes.

1.2.53 Detección OWE

La solución deberá detectar dispositivos que utilicen Opportunistic Wireless Encryption (OWE), o mecanismos equivalentes de cifrado oportunista.

1.2.54 Protección en ambientes PMF

La solución deberá soportar detección y contención de clientes rogue en ambientes con Protected Management Frames (PMF), o mecanismos equivalentes de protección de tramas de administración.

1.2.55 Inventario inalámbrico

La solución deberá mantener inventario actualizado de puntos de acceso, clientes, sensores, dispositivos autorizados, dispositivos no autorizados, rogues, SSID, BSSID y demás elementos inalámbricos detectados.

1.2.56 Clasificación de dispositivos

La plataforma deberá clasificar dispositivos inalámbricos como autorizados, vecinos,

sospechosos, rogue, no administrados, clientes, AP, sensores u otras categorías necesarias para análisis de seguridad.

1.2.57 Priorización de riesgos

La solución deberá asignar severidad o criticidad a eventos de seguridad, permitiendo priorizar la atención de incidentes según impacto, tipo de amenaza, ubicación y exposición de red.

1.2.58 Gestión por planos

La solución deberá permitir carga, administración y uso de planos de piso para ubicar sensores, AP, clientes, rogues e incidentes de seguridad inalámbrica.

1.2.59 Auditoría de acciones

La plataforma deberá registrar acciones administrativas, cambios de configuración, creación de políticas, respuestas automáticas, mitigaciones y consultas relevantes para trazabilidad.

1.2.60 Control de acceso administrativo

La solución deberá soportar perfiles de usuario o roles administrativos para separar funciones de monitoreo, administración, auditoría, operación y consulta.

1.2.61 Licenciamiento WIPS

La solución deberá incluir las licencias necesarias para operar las funciones WIPS dedicadas sobre la totalidad de sensores propuestos, incluyendo detección, prevención, políticas, Live View y funcionalidades mínimas descritas.

1.2.62 Licenciamiento de plataforma

La propuesta deberá incluir licencias de virtual appliance, consola, base de datos, sensores, módulos y cualquier otro componente requerido para operación completa, sin costos ocultos para las funcionalidades solicitadas.

1.2.63 Compatibilidad de sensores

Los sensores o puntos de acceso usados como sensores deberán estar soportados oficialmente por el fabricante para la versión propuesta de la solución WIPS.

1.2.64 Administración centralizada de versiones

La solución deberá permitir mantenimiento, actualización y gestión centralizada de la plataforma y sensores conforme a las mejores prácticas del fabricante.

1.2.65 Documentación técnica

El oferente deberá entregar documentación técnica oficial del fabricante que demuestre cumplimiento de los requerimientos, arquitectura propuesta, dimensionamiento, licencias, matriz de compatibilidad y guías de operación.

1.2.66 Capacitación

El oferente deberá incluir capacitación técnica para administradores sobre operación WIPS, gestión de políticas, análisis de alarmas, mitigación de rogues, forense, reportes y solución de problemas.

1.2.67 Transferencia de conocimiento

El oferente deberá realizar transferencia de conocimiento al equipo técnico de la entidad, incluyendo operación diaria, interpretación de eventos, mejores prácticas y procedimientos de respuesta.

1.2.68 Servicios de implementación

El oferente deberá incluir instalación, configuración, integración, carga de planos, definición inicial de políticas, alta de sensores, pruebas funcionales y puesta en producción.

1.2.69 Pruebas de aceptación

La solución deberá superar pruebas de aceptación que validen como mínimo: detección de rogue AP, detección de cliente no autorizado, alarma por violación de política, ubicación en plano, captura remota, reporte, notificación y mitigación controlada.

1.2.70 Garantía y soporte

El oferente deberá incluir soporte técnico, garantía del fabricante, actualizaciones de software, acceso a parches, atención de incidentes y escalamiento durante el periodo contractual definido por la entidad.

1.2.71 Dimensionamiento

El oferente deberá presentar dimensionamiento técnico detallado indicando cantidad de sensores dedicados, cobertura esperada, sedes, bandas monitoreadas, capacidad de procesamiento, almacenamiento histórico y licenciamiento requerido.

1.2.72 Cobertura WIPS

La cobertura WIPS deberá ser diseñada para monitoreo efectivo de las áreas definidas por la entidad, considerando densidad, planos, materiales, interferencia, criticidad de zonas y bandas requeridas.

1.2.73 Criterio de equivalencia

Se aceptarán soluciones equivalentes siempre que demuestren igual o superior cumplimiento funcional, técnico, operativo y de seguridad respecto a los requerimientos de la solución WIPS dedicada especificada.

1.2.74 Exclusión de soluciones no dedicadas

No se aceptarán soluciones que dependan únicamente de funcionalidades básicas WIDS/WIPS embebidas en controladores WLAN o access points de acceso de usuarios sin sensores dedicados o radios dedicados al monitoreo continuo.

1.2.75 Entregables mínimos

El oferente deberá entregar arquitectura final, memoria técnica, matriz de cumplimiento, licencias, configuración respaldada, manual operativo, planos cargados, reporte de pruebas, capacitación y acta de aceptación.

1.2.76 Carta del fabricante

Se debe de presentar carta del fabricante donde se indique que son proveedores autorizados y con el nivel Diamond en su plan de canales para proveer, instalar y soportas las soluciones tecnologías de dicho fabricante.

1.2.77 Certificaciones tecnicas

El proveedor deberá presentar 2 ingenieros certificados en la solución para la instalación de los equipos, deberá demostrar experiencia en tecnologías FABRIC.

El proveedor deberá ser certificado por la CWNP y deberá presentar 2 certificaciones de sus ingenieros de CWNA, deberá realizar sitesurvey para validación de cobertura, rendimiento, mitigación de interferencias, y dejar la solución funcionando en optimas condición para garantizar la conectividad.

1.2.78 Plazo del servicio y lugar de entrega

El tiempo de entrega de equipos e instalación de los equipos debe de ser en un máximo de 5 días calendario en las instalaciones de DoctorSV.

1.3 Solución de Switches de Acceso

- **Cantidad:** 4 Switches de Acceso (2 clúster de 2 switches) para el segundo nivel
- **Cantidad:** 4 Switches de Acceso (2 clúster de 2 switches) para el tercer nivel

1.3.1 Especificaciones técnicas

2 clúster de 2 switches de acceso, según los siguientes requerimientos:

Se debe considerar un cluster de equipo de acceso con las siguientes especificaciones técnicas:

- Debe contar con un mínimo de 48 interfaces Multigigabit Ethernet 100M/1G/2.5G/5G/10GBASE-T.
- Debe soportar operación Full-Duplex en todos los puertos de acceso.
- Debe contar con capacidad PoE IEEE 802.3bt de hasta 90W por puerto.
- Debe soportar alimentación PoE para dispositivos de alta demanda energética.
- Debe contar con 6 puertos SFP28 incluir transceivers de 10Gbps y 25Gbps para interconexiones.
- Debe contar con 2 puertos QSFP28 integrados para stacking de alta velocidad. Incluir transceivers de interconexión 100Gbps.
- Debe soportar una capacidad de stacking de hasta 400 Gbps por unidad.
- Debe soportar funcionalidades de apilamiento (stacking) mediante puertos QSFP28 dedicados.
- Debe contar con un puerto de consola RJ45 para administración local.

	• Debe contar con un puerto USB Micro-B para consola. • Debe contar con un puerto Ethernet dedicado para administración fuera de banda (Out-of-Band Management). • Debe contar con 2 puertos USB Tipo A para administración y almacenamiento externo. • Debe contar con un slot modular VIM (Versatile Interface Module). • Debe soportar cifrado de enlaces mediante MACsec en puertos de acceso y uplinks. • Debe soportar diseño non-blocking wire speed para procesamiento a velocidad de línea. • Debe soportar una capacidad de switching mínima de 1,700 Gbps. • Debe soportar una tasa de reenvío mínima de 1300 Mpps. • Debe soportar una tabla MAC de al menos 294,000 direcciones. • Debe soportar al menos 4,094 VLANs IEEE 802.1Q. • Debe soportar al menos 4,094 VLANs enrutadas. • Debe soportar al menos 172,000 entradas ARP IPv4. • Debe soportar al menos 294,000 rutas IPv4. • Debe soportar al menos 218,000 rutas IPv6. • Debe soportar al menos 110,000 entradas multicast IP. • Debe soportar 8 colas de QoS por puerto. • Debe soportar IEEE 802.3ab 1000BASE-T. • Debe soportar IEEE 802.3bz para velocidades 2.5GBASE-T, 5GBASE-T y 10GBASE-T. • Debe soportar IEEE 802.3ae 10GBASE-X. • Debe soportar IEEE 802.3by 25GBASE-X. • Debe soportar IEEE 802.3ba y IEEE 802.3bm para enlaces de 40GbE y 100GbE. • Debe soportar IEEE 802.3az Energy Efficient Ethernet. • Debe soportar al menos 63 perfiles de políticas (Policy Profiles). • Debe soportar un mínimo de 16,312 reglas únicas de autorización y denegación (permit/deny rules) por switch. • Debe permitir la aplicación de políticas de acceso basadas en perfiles para segmentación y control de tráfico dentro de la infraestructura de red. • Debe permitir realizar el stack de al menos 8 unidades. **1.3.2 Características Generales** • El fabricante de la solución deberá estar ubicado en el cuadrante de Gartner en al menos los últimos dos años. • El equipo deberá gestionarse desde el mismo sistema que la solución inalámbrica. • Debe soportar aprovisionamiento automático (Zero Touch Provisioning). • Debe soportar implementación simplificada mediante Instant Stack. • Debe soportar configuración automática de puertos mediante Instant Port. • Debe soportar incorporación automática y segura de dispositivos mediante Instant Secure Port. • Debe soportar operación bajo arquitectura Fabric. • Debe soportar segmentación de red basada en Fabric Connect. • Debe soportar automatización de servicios de red para simplificar tareas de configuración y operación. • Debe soportar capacidades avanzadas de analítica y visibilidad mediante herramientas de administración centralizada. • Debe soportar operaciones de red asistidas mediante Inteligencia Artificial (AI). • Debe soportar administración local y remota. • Debe soportar actualizaciones centralizadas de firmware y configuraciones. • Debe soportar autenticación y control de acceso basado en políticas. • Debe soportar perfiles de políticas (Policy Profiles).

	• Debe soportar cifrado de tráfico mediante MACsec. • Debe soportar protección de infraestructura mediante mecanismos de seguridad integrados. • Debe soportar arquitectura de alta disponibilidad orientada a entornos empresariales y de misión crítica. • Debe soportar implementación en redes convergentes para servicios de datos, voz, video e IoT. **1.3.3 Administración Centralizada** • Debe contar con una plataforma de administración centralizada basada en la nube para la gestión de switches y puntos de acceso desde una única consola. • Debe permitir el aprovisionamiento automático de dispositivos (Zero Touch Provisioning), reduciendo tiempos de implementación y errores de configuración. • Debe permitir la administración centralizada de políticas de red para múltiples sedes, edificios y pisos. • Debe permitir la incorporación masiva de dispositivos y su despliegue automatizado. • Debe permitir el descubrimiento, monitoreo y administración de dispositivos de terceros desde una única consola de administración. • Debe soportar entornos multivendor mediante una plataforma unificada de monitoreo y gestión. • Debe soportar control de acceso basado en roles (RBAC). • Debe permitir la gestión de usuarios administrativos con diferentes niveles de privilegio. • Debe mantener registros de auditoría (Audit Logs) de cambios realizados en la plataforma. • Debe soportar respaldo y restauración de configuraciones administrativas. • Debe soportar integración mediante API para automatización e integración con sistemas externos. **1.3.4 Monitoreo y Visibilidad** • Debe proporcionar monitoreo unificado en tiempo real del estado de dispositivos, usuarios, alertas y salud de la red. • Debe proporcionar vistas geográficas, lógicas, físicas y de servicios para facilitar la operación y el diagnóstico de la infraestructura. • Debe permitir visualización de mapas RF para diseño, optimización y solución de problemas en redes inalámbricas. • Debe generar alertas en tiempo real con información contextual para facilitar el análisis de causa raíz. **1.3.5 Inteligencia Artificial** • Debe incorporar capacidades de Inteligencia Artificial (IA) conversacional para asistencia operativa y resolución de incidencias. • Debe permitir consultas en lenguaje natural para obtener información de la red y generar reportes. • Debe proporcionar tableros personalizados generados mediante consultas basadas en lenguaje natural. • Debe incorporar asistentes inteligentes para análisis, diagnóstico y recomendaciones operativas. • Debe permitir automatización de flujos de trabajo mediante Inteligencia Artificial.

1.3.6 Carta del fabricante

Se debe de presentar carta del fabricante donde se indique que son proveedores autorizados y con el nivel Diamond en su plan de canales para proveer, instalar y soportas las soluciones tecnologías de dicho fabricante.

1.3.7 Certificaciones tecnicas

El proveedor deberá presentar 2 ingenieros certificados en la solución para la instalación de los equipos, deberá demostrar experiencia en tecnologías FABRIC.

El proveedor deberá ser certificado por la CWNP y deberá presentar 2 certificaciones de sus ingenieros de CWNA, deberá realizar sitesurvey para validación de cobertura, rendimiento, mitigación de interferencias, y dejar la solución funcionando en optimas condición para garantizar la conectividad.

1.3.8 Plazo del servicio y lugar de entrega

El tiempo de entrega de equipos e instalación de los equipos debe de ser en un máximo de 5 días calendario en las instalaciones de DoctorSV.

1.3.9 Garantía de equipos

- Tres (3) años de garantía.

1.4 CLUSTER DE FIREWALL

- **Cantidad: 2 (1 cluster de 2 firewall) para el tercer nivel**

1.4.1 Especificaciones técnicas

1 clúster de 2 Firewalls, según los siguientes requerimientos:

Se debe considerar un cluster de equipo de seguridad con las siguientes especificaciones técnicas:

Especificaciones mínimas:

•FW Throughput (64 bytes) [Gbps]: 70
•Concurrent Sessions (TCP): 7,800,000
•New Sessions/Second (TCP): 500,000
•IPsec VPN Throughput (512 byte) [Gbps]: 55
•Gateway-to-Gateway IPsec VPN Tunnels: 2000
•Client-to-Gateway IPsec VPN Tunnels: 50000
•SSL-VPN Throughput [Gbps]: 3.6
•Concurrent SSL-VPN Users: 5000
•IPS Throughput [Gbps]: 12
•SSL Inspection Throughput (IPS, avg. HTTPS) [Gbps]: 8
•Application Control Throughput (HTTP 64K) [Gbps]: 28
•NGFW Throughput [Gbps]: 10
•Threat Protection Throughput [Gbps]: 9

	•Maximum Number of Switches Supported: 96 •Maximum Number of APs (Total): 512 •Maximum Number of APs (Tunnel Mode): 256 •Virtual Domains (Default): 10 •Virtual Domains (Maximum): 25 •GE Interfaces cobre / Fibras: 18 cobres / 8 SFP Fibras •10GE Interfaces: 8 •Debe incluir almacenamiento interno SSD redundante. •Debe contar con dos (2) unidades SSD internas de 480 GB cada una, para un total de 960 GB de almacenamiento local. •Incluir ocho (8) cables DAC pasivos a 10 GE SFP+ de 3m **1.4.2 Caracteristicas generales** •La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo. •Debe de soportar Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos. •Equipos deben de contar con un año de licenciamiento Enterprise Protection •Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación; •La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7; •Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación; •La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo •Debe soportar configuraciones de alta disponibilidad Active-Active. •Debe soportar configuraciones de alta disponibilidad Active-Passive. •Debe soportar clustering de equipos. •Debe contar con fuentes de poder redundantes hot-swappable. •Debe suministrarse en configuración de clúster de dos equipos. •Debe soportar inspección SSL/TLS incluyendo TLS 1.3. •Debe soportar IPS basado en inteligencia artificial y aprendizaje automático. •Debe soportar control de aplicaciones. •Debe soportar filtrado web y DNS. •Debe soportar protección anti-malware. •Debe soportar prevención de amenazas de día cero (Zero-Day Protection). •Debe soportar Data Loss Prevention (DLP). •Debe soportar capacidades de Zero Trust Network Access (ZTNA). •Debe soportar segmentación dinámica de red. •Debe soportar SD-WAN segura integrada.

	•Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding; •Los dispositivos de protección de red deben soportar DHCP Relay; •Los dispositivos de protección de red deben soportar DHCP Server; •Los dispositivos de protección de red deben soportar sFlow; •Los dispositivos de protección de red deben soportar Jumbo Frames; •Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas; •Debe ser compatible con NAT dinámica (varios-a-1); •Debe ser compatible con NAT dinámica (muchos-a-muchos); •Debe soportar NAT estática (1-a-1); •Debe soportar el balanceo de enlace hash por IP de origen; •Debe soportar el balanceo de enlace por hash de IP de origen y destino; •Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red; •Enviar logs a sistemas de gestión externos simultáneamente; •Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP); •Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3); •Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico; •Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico; •Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas; •La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad **1.4.3 Carta de fabricante** Se debe de presentar carta del fabricante donde se indique que son proveedores autorizados y con el nivel EXPERT e INTEGRATOR MSSP en su plan de canales para proveer, instalar y soportas las soluciones tecnologías de dicho fabricante. **1.4.4 Certificaciones tecnicas** El proveedor deberá presentar 3 ingenieros certificados en la solución para la instalación de los equipos, deberá demostrar experiencia en las tecnologías ofertadas con las siguientes certificaciones: • FCP NETWORK SECURITY -- 2x • FCSS NETWORK SECURITY -- 3x • FCP SECURITY OPERATION -- 1x • FCSS SECURITY OPERATION -- 1x • FCSS PUBLIC CLOUD SECURITY -- 1x • EC-COUNCIL SOC ANALYST -- 2x • EC-COUNCIL INCIDENT HANDLER -- 2x • FCSS SASE -- 2x El proveedor deberá ser certificado por la CWNP y deberá presentar 2 certificaciones de

	sus ingenieros de CWNA. **1.4.5 Plazo del servicio y lugar de entrega** El tiempo de entrega de equipos e instalación de los equipos debe de ser en un máximo de 5 días calendario en las instalaciones de DoctorSV. **1.4.6 Garantía** Un (1) año de garantía
Servicios	La empresa deberá contemplar todos los accesorios, elementos e insumos necesarios para la instalación de los equipos.
Monitoreo	El proveedor deberá brindar el servicio de monitoreo NOC para los equipos ofertados, debe poseer su propio NOC de forma local y con capacidad redundante a nivel energético, de infraestructura de red y proveedores de servicio de internet para brindar un nivel de tolerancia a fallas, así mismo se requiere que posea personal certificado al menos 2 ingenieros como EC-COUNCIL SOC ANALYST y 1 ingeniero como EC-COUNCIL INCIDENT HANDLER, se realizará visita para constatar cumplimiento.
Soporte técnico local	El proveedor deberá de brindar servicio de soporte técnico local en modalidad 24x7x365, el servicio puede ser brindado remoto o presencial de acuerdo al nivel de criticidad de la falla reportada.
Documentación técnica	Se debe de presentar toda la documentación técnica que respalde las especificaciones de los equipos ofertados.
Carta de Fabricante	De conformidad a especificaciones técnicas de los bienes y servicios detalladas en el presente documento.
Certificaciones técnicas	De conformidad a especificaciones técnicas de los bienes y servicios detalladas en el presente documento.
Plazo del servicio y lugar de entrega	De conformidad a especificaciones técnicas de los bienes y servicios detalladas en el presente documento.
Garantía	De conformidad a especificaciones técnicas de los bienes y servicios detalladas en el presente documento.

ítem	Código SINAB	Código ONU	Denominación del bien o servicio	Cantidad
2	81209018	83121703	SERVICIO DE INSTALACION DE RED DE AREA LOCAL (LAN)	1

Características Técnicas	**PLATAFORMA WIFI** **1.1 Solución de Access Point para la red inalámbrica** ○ **Cantidad: 55** **1.1.1 Generalidades** • La solución debe encontrarse en el cuadrante de Gartner Wired/Wireless LAN Access Infrastructure en su más reciente edición • La solución debe soportar el estándar IEEE 802.11be (Wi-Fi 7) • La solución debe soportar WPA3 Wi-Fi • La solución debe soportar procesos de visibilidad mediante procesos de ML/AI (Machine learning and artificial intelligence) • Debe soportar e incluir administración desde la nube mediante plataforma de gestión centralizada del fabricante • Debe soportar administrarse desde una implementación On-Premises sin requerir cambios de hardware en los puntos de acceso. • Debe permitir generación de contraseñas dinámicas a usuarios invitados y enviarlas por email o mensaje de texto o un medio similar • Toda la solución ofertada debe ser monomarca (con la controladora/sistema de gestión) incluyendo los accesorios de conectividad • Cada Access Point debe soportar al menos 1536 clientes en todos los radios asociados por equipo. • Cada Access Point debe permitir al menos 48 SSID, distribuidos entre los radios inalámbricos. • Debe contar con un sensor dedicado de triple frecuencia para monitoreo permanente del espectro inalámbrico, análisis de interferencias, detección de dispositivos no autorizados y funciones de seguridad, sin utilizar los radios de servicio destinados al tráfico de usuarios. • Se debe de incluir kit de montaje de equipos. • La solución debe estar en capacidad de validar el estado de la red mediante herramientas de monitoreo en tiempo real e histórico, proporcionando visibilidad de clientes, dispositivos y eventos de conectividad. • La solución debe permitir la identificación y resolución proactiva de incidentes mediante herramientas de diagnóstico integradas. • La solución debe operar en arquitectura de Nube que garantice disponibilidades superiores al 99.995% • La solución debe permitir el monitoreo y administración centralizada de puntos de acceso, switches y dispositivos de red desde una única plataforma de gestión. • La solución debe contar con herramientas de localización con características como: Detectar la ubicación de un dispositivo Rastreo de la ubicación de un dispositivo Conteo de dispositivos por ubicación • Debe soportar funcionalidades de acceso para usuarios invitados (Guest Access). • Debe soportar servicios de autenticación mediante servidor RADIUS o proxy RADIUS. • Debe soportar funcionalidades de servidor DHCP. • Debe proporcionar una vista centralizada de todos los objetos de configuración de

	la red. • Debe permitir la programación de actualizaciones de firmware. • Capacidad para editar en masa las propiedades de los dispositivos • Posibilidad de programar la actualización del firmware. • Debe proporcionar acceso remoto a la interfaz de línea de comandos (CLI) de los dispositivos administrados. • Debe soportar integración con Microsoft Active Directory y servicios LDAP. • Debe soportar IPv4 e IPv6. • Debe permitir la configuración de servidores Syslog y SNMP. • Debe soportar aprovisionamiento automático (Auto-Provisioning). • Debe soportar auditoría de configuraciones, respaldo, restauración, importación y exportación de configuraciones. • Debe soportar generación de reportes históricos relacionados con eventos de seguridad inalámbrica y sistemas de prevención de intrusiones inalámbricas (WIPS). • Debe incorporar Trusted Platform Module (TPM) para protección criptográfica basada en hardware y almacenamiento seguro de credenciales. • Debe soportar tecnologías IoT integradas mediante Bluetooth Low Energy (BLE), Zigbee y Thread. • Debe soportar funcionalidades Zero Trust Network Access (ZTNA) e integración con arquitecturas de acceso seguro. **1.1.2 Especificación de radios** **La solución debe soportar como mínimo siguiente:** • Debe soportar operación en las bandas de frecuencia: 2.4 GHz a 2.5 GHz. 5.150 GHz a 5.850 GHz. 5.925 GHz a 7.125 GHz. • Modos de operación inalámbrica compatibles: Debe soportar IEEE 802.11a en banda de 5 GHz utilizando modulación OFDM. Debe soportar IEEE 802.11b en banda de 2.4 GHz utilizando modulación DSSS. Debe soportar IEEE 802.11g en banda de 2.4 GHz utilizando modulación OFDM. Debe soportar IEEE 802.11n en bandas de 2.4 GHz y 5 GHz. Debe soportar IEEE 802.11ac en banda de 5 GHz. Debe soportar IEEE 802.11ax en bandas de 2.4 GHz, 5 GHz y 6 GHz utilizando acceso múltiple por división de frecuencia ortogonal (OFDMA). Debe soportar IEEE 802.11be (Wi-Fi 7) en bandas de 2.4 GHz, 5 GHz y 6 GHz. •La solución deberá soportar las siguientes tecnologías de modulación: Debe soportar tecnologías de modulación y codificación definidas por los estándares IEEE 802.11a/b/g/n/ac/ax/be. **802.11 Legacy a/b/g** Soportar tecnologías de modulación DSSS y OFDM para los estándares IEEE 802.11a/b/g, permitiendo velocidades de transmisión desde 1 Mbps hasta 54 Mbps.

Debe soportar modulación 4096-QAM (4K-QAM) para maximizar el rendimiento inalámbrico en entornos Wi-Fi 7.

•La solución deberá soportar los siguientes estándares y funcionalidades inalámbricas:

Debe soportar MU-MIMO.

Debe soportar Beamforming (TxBF).

Debe soportar FCC CFR 47 part 15 Class B (USA)

Debe soportar ICES-003 Class B (Canada)

Debe soportar EN 55032 Class B

Debe soportar EN 55035

Debe soportar EN 55011

Debe soportar EN 60601-1-2

Debe soportar EN 61000-3-2: (Harmonics)

Debe soportar EN 61000-3-3 (Flicker)

Debe soportar 2014/30/EU EMC Directive

Debe soportar CISPR 32 Class B (International Emissions)

Debe soportar CISPR 11

Debe soportar AS/NZS CISPR32

Debe soportar CISPR 35 (International Immunity)

•La solución deberá incorporar un punto de acceso con arquitectura de doble radio programable, permitiendo la operación simultánea en bandas de 2.4 GHz y 5 GHz o en modo dual 5 GHz.

•Los radios deberán soportar los estándares IEEE 802.11a/b/g/n/ac/ax con tecnología 4x4:4 MIMO

•Canales de hasta 160 MHz y modulación 1024-QAM para maximizar el rendimiento inalámbrico.

•Deberá incluir un radio Bluetooth integrado para servicios IoT, localización y

•Debe soportar CCF (Cellular Coexistance Filter)

1.1.3 Interfaces

La solución debe contar con mínimo:

- 2 puertos Ethernet RJ45 integrados.
- 1 interfaz Ethernet Multigigabit con velocidades de 100/1000/2500/5000/10000 Mbps con detección automática de velocidad.
- 1 interfaz Ethernet Multigigabit con velocidades de 100/1000/2500/5000 Mbps con detección automática de velocidad.
- Debe soportar alimentación PoE mediante la interfaz Ethernet principal.
- Debe soportar alimentación PoE mediante la interfaz Ethernet secundaria.
- Debe soportar funcionalidad PoE Failover para garantizar continuidad operativa ante fallas de alimentación.
- Debe soportar funcionalidad PSE (PoE Out) a través de la segunda interfaz Ethernet.
- Debe soportar IEEE 802.3az Energy Efficient Ethernet (EEE).
- Debe contar con un puerto USB 2.0 Tipo A.
- El puerto USB deberá proporcionar alimentación de 5V / 500 mA cuando opere

mediante IEEE 802.3at.

- El puerto USB deberá proporcionar alimentación de 5V / 1000 mA cuando opere mediante IEEE 802.3bt.

1.1.4 Especificaciones de corriente

- Debe soportar alimentación mediante Power over Ethernet (PoE).
- Debe ser compatible con el estándar IEEE 802.3at PoE.
- Debe ser compatible con el estándar IEEE 802.3bt PoE.
- Debe soportar alimentación mediante fuente de corriente continua (DC) de 12V / 3A.
- Debe priorizar la alimentación mediante corriente continua (DC) cuando existan simultáneamente fuentes de alimentación DC y PoE.
- Debe presentar un consumo típico de 21 W y un consumo máximo de 25.5 W cuando opere mediante IEEE 802.3at PoE sin utilizar PoE Out ni puerto USB.
- Debe presentar un consumo típico de 28 W cuando opere mediante IEEE 802.3bt PoE.
- Debe presentar un consumo máximo de 33.6 W cuando opere mediante IEEE 802.3bt PoE sin utilización del puerto USB.

1.1.5 Antenas

La solución debe contar como mínimo con las siguientes antenas:

- Cuatro (4) antenas dual band para operación en las bandas de 2.4 GHz y 5 GHz.
- Cuatro (4) antenas dedicadas para operación en la banda de 6 GHz.
- Dos (2) antenas dedicadas para el sensor de monitoreo en bandas de 5 GHz y 6 GHz.
- Tres (3) antenas dedicadas para servicios IoT.
- Debe incorporar antenas dedicadas para el sensor de monitoreo de espectro inalámbrico.
- Debe incorporar antenas dedicadas para servicios IoT mediante Bluetooth Low Energy (BLE), Zigbee y Thread.
- Debe permitir la operación simultánea de radios de datos, sensor de seguridad y radios IoT sin degradar el desempeño de la red inalámbrica.

1.1.6 Ganancia

La solución debe contar con una ganancia mínima de antena de:

- 2.4 GHz: 3.2 dBi.
- 5 GHz: 5.1 dBi.
- 6 GHz: 6.0 dBi.
- Radios IoT (Bluetooth, Zigbee y Thread): 4.2 dBi.

Debe soportar operación simultánea en bandas de 2.4 GHz, 5 GHz y 6 GHz mediante antenas integradas de alto desempeño.

1.1.7 Cumplimiento de normativa

Los equipos ofertados deben cumplir con al menos una norma de cuidado del medio ambiente y/o manejo eficiente de energía.

Debe cumplir con las siguientes normativas ambientales:

- EU RoHS 2011/65/EU y sus enmiendas (EU) 2015/863.
- EU WEEE 2012/19/EU.

- EU REACH Regulation (EC) No. 1907/2006.
- EU SCIP Waste Framework Directive.
- China RoHS 2.
- Taiwan RoHS CNS 15663.

El oferente deberá adjuntar ficha técnica oficial del fabricante donde se evidencie el cumplimiento de las normativas ambientales ofertadas.

Cumplimiento Wi-Fi Alliance:

- Debe contar con certificación Wi-Fi CERTIFIED™ 7.
- Debe contar con certificación Wi-Fi CERTIFIED™ 6 Release 2.
- Debe contar con certificación Wi-Fi CERTIFIED™ para los estándares IEEE 802.11a/b/g/n/ac.
- Debe soportar Wi-Fi Enhanced Open™.
- Debe soportar WMM® (Wi-Fi Multimedia).
- Debe soportar Wi-Fi Agile Multiband™.
- Debe soportar Protected Management Frames (PMF).
- Debe soportar WPA™ Enterprise y Personal.
- Debe soportar WPA2™ Enterprise y Personal.
- Debe soportar WPA3™ Enterprise y Personal.

Cumplimiento de seguridad eléctrica:

- Debe cumplir con UL/CUL 62368-1.
- Debe cumplir con certificación CB IEC 62368-1.

Cumplimiento EMC y regulatorio:

- Debe cumplir con FCC CFR 47 Part 15 Class B.
- Debe cumplir con ICES-003 Class B.
- Debe cumplir con EN 55032 Class B.
- Debe cumplir con EN 55035.
- Debe cumplir con la Directiva EMC 2014/30/EU.

Debe cumplir con la Directiva RED 2014/53/EU.

1.1.8 Temperatura de operación

Al menos en los rangos de 0 a 50°C

1.1.9 Carta del fabricante

Se debe de presentar carta del fabricante donde se indique que son proveedores autorizados y con el nivel Diamond en su plan de canales para proveer, instalar y soportas las soluciones tecnologías de dicho fabricante.

1.1.10 Certificaciones tecnicas

El proveedor deberá presentar 2 ingenieros certificados en la solución para la instalación de los equipos, deberá demostrar experiencia en tecnologías FABRIC.

El proveedor deberá ser certificado por la CWNP y deberá presentar 2 certificaciones de sus ingenieros de CWNA, deberá realizar sitesurvey para validación de cobertura, rendimiento, mitigación de interferencias, y dejar la solución funcionando en

optimas condición para garantizar la conectividad.

1.1.11 Plazo del servicio y lugar de entrega

El tiempo de entrega de equipos e instalación de los equipos debe de ser en un máximo de 15 días calendario en las instalaciones de DoctorSV.

1.1.1 Garantía de equipos

- Un (1) año de garantía

1.2 Switches Multigiga para Access Point
Cantidad: 3

1.2.1 Especificaciones técnicas

Se deberá considerar el suministro de **tres (3) switches multigiga de 24 puertos**, los cuales deberán cumplir, como mínimo, con las siguientes especificaciones técnicas:

- Debe contar con un mínimo de 24 interfaces RJ45 Multigigabit compatibles con velocidades 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps y 10 Gbps (100M/1G/2.5G/5G/10GBASE-T).
- Debe soportar alimentación IEEE 802.3bt Tipo 4 (90W PoE) en todos los puertos de acceso.
- Debe soportar operación Full-Duplex en todos los puertos Ethernet.
- Debe incorporar soporte de MACsec en los puertos de acceso para cifrado de enlaces Ethernet.
- Debe contar con 2 puertos QSFP28 integrados para funciones de stacking o enlaces de alta velocidad.
- Debe soportar una capacidad de stacking de hasta 400 Gbps por unidad.
- Debe permitir el apilamiento (stacking) de hasta 8 switches.
- Debe contar con un puerto de consola serial RJ45 para administración local.
- Debe contar con un puerto USB Micro-B para consola.
- Debe contar con un puerto Ethernet 10/100/1000 Mbps dedicado para administración fuera de banda (Out-of-Band Management).
- Debe contar con 2 puertos USB Tipo A para administración y almacenamiento externo.
- Debe incorporar 1 slot VIM (Versatile Interface Module) para expansión mediante módulos de interfaces adicionales.
- Debe incorporar 1 slot SSD para soportar funcionalidades de Integrated Application Hosting.
- Debe soportar arquitectura Non-Blocking Wire-Speed para procesamiento de tráfico a velocidad de línea.
- Debe contar con una capacidad de switching de 1,280 Gbps.
- Debe soportar una tasa de reenvío de 952 millones de paquetes por segundo (Mpps).
- Debe soportar una tabla MAC de hasta 294,000 direcciones utilizando Switch Engine.
- Debe soportar hasta 172,000 entradas ARP IPv4.
- Debe soportar hasta 294,000 rutas IPv4.
- Debe soportar hasta 78,000 vecinos IPv6.
- Debe soportar hasta 218,000 rutas IPv6.
- Debe soportar hasta 110,000 entradas IP Multicast.
- Debe soportar listas de control de acceso (ACL) de hasta 38,864 reglas de entrada y

	2,048 reglas de salida bajo Switch Engine. • Debe soportar 8 colas de Calidad de Servicio (QoS) por puerto. • Debe soportar un mínimo de 4,094 VLAN IEEE 802.1Q. • Debe soportar hasta 4,094 VLANs enrutadas. • Debe soportar un mínimo de 63 perfiles de políticas (Policy Profiles). • Debe soportar hasta 16,312 reglas únicas de autorización y denegación (Permit/Deny Rules) por switch. • Debe soportar Extreme Fabric para virtualización, automatización, segmentación y seguridad de la red sin requerir licencias o controladores adicionales. • Debe soportar Extreme Platform ONE Security para la aplicación automática de políticas Zero Trust y segmentación segura de usuarios y dispositivos. • Debe permitir seleccionar el sistema operativo entre Switch Engine (EXOS) y Fabric Engine (VOSS) sobre el mismo hardware (Universal Hardware). • Debe permitir administración local mediante interfaz gráfica Web (GUI) y línea de comandos (CLI). • Debe soportar aprovisionamiento automático mediante Zero Touch Provisioning. • Debe soportar funcionalidades Instant Port, Instant Secure Port e Instant Stack para simplificar la implementación y administración de la infraestructura. • Debe soportar Integrated Application Hosting, permitiendo ejecutar aplicaciones de terceros directamente sobre el switch sin afectar su desempeño. • Debe soportar los estándares IEEE 802.3ab, IEEE 802.3bz, IEEE 802.3bt Tipo 4, IEEE 802.3ae, IEEE 802.3by, IEEE 802.3ba/802.3bm e IEEE 802.3az. **1.2.2 Características Generales** • El fabricante de la solución deberá estar ubicado en el cuadrante de Gartner en al menos los últimos dos años. • El equipo deberá gestionarse desde el mismo sistema que la solución inalámbrica. • Debe soportar aprovisionamiento automático (Zero Touch Provisioning). • Debe soportar implementación simplificada mediante Instant Stack. • Debe soportar configuración automática de puertos mediante Instant Port. • Debe soportar incorporación automática y segura de dispositivos mediante Instant Secure Port. • Debe soportar operación bajo arquitectura Fabric. • Debe soportar segmentación de red basada en Fabric Connect. • Debe soportar automatización de servicios de red para simplificar tareas de configuración y operación. • Debe soportar capacidades avanzadas de analítica y visibilidad mediante herramientas de administración centralizada. • Debe soportar operaciones de red asistidas mediante Inteligencia Artificial (AI). • Debe soportar administración local y remota. • Debe soportar actualizaciones centralizadas de firmware y configuraciones. • Debe soportar autenticación y control de acceso basado en políticas. • Debe soportar perfiles de políticas (Policy Profiles). • Debe soportar cifrado de tráfico mediante MACsec. • Debe soportar protección de infraestructura mediante mecanismos de seguridad integrados. • Debe soportar arquitectura de alta disponibilidad orientada a entornos empresariales y de misión crítica. • Debe soportar implementación en redes convergentes para servicios de datos, voz, video e IoT. **1.2.3 Administración Centralizada**

	• Debe contar con una plataforma de administración centralizada basada en la nube para la gestión de switches y puntos de acceso desde una única consola. • Debe permitir el aprovisionamiento automático de dispositivos (Zero Touch Provisioning), reduciendo tiempos de implementación y errores de configuración. • Debe permitir la administración centralizada de políticas de red para múltiples sedes, edificios y pisos. • Debe permitir la incorporación masiva de dispositivos y su despliegue automatizado. • Debe permitir el descubrimiento, monitoreo y administración de dispositivos de terceros desde una única consola de administración. • Debe soportar entornos multivendor mediante una plataforma unificada de monitoreo y gestión. • Debe soportar control de acceso basado en roles (RBAC). • Debe permitir la gestión de usuarios administrativos con diferentes niveles de privilegio. • Debe mantener registros de auditoría (Audit Logs) de cambios realizados en la plataforma. • Debe soportar respaldo y restauración de configuraciones administrativas. • Debe soportar integración mediante API para automatización e integración con sistemas externos. **1.2.4 Monitoreo y Visibilidad** • Debe proporcionar monitoreo unificado en tiempo real del estado de dispositivos, usuarios, alertas y salud de la red. • Debe proporcionar vistas geográficas, lógicas, físicas y de servicios para facilitar la operación y el diagnóstico de la infraestructura. • Debe permitir visualización de mapas RF para diseño, optimización y solución de problemas en redes inalámbricas. • Debe generar alertas en tiempo real con información contextual para facilitar el análisis de causa raíz. **1.2.5 Inteligencia Artificial** • Debe incorporar capacidades de Inteligencia Artificial (IA) conversacional para asistencia operativa y resolución de incidencias. • Debe permitir consultas en lenguaje natural para obtener información de la red y generar reportes. • Debe proporcionar tableros personalizados generados mediante consultas basadas en lenguaje natural. • Debe incorporar asistentes inteligentes para análisis, diagnóstico y recomendaciones operativas. • Debe permitir automatización de flujos de trabajo mediante Inteligencia Artificial. **1.2.6 Carta del fabricante** Se debe de presentar carta del fabricante donde se indique que son proveedores autorizados y con el nivel Diamond en su plan de canales para proveer, instalar y soportas las soluciones tecnologías de dicho fabricante. **1.2.7 Certificaciones tecnicas** El proveedor deberá presentar 2 ingenieros certificados en la solución para la instalación de los equipos, deberá demostrar experiencia en tecnologías FABRIC.

El proveedor deberá ser certificado por la CWNP y deberá presentar 2 certificaciones de sus ingenieros de CWNA, deberá realizar sitesurvey para validación de cobertura, rendimiento, mitigación de interferencias, y dejar la solución funcionando en optimas condición para garantizar la conectividad.

1.2.8 Plazo del servicio y lugar de entrega

El tiempo de entrega de equipos e instalación de los equipos debe de ser en un máximo de 15 días calendario en las instalaciones de DoctorSV.

1.2.9 Garantía de equipos

- Un (1) año de garantía.

1.3 Switches de acceso

- **Cantidad: 29**

1.3.1 Especificaciones técnicas

Se debe considerar equipos de 48 puertos con las siguientes especificaciones técnicas:

- Debe contar con un mínimo de 48 interfaces RJ45 10/100/1000BASE-T con detección automática de velocidad y operación Full/Half Duplex.
- Debe soportar alimentación PoE+ IEEE 802.3at de hasta 30W por puerto.
- Debe incorporar soporte de MACsec (IEEE 802.1AE) en todos los puertos de acceso para cifrado de enlaces Ethernet.
- Debe contar con 4 puertos SFP+ de 1/10GbE para enlaces ascendentes (uplinks).
- Debe incorporar 2 puertos SFP-DD para funciones de stacking o enlaces Ethernet de alta velocidad.
- Debe soportar stacking de hasta 8 switches.
- Debe soportar una capacidad de stacking de hasta 80 Gbps por unidad.
- Debe contar con un puerto de consola RJ45 para administración local.
- Debe contar con un puerto USB Micro-B para consola.
- Debe contar con un puerto Ethernet 10/100/1000 Mbps dedicado para administración fuera de banda (Out-of-Band Management).
- Debe contar con 2 puertos USB Tipo A para administración y almacenamiento externo.
- Debe soportar arquitectura Non-Blocking Wire-Speed para procesamiento de tráfico a velocidad de línea.
- Debe contar con una capacidad de switching de 256 Gbps.
- Debe soportar una tasa de reenvío de 190.5 millones de paquetes por segundo (Mpps).
- Debe soportar una tabla MAC de hasta 32,000 direcciones cuando opere con Switch Engine.
- Debe soportar hasta 16,000 entradas ARP IPv4.
- Debe soportar hasta 12,000 rutas IPv4.
- Debe soportar hasta 6,000 rutas IPv6.
- Debe soportar hasta 6,000 entradas IP Multicast.
- Debe soportar listas de control de acceso (ACL) de hasta 8,000 reglas de entrada y 1,024 reglas de salida.
- Debe soportar 8 colas de Calidad de Servicio (QoS) por puerto.

	• Debe soportar un mínimo de 4,094 VLAN IEEE 802.1Q. • Debe soportar hasta 1,533 interfaces IP (Routed VLANs) cuando opere con Switch Engine. • Debe soportar un mínimo de 63 perfiles de políticas (Policy Profiles). • Debe soportar Extreme Fabric para virtualización, automatización, segmentación y seguridad de la red, sin requerir licencias o controladores adicionales. • Debe soportar Extreme Platform ONE Security para la aplicación automática de políticas Zero Trust y segmentación segura de usuarios y dispositivos. • Debe permitir seleccionar el sistema operativo entre Switch Engine (EXOS) y Fabric Engine (VOSS) sobre el mismo hardware (Universal Hardware). • Debe permitir administración mediante interfaz gráfica Web (GUI) y línea de comandos (CLI). • Debe soportar aprovisionamiento automático mediante Zero Touch Provisioning. • Debe soportar funcionalidades Instant Port, Instant Secure Port e Instant Stack para simplificar la implementación y administración de la infraestructura. • Debe soportar Audio Video Bridging (IEEE 802.1 AVB) cuando opere con Switch Engine, permitiendo el transporte de audio y video en tiempo real sobre Ethernet. • Debe soportar los estándares IEEE 802.3ab, IEEE 802.3bz, IEEE 802.3bt Tipo 4, IEEE 802.3ae, IEEE 802.3by e IEEE 802.3az. **1.3.2 Caracteristicas generales** • El fabricante de la solución deberá estar ubicado en el cuadrante de Gartner en al menos los últimos dos años. • El equipo deberá gestionarse desde el mismo sistema que la solución inalámbrica. • Debe soportar aprovisionamiento automático (Zero Touch Provisioning). • Debe soportar implementación simplificada mediante Instant Stack. • Debe soportar configuración automática de puertos mediante Instant Port. • Debe soportar incorporación automática y segura de dispositivos mediante Instant Secure Port. • Debe soportar operación bajo arquitectura Fabric. • Debe soportar segmentación de red basada en Fabric Connect. • Debe soportar automatización de servicios de red para simplificar tareas de configuración y operación. • Debe soportar capacidades avanzadas de analítica y visibilidad mediante herramientas de administración centralizada. • Debe soportar operaciones de red asistidas mediante Inteligencia Artificial (AI). • Debe soportar administración local y remota. • Debe soportar actualizaciones centralizadas de firmware y configuraciones. • Debe soportar autenticación y control de acceso basado en políticas. • Debe soportar perfiles de políticas (Policy Profiles). • Debe soportar cifrado de tráfico mediante MACsec. • Debe soportar protección de infraestructura mediante mecanismos de seguridad integrados. • Debe soportar arquitectura de alta disponibilidad orientada a entornos empresariales y de misión crítica. • Debe soportar implementación en redes convergentes para servicios de datos, voz, video e IoT. **1.3.3 Administración centralizada** • Debe contar con una plataforma de administración centralizada basada en la nube para la gestión de switches y puntos de acceso desde una única consola. • Debe permitir el aprovisionamiento automático de dispositivos (Zero Touch

Provisioning), reduciendo tiempos de implementación y errores de configuración.

- Debe permitir la administración centralizada de políticas de red para múltiples sedes, edificios y pisos.
- Debe permitir la incorporación masiva de dispositivos y su despliegue automatizado.
- Debe permitir el descubrimiento, monitoreo y administración de dispositivos de terceros desde una única consola de administración.
- Debe soportar entornos multivendor mediante una plataforma unificada de monitoreo y gestión.
- Debe soportar control de acceso basado en roles (RBAC).
- Debe permitir la gestión de usuarios administrativos con diferentes niveles de privilegio.
- Debe mantener registros de auditoría (Audit Logs) de cambios realizados en la plataforma.
- Debe soportar respaldo y restauración de configuraciones administrativas.
- Debe soportar integración mediante API para automatización e integración con sistemas externos.

1.3.4 Monitoreo y visbilidad

- Debe proporcionar monitoreo unificado en tiempo real del estado de dispositivos, usuarios, alertas y salud de la red.
- Debe proporcionar vistas geográficas, lógicas, físicas y de servicios para facilitar la operación y el diagnóstico de la infraestructura.
- Debe permitir visualización de mapas RF para diseño, optimización y solución de problemas en redes inalámbricas.
- Debe generar alertas en tiempo real con información contextual para facilitar el análisis de causa raíz.

1.3.5 Inteligencia artificial

- Debe incorporar capacidades de Inteligencia Artificial (IA) conversacional para asistencia operativa y resolución de incidencias.
- Debe permitir consultas en lenguaje natural para obtener información de la red y generar reportes.
- Debe proporcionar tableros personalizados generados mediante consultas basadas en lenguaje natural.
- Debe incorporar asistentes inteligentes para análisis, diagnóstico y recomendaciones operativas.
- Debe permitir automatización de flujos de trabajo mediante Inteligencia Artificial.

1.3.6 Carta del fabricante

Se debe de presentar carta del fabricante donde se indique que son proveedores autorizados y con el nivel Diamond en su plan de canales para proveer, instalar y soportas las soluciones tecnologías de dicho fabricante.

1.3.7 Certificaciones técnicas

El proveedor deberá presentar 2 ingenieros certificados en la solución para la instalación de los equipos, deberá demostrar experiencia en tecnologías FABRIC.

El proveedor deberá ser certificado por la CWNP y deberá presentar 2 certificaciones de sus ingenieros de CWNA, deberá realizar sitesurvey para validación de cobertura,

rendimiento, mitigación de interferencias, y dejar la solución funcionando en optimas condición para garantizar la conectividad.

1.3.8 Plazo del servicio y lugar de entrega

El tiempo de entrega de equipos e instalación de los equipos debe de ser en un máximo de 15 días calendario en las instalaciones de DoctorSV.

1.3.9 Garantía

Un (1) año de garantía.

1.4 CLUSTER DE FIREWALL

- **Cantidad: 2 (1 cluster de 2 firewall) para nivel 5 – nivel 8**

1.4.1 Especificaciones técnicas

1 clúster de 2 Firewalls, según los siguientes requerimientos:

- Debe contar con 16 interfaces Gigabit Ethernet RJ45 aceleradas por hardware.
- Debe contar con 8 interfaces Gigabit Ethernet SFP aceleradas por hardware.
- Debe contar con 4 interfaces 10GE SFP+/GE SFP aceleradas por hardware.
- Debe contar con 4 interfaces 25GE SFP28, compatibles con 10GE SFP+, aceleradas por hardware y de ultra baja latencia (ULL).
- Debe contar con 1 puerto dedicado HA de 2.5GE/GE RJ45.
- Debe contar con 1 puerto de administración Gigabit Ethernet RJ45 dedicado.
- Debe contar con 2 puertos USB Host y 2 puertos USB Client.
- Debe contar con 1 puerto de consola para administración local.
- Debe incorporar dos (2) unidades SSD internas de 480 GB, para un total de 960 GB de almacenamiento local.
- Debe contar con fuentes de alimentación redundantes Hot-Swap instaladas de fábrica.
- Debe instalarse en gabinete estándar de 19 pulgadas, ocupando 1RU de espacio.
- Debe proporcionar un rendimiento de Firewall IPv4 de 153 Gbps (paquetes de 64 bytes).
- Debe soportar un rendimiento Firewall IPv6 de hasta 153 Gbps.
- Debe soportar un rendimiento de IPS de hasta 42 Gbps.
- Debe soportar un rendimiento NGFW de hasta 31 Gbps.
- Debe soportar un rendimiento de Threat Protection de hasta 30 Gbps.
- Debe soportar un rendimiento de Control de Aplicaciones de hasta 74.8 Gbps.
- Debe soportar un rendimiento de Inspección SSL (HTTPS promedio) de hasta 16.7 Gbps.
- Debe soportar un rendimiento de VPN IPsec de hasta 55 Gbps utilizando cifrado AES-256.
- Debe soportar hasta 28 millones de sesiones TCP concurrentes.
- Debe soportar hasta 720,000 nuevas sesiones TCP por segundo.
- Debe soportar un mínimo de 50,000 políticas de firewall.
- Debe soportar hasta 2,000 túneles VPN IPsec Gateway-to-Gateway.
- Debe soportar hasta 50,000 túneles VPN Client-to-Gateway.
- Debe soportar un rendimiento de SSL-VPN de hasta 10 Gbps.
- Debe soportar hasta 10,000 usuarios SSL-VPN concurrentes en modo túnel.
- Debe soportar hasta 18,000 conexiones SSL inspeccionadas por segundo (SSL

	Inspection CPS). • Debe soportar hasta 1.6 millones de sesiones SSL inspeccionadas concurrentemente. • Debe soportar un rendimiento CAPWAP de hasta 133 Gbps. • Debe soportar hasta 10 dominios virtuales (VDOM) por defecto, ampliables hasta 50 VDOMs. • Debe soportar la administración de hasta 196 switches FortiSwitch. • Debe soportar la administración de hasta 2,048 FortiAP, de los cuales 1,024 podrán operar en modo túnel. • Debe soportar hasta 5,000 FortiTokens para autenticación multifactor. • Debe soportar configuraciones de Alta Disponibilidad (HA) en modos Active-Active, Active-Passive y Clustering. **1.4.2 Caracteristicas generales** •La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo. •Debe de soportar Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos. •Equipos deben de contar con un año de licenciamiento Enterprise Protection •Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación; •La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7; •Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación; •La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo •Debe soportar configuraciones de alta disponibilidad Active-Active. •Debe soportar configuraciones de alta disponibilidad Active-Passive. •Debe soportar clustering de equipos. •Debe contar con fuentes de poder redundantes hot-swappable. •Debe suministrarse en configuración de clúster de dos equipos. •Debe soportar inspección SSL/TLS incluyendo TLS 1.3. •Debe soportar IPS basado en inteligencia artificial y aprendizaje automático. •Debe soportar control de aplicaciones. •Debe soportar filtrado web y DNS. •Debe soportar protección anti-malware. •Debe soportar prevención de amenazas de día cero (Zero-Day Protection). •Debe soportar Data Loss Prevention (DLP). •Debe soportar capacidades de Zero Trust Network Access (ZTNA). •Debe soportar segmentación dinámica de red. •Debe soportar SD-WAN segura integrada.

	•Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding; •Los dispositivos de protección de red deben soportar DHCP Relay; •Los dispositivos de protección de red deben soportar DHCP Server; •Los dispositivos de protección de red deben soportar sFlow; •Los dispositivos de protección de red deben soportar Jumbo Frames; •Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas; •Debe ser compatible con NAT dinámica (varios-a-1); •Debe ser compatible con NAT dinámica (muchos-a-muchos); •Debe soportar NAT estática (1-a-1); •Debe soportar el balanceo de enlace hash por IP de origen; •Debe soportar el balanceo de enlace por hash de IP de origen y destino; •Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red; •Enviar logs a sistemas de gestión externos simultáneamente; •Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP); •Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3); •Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico; •Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico; •Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas; •La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad **1.4.3 Carta de fabricante** Se debe de presentar carta del fabricante donde se indique que son proveedores autorizados y con el nivel EXPERT e INTEGRATOR MSSP en su plan de canales para proveer, instalar y soportas las soluciones tecnologías de dicho fabricante. **1.4.4 Certificaciones tecnicas** El proveedor deberá presentar 3 ingenieros certificados en la solución para la instalación de los equipos, deberá demostrar experiencia en las tecnologías ofertadas con las siguientes certificaciones: • FCP NETWORK SECURITY -- 2x • FCSS NETWORK SECURITY -- 3x • FCP SECURITY OPERATION -- 1x • FCSS SECURITY OPERATION -- 1x • FCSS PUBLIC CLOUD SECURITY -- 1x • EC-COUNCIL SOC ANALYST -- 2x • EC-COUNCIL INCIDENT HANDLER -- 2x • FCSS SASE -- 2x El proveedor deberá ser certificado por la CWNP y deberá presentar 2 certificaciones de

sus ingenieros de CWNA.

1.4.5 Plazo del servicio y lugar de entrega

El tiempo de entrega de equipos e instalación de los equipos debe de ser en un máximo de 15 días calendario en las instalaciones de DoctorSV.

1.4.6 Garantía

Un (1) año de garantía

1.5 CLUSTER DE FIREWALL

- **Cantidad: 2 (1 cluster de 2 firewall) para nivel 9**

1.5.1 Especificaciones técnicas

1 clúster de 2 Firewalls, según los siguientes requerimientos:

- Debe contar con 8 interfaces RJ45 Multigigabit compatibles con velocidades 1/2.5/5 Gbps, aceleradas por hardware.
- Debe contar con 16 interfaces Gigabit Ethernet SFP, aceleradas por hardware.
- Debe contar con 4 interfaces 10GE SFP+/GE SFP, configurables como FortiLink o interfaces de datos, aceleradas por hardware.
- Debe contar con 4 interfaces 25GE SFP28, compatibles con módulos 10GE SFP+, aceleradas por hardware.
- Debe contar con 1 puerto dedicado HA de 2.5GE RJ45.
- Debe contar con 1 puerto dedicado de administración GE RJ45.
- Debe contar con 2 puertos USB para funciones de cliente y servidor.
- Debe contar con 1 puerto de consola para administración local.
- Debe incorporar dos (2) unidades SSD internas de 480 GB, para un total de 960 GB de almacenamiento local.
- Debe contar con fuentes de alimentación redundantes AC instaladas de fábrica.
- Debe instalarse en gabinete estándar de 19 pulgadas, ocupando 1RU de espacio.
- Debe proporcionar un rendimiento de Firewall IPv4 de hasta 145 Gbps (paquetes de 64 bytes).
- Debe soportar un rendimiento Firewall IPv6 de hasta 145 Gbps.
- Debe soportar un rendimiento de IPS de hasta 25 Gbps.
- Debe soportar un rendimiento NGFW de hasta 14 Gbps.
- Debe soportar un rendimiento de Threat Protection de hasta 13 Gbps.
- Debe soportar un rendimiento de Control de Aplicaciones de hasta 50 Gbps.
- Debe soportar un rendimiento de Inspección SSL (HTTPS promedio) de hasta 11.5 Gbps.
- Debe soportar un rendimiento de VPN IPsec de hasta 55 Gbps utilizando cifrado AES-256.
- Debe soportar hasta 28 millones de sesiones TCP concurrentes.
- Debe soportar hasta 580,000 nuevas sesiones TCP por segundo.
- Debe soportar un mínimo de 10,000 políticas de firewall.
- Debe soportar hasta 2,000 túneles VPN IPsec Gateway-to-Gateway.
- Debe soportar hasta 50,000 túneles VPN Client-to-Gateway.
- Debe soportar un rendimiento de SSL-VPN de hasta 6.1 Gbps.
- Debe soportar hasta 5,000 usuarios SSL-VPN concurrentes en modo túnel.
- Debe soportar hasta 9,700 conexiones SSL inspeccionadas por segundo (SSL

Inspection CPS).

- Debe soportar hasta 3 millones de sesiones SSL inspeccionadas concurrentemente.
- Debe soportar un rendimiento CAPWAP de hasta 131 Gbps.
- Debe soportar hasta 10 dominios virtuales (VDOM) por defecto, ampliables hasta 50 VDOMs.
- Debe soportar la administración de hasta 96 switches FortiSwitch.
- Debe soportar la administración de hasta 512 FortiAP, de los cuales 256 podrán operar en modo túnel.
- Debe soportar hasta 5,000 FortiTokens para autenticación multifactor.

Debe soportar configuraciones de Alta Disponibilidad (HA) en modos Active-Active, Active-Passive y Clustering

1.5.2 Caracteristicas generales

•La solución debe consistir en una plataforma de protección de Red, basada en un dispositivo con funcionalidades de Firewall de Próxima Generación (NGFW), así como consola de gestión y monitoreo.

•Debe de soportar Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.

•Equipos deben de contar con un año de licenciamiento Enterprise Protection

•Las funcionalidades de protección de red que conforman la plataforma de seguridad, puede ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación;

•La plataforma debe estar optimizada para análisis de contenido de aplicaciones en capa 7;

•Todo el equipo proporcionado debe ser adecuado para montaje en rack de 19 ", incluyendo un rail kit (si sea necesario) y los cables de alimentación;

•La gestión del equipo debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo

•Debe soportar configuraciones de alta disponibilidad Active-Active.

•Debe soportar configuraciones de alta disponibilidad Active-Passive.

•Debe soportar clustering de equipos.

•Debe contar con fuentes de poder redundantes hot-swappable.

•Debe suministrarse en configuración de clúster de dos equipos.

•Debe soportar inspección SSL/TLS incluyendo TLS 1.3.

•Debe soportar IPS basado en inteligencia artificial y aprendizaje automático.

•Debe soportar control de aplicaciones.

•Debe soportar filtrado web y DNS.

•Debe soportar protección anti-malware.

•Debe soportar prevención de amenazas de día cero (Zero-Day Protection).

•Debe soportar Data Loss Prevention (DLP).

•Debe soportar capacidades de Zero Trust Network Access (ZTNA).

•Debe soportar segmentación dinámica de red.

•Debe soportar SD-WAN segura integrada.

•Los dispositivos de protección de red deben soportar Policy based routing y policy

based forwarding;

- Los dispositivos de protección de red deben soportar DHCP Relay;
- Los dispositivos de protección de red deben soportar DHCP Server;
- Los dispositivos de protección de red deben soportar sFlow;
- Los dispositivos de protección de red deben soportar Jumbo Frames;
- Los dispositivos de protección de red deben soportar sub-interfaces Ethernet lógicas;
- Debe ser compatible con NAT dinámica (varios-a-1);
- Debe ser compatible con NAT dinámica (muchos-a-muchos);
- Debe soportar NAT estática (1-a-1);
- Debe soportar el balanceo de enlace hash por IP de origen;
- Debe soportar el balanceo de enlace por hash de IP de origen y destino;
- Debe permitir el monitoreo por SNMP de fallas de hardware, uso de recursos por gran número de sesiones, conexiones por segundo, cantidad de túneles establecidos en la VPN, CPU, memoria, estado del clúster, ataques y estadísticas de uso de las interfaces de red;
- Enviar logs a sistemas de gestión externos simultáneamente;
- Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP);
- Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3);
- Debe soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico;
- Debe soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico;
- Debe soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas;
- La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad

1.5.3 Carta de fabricante

Se debe de presentar carta del fabricante donde se indique que son proveedores autorizados y con el nivel EXPERT e INTEGRATOR MSSP en su plan de canales para proveer, instalar y soportas las soluciones tecnologías de dicho fabricante.

1.5.4 Certificaciones tecnicas

El proveedor deberá presentar 3 ingenieros certificados en la solución para la instalación de los equipos, deberá demostrar experiencia en las tecnologías ofertadas con las siguientes certificaciones:

- FCP NETWORK SECURITY -- 2x
- FCSS NETWORK SECURITY -- 3x
- FCP SECURITY OPERATION -- 1x
- FCSS SECURITY OPERATION -- 1x
- FCSS PUBLIC CLOUD SECURITY -- 1x
- EC-COUNCIL SOC ANALYST -- 2x
- EC-COUNCIL INCIDENT HANDLER -- 2x
- FCSS SASE -- 2x

El proveedor deberá ser certificado por la CWNP y deberá presentar 2 certificaciones de

sus ingenieros de CWNA.

1.5.5 Plazo del servicio y lugar de entrega

El tiempo de entrega de equipos e instalación de los equipos debe de ser en un máximo de 15 días calendario en las instalaciones de DoctorSV.

1.5.6 Garantía

Un (1) año de garantía

1.6 Solución de control de acceso biométrico

Cantidades: Conforme a la siguiente distribución

Nivel	Lectores Biométricos	Licencias Cloud	Botón sin contacto	Kit Z y L	Chapa Magnética	Fuente 12V	Batería 12V	Botón de Emergen
Nivel 5	4	4	4	6	6	4	4	4
Nivel 8	5	5	5	7	7	5	5	5
Nivel 9	4	4	4	6	6	4	4	4

1.6.1 Especificaciones Técnicas

Se deberá considerar el suministro e instalación de una solución de control de acceso biométrico, la cual deberá cumplir como mínimo con las siguientes especificaciones técnicas:

- La solución deberá estar basada en terminales biométricos de reconocimiento facial para control de acceso y registro de asistencia.
- El equipo deberá soportar autenticación mediante reconocimiento facial utilizando algoritmos de Inteligencia Artificial.
- Deberá incluir licencia de administración en la nube con vigencia mínima de un (1) año para la administración, monitoreo y configuración remota de los dispositivos.
- Deberá soportar tarjetas RFID EM de 125 kHz.
- Deberá soportar tarjetas MIFARE de 13.56 MHz.
- Deberá soportar credenciales HID Prox.
- Deberá soportar credenciales HID iCLASS SE/SR.
- Deberá soportar credenciales DESFire.
- Deberá permitir autenticación mediante NFC.
- Deberá permitir autenticación mediante Bluetooth (BLE).
- Deberá permitir autenticación mediante PIN.
- Deberá permitir autenticación mediante códigos QR.
- Deberá soportar una capacidad mínima de 100,000 usuarios.
- Deberá incorporar interfaz Gigabit Ethernet.
- Deberá incorporar conectividad WiFi.
- Deberá soportar alimentación mediante PoE+.
- Deberá contar con protección IP65 para uso en ambientes interiores y exteriores protegidos.

- Deberá incorporar detección de rostro vivo (Live Face Detection).
- Deberá permitir integración con BioStar 2.
- Deberá soportar protocolo OSDP.
- Deberá soportar protocolo Wiegand.
- Deberá soportar RTSP.
- Deberá permitir integración con plataformas empresariales.

1.6.2 Componentes de la solución

La solución deberá incluir como mínimo:

- Licencia de administración en la nube con vigencia de un (1) año.
- Botón de salida sin contacto.
- Kit de montaje tipo Z y L.
- Cerradura electromagnética de 600 libras.
- Fuente de alimentación de 12 Vcc con capacidad de respaldo mediante batería.
- Batería sellada de 12 V.
- Pulsador de emergencia tipo hongo.
- Todos los accesorios necesarios para la correcta instalación y funcionamiento de la solución.

1.6.3 Instalación e implementación

El proveedor deberá contemplar como mínimo:

- Suministro e instalación de lectores biométricos.
- Suministro de licencias de administración en la nube.
- Instalación de cerraduras electromagnéticas.
- Instalación de botones de salida sin contacto.
- Instalación de botones de emergencia.
- Instalación de fuentes de alimentación con respaldo.
- Instalación de baterías.
- Instalación de kits de montaje.
- Suministro e instalación del cableado UTP Categoría 6 requerido para la solución.
- Canalización mediante tubería EMT, canaleta o tecnoducto con todos los accesorios necesarios.
- Configuración de los lectores biométricos.
- Registro de dispositivos en la plataforma de administración.
- Parametrización de credenciales.
- Configuración de reglas básicas de acceso.
- Ejecución de pruebas funcionales para validar la apertura de puertas, generación de eventos y comunicación con la plataforma.
- Entrega de la solución completamente operativa.

1.6.4 Garantía

- Los equipos que conforman la solución de control de acceso biométrico deberán contar con una **garantía mínima de un (1) año** contra defectos de fabricación.
- Durante el período de garantía, el contratista deberá proporcionar soporte técnico, reparación o sustitución de los equipos defectuosos sin costo adicional para la

	institución. • Las licencias de administración en la nube deberán contar con una vigencia mínima de **un (1) año**. **1.6.5 Plazo del servicio y lugar de entrega** El tiempo de entrega de equipos e instalación de los equipos debe de ser en un máximo de 15 días calendario en las instalaciones de DoctorSV.
Servicios	La empresa deberá contemplar todos los accesorios, elementos e insumos necesarios para la instalación de los equipos.
Monitoreo	El proveedor deberá brindar el servicio de monitoreo NOC para los equipos ofertados, debe poseer su propio NOC de forma local y con capacidad redundante a nivel energético, de infraestructura de red y proveedores de servicio de internet para brindar un nivel de tolerancia a fallas, así mismo se requiere que posea personal certificado al menos 2 ingenieros como EC-COUNCIL SOC ANALYST y 1 ingeniero como EC-COUNCIL INCIDENT HANDLER, se realizará visita para constatar cumplimiento (No aplica para la solución de accesos biométricos).
Soporte técnico local	El proveedor deberá de brindar servicio de soporte técnico local en modalidad 24x7x365, el servicio puede ser brindado remoto o presencial de acuerdo al nivel de criticidad de la falla reportada.
Documentación técnica	Se debe de presentar toda la documentación técnica que respalde las especificaciones de los equipos ofertados.
Carta de Fabricante	De conformidad a especificaciones técnicas de los bienes y servicios detalladas en el presente documento.
Certificaciones técnicas	De conformidad a especificaciones técnicas de los bienes y servicios detalladas en el presente documento.
Plazo del servicio y lugar de entrega	De conformidad a especificaciones técnicas de los bienes y servicios detalladas en el presente documento.
Garantía	De conformidad a especificaciones técnicas de los bienes y servicios detalladas en el presente documento.

B. Experiencia y personal técnico especializado

- **Experiencia**

Para la verificación de la **Experiencia del proveedor**, deberá presentar al menos **dos (2)** referencias o evidencias verificables de experiencia multinacional, regional o nacional en servicios similares a los solicitados, correspondientes a proyectos ejecutados dentro de los últimos **cuarenta y ocho (48) meses**, que demuestren experiencia en el suministro, instalación, configuración, implementación, integración y puesta en operación de soluciones de infraestructura tecnológica de redes de datos, conectividad inalámbrica empresarial, switching y seguridad perimetral, en instituciones públicas o privadas de similar complejidad.

Para efectos del presente requisito, se entenderá por **"referencias o evidencias"** cualquiera de los siguientes documentos: cartas de recomendación, constancias o notas simples de trabajos realizados con una calificación de excelente o muy bueno, casos de éxito públicos, documentación contractual o facturas electrónicas que respalden la prestación del servicio.

- **Personal técnico especializado**

Para que el Proveedor sea considerado en la etapa de evaluación deberá cumplir las siguientes condiciones, sin excepciones:

- El Proveedor deberá proveer el personal técnico especializado necesario para ejecutar el suministro, instalación, configuración, integración, pruebas, puesta en operación y soporte técnico de la infraestructura tecnológica objeto del presente proceso.
- El personal del Proveedor deberá tener disponibilidad para trabajar de forma remota o presencial en las instalaciones que la institución contratante determine, previo acuerdo entre las partes.
- El Proveedor deberá comprobar la experiencia del líder del equipo mediante la presentación de su currículum vitae, acreditando experiencia en la dirección, implementación y administración de proyectos de infraestructura tecnológica, redes empresariales, conectividad inalámbrica, switching, seguridad perimetral o soluciones de tecnología de información de similar complejidad.
- El Proveedor deberá presentar la documentación que respalde las certificaciones y experiencia del personal técnico requerido para cada una de las soluciones ofertadas, de conformidad con las especificaciones técnicas establecidas en los presentes Términos de Referencia.

C. Calidad y seguridad de la solución.

El oferente deberá garantizar que la solución ofertada cumpla con los principios de confidencialidad, integridad, disponibilidad y protección de la información, mediante la implementación de mecanismos de seguridad incorporados en los equipos, plataformas y licencias suministradas. La solución deberá incluir las funcionalidades necesarias para proteger la infraestructura tecnológica frente a accesos no autorizados, amenazas de seguridad, interrupciones del servicio y demás riesgos asociados a la operación de la red.

Asimismo, el oferente deberá presentar una certificación vigente de la norma **ISO/IEC 27001** o su equivalente, emitida por un organismo certificador acreditado, que respalde la implementación de un Sistema de Gestión de Seguridad de la Información aplicable a la organización del fabricante o del oferente, según corresponda.

La solución deberá incorporar mecanismos de autenticación, control de acceso, registro de eventos, trazabilidad, respaldo de configuraciones y demás funcionalidades de seguridad definidas en las especificaciones técnicas del presente documento, garantizando la protección de la infraestructura tecnológica y de la información que transite a través de ella.

Finalmente, el oferente deberá presentar una carta compromiso debidamente autenticada por notario, mediante la cual se obligue a cumplir durante toda la vigencia contractual con las medidas, controles,

políticas y procedimientos de seguridad de la información establecidos en los presentes Términos de Referencia, así como a mantener la confidencialidad de la información institucional a la que tenga acceso durante la ejecución del contrato.

La información proporcionada por la institución deberá ser utilizada exclusivamente para la ejecución de los servicios contratados, quedando prohibida su divulgación, transferencia, comercialización o utilización para fines distintos a los establecidos contractualmente, salvo autorización expresa y por escrito de la institución o disposición legal aplicable.

D. Interoperabilidad con otros sistemas

La solución ofertada deberá garantizar la interoperabilidad con la infraestructura tecnológica y los sistemas institucionales del Programa DoctorSV, permitiendo su integración con los diferentes componentes de la red, plataformas de administración, soluciones de seguridad y demás servicios tecnológicos que conforman el ecosistema digital de la institución.

El proveedor deberá implementar y mantener los mecanismos necesarios que permitan la integración de la solución con otros servicios tecnológicos, utilizando estándares abiertos, protocolos de comunicación ampliamente aceptados y las interfaces soportadas por el fabricante.

Las soluciones ofertadas deberán diseñarse e implementarse de forma que faciliten su escalabilidad e integración futura con nuevos componentes de infraestructura, plataformas tecnológicas o servicios institucionales, sin afectar la continuidad operativa de la red.

E. Respaldo y recuperación de datos

El proveedor deberá garantizar mecanismos de respaldo y recuperación que permitan preservar la disponibilidad y continuidad operativa de la infraestructura tecnológica implementada. Como parte de su oferta, deberá describir el esquema de respaldo de configuraciones, licenciamiento, políticas y demás componentes críticos de la solución, indicando la forma en que dichos respaldos serán almacenados y administrados.

Asimismo, deberá describir los procedimientos previstos para la restauración de configuraciones y recuperación de la operación de los equipos ante fallas, incidentes o contingencias, con el propósito de minimizar los tiempos de indisponibilidad y asegurar la continuidad de los servicios tecnológicos del Programa DoctorSV.

5. ADJUDICACIÓN

La presente contratación será adjudicada de manera total a un único oferente, por el valor total del servicio requerido. En consecuencia, no se realizará una adjudicación parcial ni se distribuirá el alcance del servicio entre varios oferentes. La adjudicación recaerá en el oferente que cumpla con el alcance, las especificaciones técnicas y las demás condiciones establecidas en el presente proceso de contratación. El monto adjudicado corresponderá a la suma del valor ofertado por el adjudicatario y el saldo

presupuestario remanente asignado al presente proceso, de conformidad con la disponibilidad presupuestaria correspondiente.

6. FORMA DE PAGO.

Forma de pago del servicio:

La institución realizará **dos (2) pagos**, distribuidos de la siguiente manera:

- **Primer pago:** Correspondiente al **Ítem 1**, una vez se haya efectuado el suministro, instalación, configuración, integración, pruebas y puesta en operación de la solución correspondiente, previa emisión del Acta de Recepción a satisfacción por parte del Supervisor de la orden de pedido y la documentación requerida para el trámite de pago.
- **Segundo pago:** Correspondiente al **Ítem 2**, una vez se haya efectuado el suministro, instalación, configuración, integración, pruebas y puesta en operación de la solución correspondiente, previa emisión del Acta de Recepción a satisfacción por parte del Supervisor de la orden de pedido y la documentación requerida para el trámite de pago.

Los pagos se efectuarán de conformidad con los procedimientos administrativos y financieros establecidos por la institución, previa presentación del comprobante fiscal correspondiente y demás documentos exigidos por la normativa aplicable.

Para la tramitación del pago, el proveedor deberá presentar como mínimo la siguiente documentación:

a) Informe de Ejecución del Servicio, que incluya el detalle y la descripción de lo ejecutado.
b) Factura de consumidor final a nombre de la institución contratante.

El Supervisor de la Orden de Pedido verificará el cumplimiento de las actividades reportadas y emitirá la correspondiente constancia o acta de conformidad del servicio, la cual habilitará el trámite del pago correspondiente.

Disposiciones comunes para el trámite de pago:

En caso de identificarse observaciones en los informes presentados, el proveedor deberá subsanarlas dentro del plazo que establezca la institución contratante a través del Supervisor de la Orden de Pedido, previo a la aprobación de los mismos.

El pago correspondiente se realizará únicamente una vez que los informes hayan sido revisados y aprobados por el Supervisor de la Orden de Pedido, verificándose el cumplimiento de las obligaciones contractuales durante el período reportado.

7. CRITERIOS DE EVALUACIÓN

Las ofertas presentadas serán evaluadas de acuerdo con los siguientes criterios:

CRITERIO	**PUNTUACION MÁXIMA**
PROPUESTA TÉCNICA	85 puntos
PROPUESTA ECÓNOMICA	15 puntos
TOTAL	**100 PUNTOS**

PROPUESTA TÉCNICA

Los proveedores deberán cumplir con la totalidad de los requisitos indicados en la siguiente tabla:

No.	**CRITERIO A EVALUAR**	**CUMPLE**	**NO CUMPLE**
PROPUESTA Y CARACTERISTICAS TÉCNICAS			
1	Cumplimiento de las especificaciones técnicas establecidas para cada uno de los componentes de la solución ofertada.		
2	Presenta la descripción de la metodología para el suministro, instalación, configuración, integración, pruebas y puesta en operación de la infraestructura tecnológica ofertada.		
3	Presenta el detalle de la arquitectura de la solución, indicando los equipos, licencias, componentes, accesorios y demás elementos que conforman la solución ofertada.		
4	Presenta el listado del personal técnico que participará en la implementación de la solución, adjuntando las hojas de vida y certificaciones requeridas en los presentes Términos de Referencia.		
5	Presenta el cronograma de ejecución del proyecto, indicando las actividades de suministro, instalación, configuración, integración, pruebas, capacitación y puesta en operación.		
6	Presenta la documentación técnica (fichas técnicas, manuales, datasheets y demás documentación) que respalde el cumplimiento de las especificaciones técnicas de los bienes ofertados.		
7	Presenta los Acuerdos de Nivel de Servicio (SLA) aplicables al soporte técnico de la solución, detallando como mínimo los horarios de atención, tiempos de respuesta, tiempos de solución, mecanismos de escalamiento y canales de atención.		
8	Presenta la carta de respaldo del fabricante y la documentación que acredite el nivel de partnership requerido, de conformidad con las especificaciones técnicas de cada componente.		
9	Presenta las certificaciones técnicas del personal y del fabricante requeridas para cada una de las soluciones ofertadas, de conformidad con las especificaciones técnicas establecidas en los presentes Términos de Referencia.		

SEGUNDA ETAPA. Perfil del proveedor

PERFIL DEL PROVEEDOR		**PUNTAJE**
1	Presenta certificación vigente de la norma ISO/IEC 27001 o su equivalente, emitida por un organismo certificador acreditado.	20 puntos
2	Presenta carta compromiso debidamente autenticada por notario, mediante la cual se compromete a cumplir durante toda la ejecución contractual con las medidas, controles, políticas y procedimientos de seguridad de la información establecidos en los presentes Términos de Referencia. (Anexo 2)	20 puntos
3	Presenta los Acuerdos de Nivel de Servicio (SLA) aplicables al soporte técnico de la solución, detallando como mínimo los horarios de atención, tiempos de respuesta, tiempos de solución, mecanismos de escalamiento y canales de atención.	5 puntos
4	Presenta carta compromiso debidamente autenticada por notario, mediante la cual garantice el mantenimiento, continuidad operativa y recuperación de la infraestructura tecnológica durante la vigencia contractual, de conformidad con los presentes Términos de Referencia.. (Anexo 3)	5 puntos
Experiencia del Proveedor		
6	El proveedor deberá presentar al menos dos (2) referencias o evidencias de servicios similares a los solicitados, correspondientes a proyectos ejecutados dentro de los últimos cuarenta y ocho (48) meses.	20 puntos
Perfil del personal clave		
7	Presenta al líder técnico del proyecto, acreditando experiencia en la implementación de soluciones de infraestructura tecnológica, redes empresariales, conectividad inalámbrica, switching, seguridad perimetral o proyectos de similar complejidad, de conformidad con lo requerido en los presentes Términos de Referencia.	15 puntos
PUNTAJE MÁXIMO		**85 puntos**

❖ El proveedor podrá cumplir los criterios anteriores con documentación propia, de sus subcontratistas, de su sociedad matriz, empresas del mismo grupo empresarial y/o afiliadas.

❖ Para el cumplimiento del criterio de **"Experiencia del proveedor"**, deberá presentar al menos dos (2) referencias o evidencias verificables de experiencia multinacional, regional o nacional en servicios similares a los solicitados, correspondientes a proyectos ejecutados dentro de los últimos cuarenta y ocho (48) meses, que demuestren experiencia en el **suministro, instalación, configuración, implementación, integración y puesta en operación de soluciones de infraestructura tecnológica**, incluyendo redes empresariales, conectividad inalámbrica, switching, seguridad perimetral, control de acceso biométrico o soluciones de tecnología de información de similar complejidad.
Para efectos del presente requisito, se entenderá por “referencias o evidencias” cualquiera de los siguientes documentos: cartas de recomendación, constancias o notas simples de trabajos realizados con una calificación de

excelente o muy bueno, casos de éxito públicos, documentación contractual o facturas electrónicas que respalden la prestación del servicio.

PROPUESTA ECONÓMICA

Se valorará con 15 puntos la propuesta de menor valor, a la siguiente propuesta de menor precio, se le otorgará un puntaje de 12 puntos, a la siguiente de 9 puntos y así sucesivamente se colocará un puntaje equivalente al resultado del puntaje anterior menos tres puntos.

El Proveedor deberá presentar su oferta económica tomando en cuenta el anexo 1.

Anexo 1. OFERTA ECONÓMICA

El proveedor deberá presentar dentro de su oferta económica el detalle siguiente:

ítem	Código SINAB	Código ONU	Denominación del bien o servicio	Cantidad	Precio Unitario	Precio Total
1	X	X	SERVICIO DE INSTALACION Y CERTIFICACION DE CABLEADO ESTRUCTURADO PARA VOZ Y DATOS	1	$	$
2	X	X	SERVICIO DE INSTALACION DE RED DE AREA LOCAL (LAN)	1	$	$

Anexo 2. FORMATO DE CARTA COMPROMISO DE SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

[Ciudad], [día] de [mes] de [año]

Señores:
[Nombre de la Institución]
Presente.

Yo, [Nombre completo del representante legal], mayor de edad, [profesión u oficio], del domicilio de [ciudad], actuando en mi calidad de Representante Legal de [Nombre del oferente], por medio de la presente DECLARO Y ME COMPROMETO a lo siguiente:

PRIMERO. Que mi representada cumple y cumplirá durante toda la vigencia contractual con las medidas, controles, políticas y procedimientos de seguridad de la información requeridos en los Términos de Referencia correspondientes al proceso de contratación denominado “[nombre del proceso]”.

SEGUNDO. Que mi representada garantizará la confidencialidad, integridad, disponibilidad y protección de toda la información que sea procesada, almacenada, transmitida o gestionada mediante la plataforma objeto de la contratación.

TERCERO. Que mi representada mantendrá implementados controles de seguridad de la información, incluyendo, entre otros, mecanismos de autenticación, control de acceso, registro y trazabilidad de eventos, respaldo y recuperación de configuraciones, gestión de incidentes de seguridad y demás controles que resulten aplicables a la infraestructura tecnológica ofertada.

CUARTO. Que la información proporcionada por la institución contratante y por sus usuarios será utilizada exclusivamente para la ejecución de los servicios contratados y no será divulgada, transferida, comercializada, compartida ni utilizada para fines distintos a los establecidos en la orden de pedido, salvo autorización expresa y por escrito de la institución o por mandato legal aplicable.

QUINTO. Que mi representada adoptará las medidas técnicas, administrativas y organizativas necesarias para prevenir accesos no autorizados, pérdida, alteración, divulgación o uso indebido de la información que sea procesada en el marco de la prestación del servicio.

SEXTO. Que, en caso de producirse cualquier incidente de seguridad que pueda comprometer la información administrada mediante la infraestructura tecnológica, equipos, plataformas de administración, licencias y demás componentes objeto de la contratación, mi representada notificará oportunamente a la institución contratante y ejecutará las acciones necesarias para su atención, mitigación y resolución.

SÉPTIMO. Que mi representada mantendrá vigente durante la ejecución contractual la certificación ISO/IEC 27001 o certificación equivalente presentada como parte de su oferta, o en su defecto implementará medidas equivalentes que garanticen el cumplimiento de los estándares de seguridad comprometidos.

La presente carta compromiso se emite para ser incorporada a la oferta presentada en el proceso antes referido, obligando a mi representada al cumplimiento de las condiciones aquí establecidas durante toda la vigencia de la relación contractual.

Atentamente,

[Nombre del representante legal]
Representante Legal
[Nombre del oferente]

[Sello de la empresa]

AUTENTICACIÓN NOTARIAL
(La presente firma deberá ser autenticada por notario de conformidad con la legislación aplicable).

Anexo 3. CARTA COMPROMISO DE CONTINUIDAD DEL SERVICIO, MANTENIMIENTO Y RECUPERACIÓN ANTE DESASTRES

[Ciudad], [día] de [mes] de [año]

Señores
[Nombre de la Institución]
Presente.

Yo, [nombre completo], actuando en mi calidad de Representante Legal de [nombre del oferente], por medio de la presente me comprometo, en nombre de mi representada, a garantizar durante toda la vigencia contractual la continuidad operativa de la plataforma ofertada, así como la prestación de los servicios de mantenimiento, actualización, soporte y evolución requeridos para su adecuado funcionamiento.

Asimismo, nos comprometemos a mantener e implementar mecanismos y procedimientos de continuidad del servicio y recuperación ante desastres que permitan restablecer oportunamente la operación de la plataforma ante fallas, incidentes o eventos que puedan afectar su disponibilidad.

De igual forma, garantizamos que la solución tecnológica será operada bajo criterios de calidad, sostenibilidad operativa y uso eficiente de los recursos tecnológicos necesarios para su funcionamiento, procurando la continuidad y estabilidad de los servicios prestados a la institución contratante.

La presente carta se emite para ser incorporada a la oferta presentada dentro del proceso de contratación denominado “[nombre del proceso]”, obligándonos al cumplimiento de los compromisos aquí establecidos durante toda la ejecución contractual.

Atentamente,

[Nombre del Representante Legal]

Representante Legal

[Nombre del Oferente]

[Sello de la empresa]

AUTENTICACIÓN NOTARIAL
(La presente firma deberá ser autenticada por notario de conformidad con la legislación aplicable).