Fallo de adjudicación
LPL 05/2026
"SERVICIO DE MANTENIMIENTO DE LA RED DE CONECTIVIDAD Y TELEFONIA DEL CENTRO ADMINISTRATIVO TLAJOMULCO (CAT)"

Con fundamento en los artículos 115 fracción II, primer párrafo y IV, primer párrafo, así como el artículo 134 de la Constitución Política de los Estados Unidos Mexicanos; 9° primer párrafo, fracciones I, II, III, IV, V y VI, 73 primer párrafo, 79, 85 fracción IV y 88 primer y último párrafos de la Constitución Política del Estado de Jalisco; artículo 1 numeral 1, fracción III, y artículo 2 y 3, fracción IX, 34, 35 numeral 1, fracción III, 47, 59 numerales 1 y 2, 67, 69 y demás concurrente de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios; los artículos 1, 2, fracción III, 6, 15 y 16 de la Ley de Austeridad y Ahorro del Estado de Jalisco y sus Municipios; correspondiente al oficio CGIIS/DI/022/2026 para la Licitación **LPL 05/2026** referente a **"SERVICIO DE MANTENIMIENTO DE LA RED DE CONECTIVIDAD Y TELEFONIA DEL CENTRO ADMINISTRATIVO TLAJOMULCO (CAT)"** Requerido por la **Dirección de Infraestructura de Tecnologías de la Información.**

ANTECEDENTES:

1. El Comité de Adquisiciones de Tlajomulco de Zúñiga, aprobó en su cuarta sesión ordinaria del 26 veintiséis de marzo de 2026 dos mil veintiséis, las bases de este proceso de adquisición, por lo que a través de la Dirección de Recursos Materiales y por medio del portal del Gobierno de Tlajomulco de Zúñiga, en la misma fecha se publicó la convocatoria para participar, de acuerdo con el artículo 47 numeral 1 de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, así como con lo establecido en el rubro "Publicación de la Convocatoria en el portal web del Municipio de Tlajomulco de Zúñiga, Jalisco (en formato descargable)" de las bases de la licitación.

2. El 01 primero de abril de 2026 dos mil veintiséis se llevó a cabo una junta de aclaraciones, de conformidad con los artículos 63 y 70 de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, así como al rubro "Fecha, hora y lugar de la celebración de la primera Junta de Aclaraciones" de las bases de la licitación.

3. El 09 nueve de abril de 2026 dos mil veintiséis durante la quinta sesión con carácter de Ordinaria del Comité de Adquisiciones de Tlajomulco de Zúñiga, se llevó a cabo el registro y el acto de presentación de propuestas técnicas y económicas en apego a los artículos 59, fracciones V a XI y 64 a 70 de la Ley de Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

El Comité recibieron las propuestas de (01) un licitante, en la inteligencia de que se condujo sin limitar el proceso de competencia y libre concurrencia, disposición contenida en el artículo 51, Numeral 1 de la Ley de compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios.

Establecido lo anterior se hace constar que el licitante fue:

- **HOLA INNOVACIÓN S.A. DE C.V.**

En función de lo antes expuesto, así como a lo deliberado y resuelto por los miembros de este Comité y el área requirente, quienes conforman este acto, se emite el siguiente:

FALLO DE ADJUDICACIÓN:

Primero. El Comité de Adquisiciones de Tlajomulco de Zúñiga, resolvió que el licitante **HOLA INNOVACIÓN S.A. DE C.V.** En su propuesta **cumple** con los requisitos legales establecidos en las bases, los anexos y en la convocatoria de la licitación, al entregar todos los documentos. Esto es así de acuerdo con la revisión realizada por la Dirección de Recursos Materiales.

En virtud de lo anterior se adjunta tabla:

Tabla 1:

DESCRIPCIÓN DEL DOCUMENTO SOLICITADO EN BASES	HOLA INNOVACIÓN S.A. DE C.V.
Acta Constitutiva (copia) en caso de ser persona moral.	CUMPLE
Poder Representante (copia).	CUMPLE
Copia de identificación vigente	CUMPLE
Copia de comprobante de domicilio, vigencia no mayor a 2 meses.	CUMPLE
Carátula con el texto solicitado incluyendo el nombre del participante y número de hojas de su propuesta.	CUMPLE
Copia del Recibo Oficial de pago de Derechos de Bases de Licitación	CUMPLE
Anexo 1 Propuesta técnica	CUMPLE
Constancia de visita de campo (en caso de)	N/A
Anexo 4 Constancia de entrega de muestras (en caso de)	N/A
Curriculum del participante.	CUMPLE
Carta original firmada de aceptación y apego a las disposiciones establecidas en las bases.	CUMPLE
Carta bajo protesta de decir verdad de entregar los servicios solicitados de acuerdo a las necesidades y tiempos de la dependencia solicitante.	CUMPLE
Carta compromiso bajo protesta de decir verdad, de mantener el precio de los bienes y/o servicios ofertados. Así como cubrir cualquier eventualidad.	CUMPLE

Carta bajo protesta de decir verdad en la que garanticen la calidad de lo ofertado contra vicios ocultos del bien o servicio que ofrecen.	CUMPLE
Opinión positiva emitida por el SAT, con una antigüedad menor a 30 días.	CUMPLE
Constancia de Situación Fiscal Actualizada	CUMPLE
Constancia de Situación Fiscal de no adeudos "INFONAVIT". con una antigüedad menor a 30 días.	CUMPLE
Licencia Municipal vigente o copia de la SIEM Sistema de Información Empresarial Mexicano.	CUMPLE
Comprobante Fiscal Digital por Internet (CFDI) del pago del Impuesto sobre nómina del Estado o CARTA BAJO PROTESTA DE DECIR VERDAD, si no cuenta con trabajadores.	CUMPLE
Opinión de cumplimiento de Obligaciones Fiscales en materia de Seguridad Social con una antigüedad menor a 30 días.	CUMPLE
Anexo 7 Declaración constancia de proveedores	CUMPLE
Anexo 8 Declaración escrita, bajo protesta de decir verdad, de integridad y no colusión, con el texto establecido en las bases.	CUMPLE
Anexo 9 Carta de manifestación a la retención de la aportación "cinco al millar para fondo impulso Jalisco"	CUMPLE (No acepta)
Anexo 10 Carta bajo protesta, si alguno de los miembros de su administración, socios o accionistas, asociados, miembros, así como apoderados, han trabajado, colaborado, operado o sido parte, bajo cualquier modalidad, durante los últimos 02 años, de alguna otra de las empresas o proveedores que participen.	CUMPLE
Anexo 12 Estratificación de empresa	CUMPLE (grande)
Anexo 5, Propuesta Económica, de acuerdo a cotización.	CUMPLE

Segundo. En atención al dictamen técnico, con número de oficio **CGIIS/DI/083/2026** mediante el que el área requirente (Dirección de Infraestructura de Tecnologías de la Información) evaluó la propuesta, donde se valora puntualmente el cumplimiento de las especificaciones técnicas mínimas, se califica a la propuesta del licitante **HOLA INNOVACIÓN S.A. DE C.V.** de **no solvente técnicamente** por ende, no garantiza el cumplimiento de las obligaciones respectivas.

En virtud de lo anterior se adjunta la siguiente tabla comparativa.

Tabla 2:

CONCEPTO	HOLA INNOVACIÓN S.A. DE C.V.		
	DESCRIPCIÓN	**CUMPLE**	**MOTIVO**
1	Las tecnologías que el Licitante oferte en el "Contrato de servicio de mantenimiento de la red de conectividad y telefonía del Centro Administrativo de Tlajomulco (CAT)" deberán permitir un crecimiento modular a futuro conforme las necesidades del Gobierno de Tlajomulco de Zúñiga considerando la compatibilidad y funcionalidad con las tecnologías que actualmente operan en el Centro Administrativo Tlajomulco, garantizando que la solución y sus componentes queden implementados con las versiones más recientes liberadas por los fabricantes. Los LICITANTES que deseen participar en el proceso de licitación deberán de cumplir con lo siguiente: • Todos los proveedores participantes deberán acreditar su participación en por lo menos dos (2) proyectos exitosos comprobables similares y contar con amplia trayectoria en el ramo • Las propuestas y lo anexos técnicos deberán de presentarse en idioma español, para el caso de fichas técnicas, folletos y/o catálogos, estos deberán presentarse en idioma español y como única opción en idioma inglés. • Todas las propuestas deberán considerar soporte de fabricante con vigencia a partir del fallo de la licitación y hasta el 31 de diciembre de 2026. • El licitante deberá de acreditar que cuenta con las siguientes certificaciones vigentes: o Information Security Management System ISO/IEC 27001. o IT Service Management System ISO/IEC 20000. o Cisco Gold Partner.	NO CUMPLE	El proveedor no acredita con todas las certificaciones del inciso D, en los subincisos de la H a la L del mismo apartado se requieren. h. dos ingenieros con certificación CCIE 2 ingeniero con certificación CCIE Enterprise Infraestructure. i. 2 ingenieros con certificación ITIL Foundation. j. 1 ingeniero con certificación PMI. K. 1 ingeniero con certificación Veeam (VMCE). I. 1 ingeniero con certificación Scrum Master.

	o Certificación ITIL Expert de al menos un ingeniero. o Carta del fabricante de sistema de telefonía y centro de contacto, en el que indique que puede comercializar, instalar y soportar la solución. o Carta de distribuidor autorizado de la solución de grabación de voz y pantallas. o Carta del fabricante de la solución de WIFI, en el que indique que puede comercializar, instalar y soportar la solución. o 2 ingeniero con certificación CCIE Enterprise Infraestructure. o 2 ingenieros con certificación ITIL Foundation. o 1 ingeniero con certificación PMI. o 1 ingeniero con certificación Veeam (VMCE). o 1 ingeniero con certificación Scrum Master. o Carta de fabricante de la solución de monitoreo de tráfico, en la que especifique que la arquitectura abierta de XDR es compatible con la infraestructura de ciberseguridad con que cuenta el Municipio de Tlajomulco de Zúñiga. o Carta de distribuidor autorizado de la solución de monitoreo de tráfico.		
2	**1. Requerimientos Generales.** El Centro Administrativo Tlajomulco en lo sucesivo el "**CAT**" requiere de: • La renovación de los servicios de conectividad para las distintas ubicaciones del CAT. • La adquisición de 150 teléfonos IP y licenciamiento. • La renovación de suscripciones y soporte de fabricante de Telefonía, Centro de Contacto y sistema de grabación de llamadas. • La renovación de soportes de fabricante de la solución WIFI que actualmente se encuentra operando en el CAT. • La renovación de suscripciones de respaldos Veeam BackUp. • La adquisición de infraestructura de ciberseguridad, así como entrenamiento del personal en ciberseguridad.	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 320 – 323, 325 – 326, 406 - 865
3	**1.1 RENOVACIÓN CONECTIVIDAD** El licitante deberá suministrar un enlace Ethernet por medio de fibra óptica para cada una de las ubicaciones del CAT, por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 321 - 322

4	**1.1.1 ESPECIFICACIONES DEL SERVICIO DE ENLACE ETHERNET.** Los servicios de enlace Ethernet deberán estar distribuidos de la siguiente manera: - **7** enlaces de **20Mbps.** - **14** enlaces de **50Mbps.** - **1** enlace de **100Mbps.** - **1** servicio de **70 troncales SIP.** - **10** enlaces de **LAN-TO-LAN 50Mbps.** - **16** enlaces de internet **Asimétricos de 100Mbps.** - **10** enlaces de internet **Dedicados de 50Mbps.** - **1** servicio de **200Mbps simétrico.** **OPERACIÓN DEL SERVICIO.** - EL LICITANTE debe entregar el servicio operando en la capa 2 del modelo OSI, haciendo la propuesta de la distribución de VLANs de acuerdo con las mejores prácticas. - El servicio entregado por EL LICITANTE deberá tener la capacidad de agregar más servicios sin que esto represente la necesidad de agregar otro equipamiento o actualizar el entregado inicialmente. - EL LICITANTE debe presentar carta o escrito bajo protesta de decir verdad donde manifieste que tiene la capacidad para ofrecer el servicio de conectividad en la modalidad dual stack utilizando direcciones IPv4 e IPv6. - EL LICITANTE debe de incluir para la operación del servicio un equipo terminal (router) con capacidad suficiente para el enlace y funcionalidades requeridas, el cual será responsabilidad de EL LICITANTE la operación como en el mantenimiento, con al menos las siguientes características: • La compatibilidad con IPv6/ IPv4 (DUAL STACK). • Soporte protocolo de ruteo: BGP, OSPF. • La capacidad de procesamiento de dichos equipos no debe exceder el 80% cuando se esté transmitiendo al 100% de la capacidad de cada enlace. • El equipo que debe ser proporcionado por EL LICITANTE del servicio debe soportar IPv4 routing protocols RIP v1/v2, EIGRP, OSPF, BGP, PBR, PfR. • El equipo que debe ser proporcionado por EL LICITANTE del servicio debe soportar IPv6 routing protocolos EIGRP, RIP, OSPFv3, IS-IS, BGP and PBR. • El equipo que debe ser proporcionado por EL LICITANTE debe tener la opción de mecanismos	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 321 - 322

	estándares de cifrado de datos AES sin necesidad de nuevo hardware. **CONSIDERACIONES GENERALES.** - EL LICITANTE debe certificar mediante una carta u hoja de especificaciones técnicas del fabricante del equipo, que el equipamiento propuesto cumple con las características técnicas requeridas en este concurso. - EL LICITANTE debe considerar todo el equipo activo necesario para la prestación del servicio de Enlace Ethernet.		
5	**1.2 DESCRIPCIÓN DE LOS EQUIPOS DE TELEFONÍA IP.** Los equipos para telefonía IP se deberán suministrar de acuerdo con lo especificado en las características técnicas e incluir como mínimo los elementos de hardware, software y funcionalidades requeridas en el presente anexo técnico. ***Las funcionalidades que deben cumplir los teléfonos IP son:*** - Recibir llamadas. - Transferencia de llamada. - Retención de llamada. - Conferencia. - Tecnología IP. - Grabación de llamadas. ***Entre los beneficios que busca el CAT, son:*** - Mejorar los niveles de calidad en el servicio. - Mejor experiencia en la atención del cliente. - Estar a la vanguardia tecnológica que apoye a las necesidades del **CAT**. - Estabilidad y disponibilidad de la solución. - Actualización y evitar la obsolescencia de equipo. - Escalabilidad de la solución. La finalidad de la contratación es ampliar las herramientas tecnologías en materia de telefonía IP del **CAT**, a fin de mantener la continuidad de los servicios que proporciona y, de esta manera, alcanzar sus metas. **Tabla 1. Equipos requeridos para telefonía IP.**	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 322 - 326

1	Telefonía IP	Teléfono IP Gama Baja	75	Equipo
		Teléfono IP Gama Media	75	Equipo

	Las características aquí descritas son mínimas enunciativas más no limitativas del servicio requerido que el licitante deberá de cumplir.		
6	**1.2.1 FUNCIONALIDADES BÁSICAS.** El licitante deberá incluir en su propuesta técnica, que el Equipo de Procesamiento de Llamadas IP que se utilice para proporcionar el Servicio de Voz IP objeto de estas especificaciones técnicas, deberá contar con los elementos necesarios para garantizar como mínimo, el cumplimiento de las siguientes funcionalidades básicas: ***Establecimiento de llamadas***. Capacidad de realizar llamadas internas y hacia la Red Pública de Telefonía. ***Estado de la llamada***. Facilidad que permite visualizar en el display del Teléfono IP, el estado de las llamadas establecidas (recibidas o realizadas), en el que se muestre como mínimo el número y la duración. ***Identificación de llamada***. (CLID/nombre del llamante (CNID) Funcionalidades que permiten que un teléfono que recibe una llamada, además de timbrar, también reciba la información del número telefónico de la línea que lo llama (CLID o Calling Line Identification) y en su caso, el nombre asociado a dicha línea telefónica (CNID o Calling Number Identification) ***Indicador de Mensaje de Voz.*** Indicador visual en el teléfono de que se recibió un mensaje de voz. ***Indicador de llamada en espera***. Indicador audible mediante un tono que deberá escucharse cuando se tenga una llamada en espera, además de un indicador visual en el display del Teléfono IP, que deberá activarse cuando una llamada se pone en espera. ***Multilínea***. Facilidad que permite configurar varias líneas o accesos asociados a un número de extensión en un teléfono IP. ***Multirepresentación* de número** Facilidad que permite que se anuncien las llamadas de un mismo número de extensión, en diferentes teléfonos IP, inclusive en inmuebles diferentes. ***Accesos rápidos.*** El Sistema deberá permitir a través del Teléfono IP, la programación de marcaciones rápidas mediante teclas, dependiendo de la capacidad de teclas programables que se tenga. ***Control de volumen***. El Sistema deberá permitir fijar el volumen mínimo de audio y tono de timbre de los teléfonos IP. ***Transferencia de llamadas con y sin consulta***. Esta facilidad deberá permitir transferir una llamada establecida (interna o externa) a otra extensión o a cualquier otro número telefónico externo, consultando previamente si se desea recibir la llamada o directamente sin realizar esta consulta ***Desvío automático de llamadas (Externas/Internas)***. Facilidad que permite que todas las llamadas dirigidas a	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 323 - 326

	una extensión puedan enrutarse de manera automática hacia otra extensión, una operadora, un número externo o un equipo de correo de voz. ***Desvío de llamadas en ocupado***. En una llamada establecida, se deberá recibir una alerta en la pantalla del teléfono, indicando que hay una llamada entrante y deberá contarse con la opción de desviarla al correo de voz del usuario o un número predeterminado. ***Desvío de llamadas no atendidas***. Facilidad que en caso de no responder una llamada redirige la misma a un número telefónico predefinido o al correo de voz del usuario, después de un determinado número de timbrados. ***Conferencia Múltiple***. Capacidad de establecer conferencias de un mínimo de 6 participantes. Se deberán visualizar el nombre y/o número de línea de los participantes. ***Remarcación***. Facilidad que permite remarcar el último número marcado, con una tecla específica o digitando algún prefijo. ***Función de No Molestar***. Facilidad que permite a los usuarios pulsar una tecla o un prefijo para que no timbre el teléfono y no sean molestados con llamadas entrantes. ***Arreglo Jefe/Secretaria***. Configuración de esquemas Jefe- Secretaria con consulta y transferencia de llamada, además de contar con identificación visual del estado de la línea del Jefe (colgado-descolgado al. menos). ***Aparcamiento de llamada***. Esta función permite poner una llamada en espera (estacionarla) pulsando una tecla o prefijo y recuperarla desde otro teléfono ***Captura de llamadas por grupo***. Configuración de un grupo de teléfonos que permite, que de cualquiera de ellos, se pueda responder las llamadas del resto. ***Retención/Recuperación de llamada***. Esta facilidad permite a un usuario atender una llamada, no obstante, tenga una llamada establecida. El usuario puede elegir atender la nueva llamada poniendo a la primera en espera o alternarlas. ***Códigos de Marcación.*** El Sistema deberá contar con la funcionalidad de marcación a números restringidos (larga distancia, llamadas a celular y números de entretenimiento como mínimo), a través de un Código de Marcación personalizado de al menos 5 dígitos, que podrá utilizar el usuario en cualquier teléfono físico. ***Música en espera***. Facilidad que permite oír música o mensajes de audio de fondo, cuando se coloca una llamada en espera. El Sistema deberá incluir la música; por lo que respecta a los mensajes de audio, podrán ser predefinidos por el CAT. ***Historial de llamadas***. En los teléfonos IP se deberá observar el registro de las llamadas recibidas, realizadas y perdidas, con información de la llamada como; día, hora y duración, como mínimo. ***Timbres distintivos del teléfono***. Facilidad que permite personalizar el tono del timbre del Teléfono IP.		

Personalización de la pantalla del Teléfono IP. Personalización de la imagen de fondo de la pantalla.
Generación de tonos (DTMF). Envío de tonos desde Teléfonos IP hacia la Red Pública, con el fin de interactuar con sistemas de audio respuesta.
Acceso al Correo de voz. Facilidad que permite acceder al correo de voz mediante una tecla predefinida en el Teléfono IP. Para escuchar los mensajes de voz, se deberá requerir un PIN.
Configuración de Redes Privadas.
El Sistema deberá contar con la capacidad de configurar redes privadas, con esquemas de marcación cerrada. El Equipo de Procesamiento de Llamadas IP, deberá permitir inclusive la programación de un número de Red Privada en un Teléfono IP de cualquiera de las categorías solicitadas (con excepción de las analógicas), sin que se pierda el esquema de marcación cerrada.
Acceso al Directorio Telefónico. Capacidad del Sistema de acceder al Directorio Telefónico a través de los teléfonos IP. El licitante deberá considerar el acceso a LDAP.

Licenciamiento para usuarios de telefonía.
El licitante deberá proveer mediante derechos de uso de programas de software las licencias necesarias para los teléfonos solicitados por el **CAT**. La cantidad de nuevas extensiones telefónicas son 150 las cuales son a través de aparatos telefónicos.

El licitante deberá contemplar dentro de su propuesta técnica:

Tabla 2. Tipo de Licencias.

Tipo de Licencia	Cantidad
Licenciamiento para clientes de telefonía con dispositivos gama media	75
Licenciamiento para clientes de telefonía con dispositivos gama baja	75

Terminales Telefónicas.
Como parte de la solución de telefonía, EL LICITANTE deberá incluir los aparatos telefónicos IP para los usuarios del Municipio de Tlajomulco de Zúñiga.

Teléfonos Gama Media.
EL LICITANTE deberá incluir dentro de su propuesta técnica 75 teléfonos de Gama Media, los cuales deben cumplir con las siguientes características técnicas y funcionalidades:

Tabla 3. Características y especificaciones

DESCRIPCIÓN	CARACTERISTICA
Protocolo	SIP
Pantalla	3.5 pulgadas, escala de grises
Número de líneas	4
Speakerphone	Full Duplex
Botones programables (físicos o SoftKey)	4

Led indicador	Message Waiting
Botones físicos	Speaker audio, Audio Mute, Control de volumen, Messages, Directorio o Contactos Transfer o Forward, Conference, Estándar Keypad.
Funciones de llamadas	1. Transferir llamada de voz 2. Reenvío de llamadas, o desvío de llamadas de voz. 3. Conferencia de voz 4. Call hold o llamada en espera 5 -Call Pick
Acceso al Directorio personal/corporativo	SI
Soporte de protocolos	SIP, DHCP, HTTPS
Audio codec	G.711, G.722, G.729
Puertos Ethernet	2 (dos) Gigabit Ethernet (10/100/1000),
Alimentación de Energía	PoE 802.3af

Base	Escritorio
QoS	802.1Q/p
Seguridad	Debe tener la capacidad habilitada de encriptar el tráfico de voz (media y señalización) con clave de cifrado de 128 bits.
Idioma	Español
Cumplimiento de normativa de Seguridad	NOM-019-SCFI-1998 ó UL 60950 o CAN/CSA-C22.2 No. 60950 Second Edition

Teléfonos Gama Baja.

El licitante deberá incluir dentro de su propuesta técnica 75 teléfonos de Gama Baja, los cuales deben cumplir con las siguientes características técnicas y funcionalidades:

Tabla 4. Caracteristicas y especificaciones.

	<table><tr><th>DESCRIPCIÓN</th><th>CARACTERISTICA</th></tr><tr><td>Protocolo</td><td>SIP</td></tr><tr><td>Pantalla</td><td>3.5 pulgadas, escala de grises</td></tr><tr><td>Número de lineas</td><td>2</td></tr><tr><td>Speakerphone</td><td>Full Duplex</td></tr><tr><td>Botones programables (físicos o SoftKey)</td><td>2</td></tr><tr><td>Botones físicos</td><td>Speaker audio, Audio Mute, Control de volumen, Messages, Directorio o Contactos Transfer o Forward, Conference, Estándar Keypad</td></tr><tr><td>Funciones de llamadas</td><td>1. Transferir llamada de voz 2. Reenvío de llamadas, o desvío de llamadas de voz. 3. Conferencia de voz. 4. Call hold o llamada en espera</td></tr><tr><td>Acceso al Directorio personal/corporativo</td><td>SI</td></tr><tr><td>Soporte de protocolos</td><td>SIP, DHCP, HTTPS</td></tr><tr><td>Audio codec</td><td>G.711, G.722, G.729</td></tr><tr><td>Puertos Ethernet</td><td>1 puerto Gigabit Ethernet (10/100),</td></tr><tr><td>Alimentación de Energía</td><td>PoE 802.3af</td></tr><tr><td>Base</td><td>Escritorio</td></tr><tr><td>QoS</td><td>802.1Q/p</td></tr><tr><td>Seguridad</td><td>Debe tener la capacidad habilitada de encriptar el tráfico de voz (media y señalización) con clave de cifrado de 128 bits.</td></tr><tr><td>Idioma</td><td>Español</td></tr><tr><td>Cumplimiento de normativa de Seguridad</td><td>NOM-019-SCFI-1998 ó UL 60950 o CAN/CSA-C22.2 No. 60950 Second Edition</td></tr></table>		
7	**1.3 LICENCIAS DE SUSCRIPCIÓN DE TELEFONÍA Y CENTRO DE CONTACTO.** El licitante deberá proveer las distintas suscripciones y soporte de fabricante para las soluciones de Telefonía y Centro de Contacto que actualmente operan en el CAT por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 326 -

	<table><tr><th>Licenciamiento</th><th>Cantidad</th></tr><tr><td>Flex 3.0 for Contact Center</td><td>1</td></tr><tr><td>Solution Support for Collaboration</td><td>1</td></tr><tr><td>On-Premises UCCX.Premium Concurrent Agent</td><td>15</td></tr><tr><td>Collaboration Flex Plan 3.0</td><td>1</td></tr><tr><td>NU On-Premises Calling Enhanced</td><td>165</td></tr><tr><td>Unified Attendant Console Advanced</td><td>2</td></tr><tr><td>NU On-Premises Calling Professional</td><td>30</td></tr><tr><td>NU TelePresence Room</td><td>1</td></tr><tr><td>NU On-Premises Calling Access</td><td>655</td></tr><tr><td>CUBE Standard Trunk Session License</td><td>100</td></tr></table>		
8	**1.4 SOPORTE DE FABRICANTE DEL SISTEMA DE GRABACIÓN DE VOZ Y PANTALLAS.** EL LICITANTE deberá de contemplar dentro de su propuesta técnica y económica el soporte, mantenimiento preventivo y correctivo para el sistema de grabación de voz y pantallas marca Verint, por un periodo que comienza a partir del fallo de la licitación y hasta el 31 de diciembre de 2026. La propuesta del Licitante debe contemplar: a) Actualización de Hot Fixes, KB´s de la plataforma y del sistema operativo. b) 1 mantenimiento preventivo en sitio para limpieza de componentes del servidor. c) Revisión de logs, estado físico del servidor y eventos del sistema operativo. d) La plataforma de voz y pantallas deberá estar integrada con la plataforma de telefonía y centro de contacto con que cuenta el Municipio de Tlajomulco de Zúñiga. e) Las grabaciones se deben realizar mediante integración BIB de la plataforma de telefonía y usando la API JTAPI. f) EL LICITANTE deberá incluir actualizaciones menores y kb´s que surjan de la plataforma. g) EL LICITANTE deberá considerar la grabación del 100% de las interacciones de voz de los agentes del Centro de Contacto.	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 327, 390, 391, 400
9	**1.5 SOPORTE DE FABRICANTE DE SOLUCIÓN WIFI (HUAWEI).** EL LICITANTE deberá proveer los soportes de Fabricante para la solución de WIFI que actualmente se encuentra operando en el CAT por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026., debiendo proveer soportes para los siguientes dispositivos:	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 327

	<table><tr><th>Equipo</th><th>Cantidad</th></tr><tr><td>AC6508 Controladora AP</td><td>1</td></tr><tr><td>AirEngine5760-51 AP's</td><td>15</td></tr></table>		
10	**1.6 LICENCIAMIENTO VEEAM BACKUP.** EL LICITANTE deberá contemplar en su propuesta técnica la renovación de la solución de backup, recuperación y seguridad de datos, con que cuenta el Municipio de Tlajomulco de Zúñiga. El licenciamiento deberá considerarse por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026. El licenciamiento deberá: i. Garantizar una protección contra el ransomware. ii. Administrarse bajo una plataforma para todas sus cargas de trabajo, aplicaciones y datos. iii. Infraestructura definida por software independiente del hardware. iv. Recuperación instantánea a gran escala. v. Proteger las siguientes cargas de trabajo con el modelo de licencia Veeam Universal License (VUL): a) Virtual: VMware vSphere, Microsoft Hyper-V, Nutanix AHV y Red Hat Virtualization. b) Cloud: cargas de trabajo nativas de la nube: AWS, Microsoft Azure y Google Cloud. c) Físico: Microsoft Windows, Linux, IBM AIX y Oracle Solaris. d) Aplicaciones empresariales: Microsoft SQL, Exchange, SharePoint/ Active Directory, SAP HANA, Oracle RMAN, Kubernetes, MySQL, PostgreSQL. e) Recursos compartidos (file shares) NAS. **Características:** **a)** Veeam Backup & Replication Licencia de suscripción universal. **b)** Características de Enterprise Plus Edition. **c)** Paquete de 10 instancias (VM). **d)** Suscripción de Veeam Backup & Replication Univeral, por un periodo que comienza a partir del fallo de la licitación y hasta el 31 de diciembre de 2026. **e)** Cargas de trabajo protegidas. **f)** Cloud: i. AWS. ii. Azure. iii. Google Cloud. iv. Oracle Cloud. **g)** Virtual: i. VMware vSphere. ii. Microsoft Hyper-V. iii. Veeam Backup for Nutanix AHV. iv. Veeam Backup for Red Hat.	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 328, 390, 391

	h) Físico. i. Windows. ii. Linux. iii. Unix. **i)** Nas. **j)** Aplicaciones. i. Microsoft. ii. Oracle. iii. SAP Hana. iv. Postgresql.		
11	**1.7 INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL.** Con el crecimiento de los servicios digitales y la ampliación de los sistemas administrativos, operativos y de atención ciudadana del Municipio de Tlajomulco de Zúñiga, surge la necesidad de actualizar y fortalecer su infraestructura de seguridad perimetral, con el objetivo de asegurar una conectividad más robusta, segura y preparada para las demandas tecnológicas actuales y futuras. Para garantizar el correcto funcionamiento de los sistemas críticos y el acceso eficiente a los servicios en línea, EL LICITANTE deberá contemplar dentro de su propuesta la renovación y modernización de los equipos de seguridad perimetral, implementando soluciones de última generación que permitan mayor protección ante incidentes. La propuesta de modernización de la infraestructura de red se basa en la necesidad de migrar hacia una plataforma unificada que garantice mayor seguridad, eficiencia y gestión simplificada, consolidando una base tecnológica alineada con las estrategias de transformación digital del municipio. EL LICITANTE deberá contemplar dentro de su propuesta la infraestructura necesaria para habilitar la solución de Seguridad perimetral para el Municipio de Tlajomulco de Zúñiga, la cual deberá incluir: **1.7.1 2 (DOS) SWITCHES DE ALTA DENSIDAD DE 48 PUERTOS DE FIBRA ÓPTICA CON LAS SIGUIENTES CARACTERÍSTICAS:**	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 328 - 352

Característica	Valor
Puertos SFP28	48 puertos 1/10/25 GE SFP/SFP+/SFP28
Puertos 40/100 GbE QSFP28 [40/100 GbE QSFP+/QSFP28]	8x 100G QSFP28
VLANs Soportadas (Máximo)	4 K (4000)
Factor de Forma	1 RU Rack Mount
Capacidad de Switching	4000 Gbps
Paquetes por Segundo	4000 Mbps
Almacenamiento de MAC Address	96K
Power Supply	Fuentes de alimentación duales (Dual hot-swappable AC)
Split-port	Soportado (4x25G en puertos 100G QSFP28)

CARACTERÍSTICAS

1. Administración:

- La solución debe ser una plataforma de conmutación (switching) diseñada para entornos de Campus Core y Data Center, ofreciendo rendimiento, seguridad y resiliencia.
- El switch deberá poder aceptar actualizaciones de firmware.
- Los switches con PoE deberán tener la capacidad de habilitar o deshabilitar la función de PoE (N/A, este modelo no soporta PoE).
- Deberá soportar detección y notificación de conflictos de direcciones IP, como se define en el RFC 5227.
- Deberá soportar administración por IPv4 e IPv6.
- Deberá soportar Telnet / SSH para acceso a la consola.
- Deberá soportar HTTP / HTTPS.
- El equipo debe tener fuentes de alimentación duales intercambiables en caliente (Dual hot-swappable AC).
- Debe soportar opciones de despliegue de toque cero (Zero-touch deployment).

2. Layer 2 / Layer 3 Networking.

- Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure.
- Deberá soportar el estándar IEEE 802.3 CSMA/CD como método de acceso y las especificaciones de la capa física.
- Deberá contar con la funcionalidad de Control de Tormentas (Storm Control).
- Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based.
- Deberá soportar la funcionalidad de Virtual-Wire (cable virtual).

	• Deberá soportar Time-Domain Reflectometer (TDR). • Deberá soportar 4094 VLANs simultáneas. • Deberá soportar IGMP Snooping. • Deberá soportar IGMP proxy y querier. • Deberá soportar emergency location identifier numbers (ELINs) en LLDP-MED. • Deberá permitir limitar la cantidad de MACs aprendidas por puerto (rango de 1 a 128). • Deberá permitir un mínimo de 15 instancias de MSTP. • Deberá permitir controlar tormentas de broadcast independientemente en cada puerto. • Deberá soportar la agregación de enlaces 802.3ad y LACP. • Deberá soportar VXLAN (RFC 7348). • Deberá soportar MACsec (depende del modelo específico, pero la serie G lo soporta). • Deberá soportar Multi-Chassis Link Aggregation (MCLAG) para redundancia a nivel de nodo. • Deberá soportar STP para garantizar una topología de Capa 2 libre de bucles. **Licenciamiento.** EL LICITANTE deberá considerar el licenciamiento que incluya las funcionalidades de seguridad avanzada, así como la descarga de firmas de seguridad y actualizaciones de Firmware. Dicho licenciamiento deberá garantizar la operación continua del sistema, contemplando actualizaciones y soporte, por un periodo que comienza a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.		
12	**1.7.2 3 (TRES) SWITCHES DE 48 PUERTOS DE FIBRA ÓPTICA CON LAS SIGUIENTES CARACTERÍSTICAS:** **CARACTERÍSTICAS** **1 Administración.** • La solución debe ser una plataforma de conmutación (switching) diseñada para entornos de Campus Core y Data Center. Los switches con	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 329 - 330

Característica	Valor
Puertos SFP	48 puertos 1/10/25 GE SFP/SFP+/SFP28
Puertos 40/100 GbE QSFP28 [40/100 GbE QSFP+/QSFP28]	4x 100G o 6x 40G
Split-port	Soportado (hasta 4x10G o 4x25G por puerto QSFP)
Factor de Forma	1 RU Rack Mount
Capacidad de Switching	1760 Gbps
Paquetes por segundo	1518 Mbps
Almacenamiento de MAC Addresss	144K
Power Supply	Fuentes de alimentación duales (Dual hot-swappable AC)
VLANs Soportadas (Máximo)	4 K (4000)

<table>
<tr><td></td><td>PoE deberán tener la capacidad de habilitar o deshabilitar la función de PoE.
• Deberá soportar detección y notificación de conflictos de direcciones IP, según el RFC 5227.
• Deberá soportar administración por IPv4 e IPv6.
• Deberá soportar Telnet / SSH para acceso a la consola.
• Deberá soportar HTTP / HTTPS.
• El equipo debe tener fuentes de alimentación duales intercambiables en caliente (Dual hot-swappable AC).
• Deberá soportar opciones de despliegue de toque cero (Zero-touch deployment).

2 Layer 2 / Layer 3 Networking
• Deberá soportar el estándar IEEE 802.3x Flow Control con Back-pressure.
• Deberá soportar los estándares IEEE 802.3 10Base-T, 802.3u 100Base-TX, 802.3z 1000Base-SX/LX y 802.3ab 1000Base-T.

Licenciamiento
EL LICITANTE deberá considerar licenciamiento que incluya las funcionalidades de seguridad avanzadas, así como la descarga de firmas de seguridad y actualizaciones de Firmware. Dicho licenciamiento deberá garantizar la operación continua del sistema, contemplando actualizaciones y soporte, por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.</td><td></td><td></td></tr>
<tr><td>13</td><td>1.7.3 56 (CINCUENTA Y SEIS) SWITCHES DE 48 PUERTOS DE RJ45 CON LAS SIGUIENTES CARACTERÍSTICAS:
<table>
<tr><th>Característica</th><th>Valor</th></tr>
<tr><td>Puertos GBE</td><td>48 puertos GE RJ45</td></tr>
<tr><td>Puertos SFP</td><td>4x 10GE SFP+</td></tr>
<tr><td>Factor de Forma</td><td>1 RU Rack Mount</td></tr>
<tr><td>Capacidad de Switching</td><td>176 Gbps</td></tr>
<tr><td>Paquetes por Segundo</td><td>260 Mbps</td></tr>
<tr><td>Almacenamiento de MAC Addresss</td><td>32 K</td></tr>
<tr><td>PoE</td><td>48 puertos PoE+ (802.3 af/at)</td></tr>
<tr><td>VLANs Soportadas (Máximo)</td><td>4 K (4000)</td></tr>
</table>
CARACTERÍSTICAS
1 Administración.
• El switch deberá poder aceptar actualizaciones de firmware.
• Los switches con PoE deberán tener la capacidad de habilitar o deshabilitar la función de PoE.
• Deberá soportar detección y notificación de conflictos de direcciones IP
• Deberá soportar administración en la nube
• Deberá soportar administración por IPv4 e IPv6.</td><td>SI CUMPLE</td><td>El proveedor cumple con lo descrito en las páginas 331 - 332</td></tr>
</table>

	• Deberá soportar Telnet / SSH para acceso a la consola. • Deberá soportar HTTP / HTTPS. • Deberá soportar SNMP v1/v2c/v3. • Deberá poder configurar su reloj mediante un NTP Server. • Deberá contar con una linea de comandos estándar y con interface para configurar via Web. • Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI. • Deberá soportar HTTP REST APIs para configuración y monitoreo. • Quality of Service. • Deberá soportar priorización de tráfico basada en 802.1p. • Deberá soportar priorización de tráfico basada en IP TOS/DSCP. • Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP.		
2	**Layer 2.** • Deberá soportar Link Aggregation estático. • Deberá soportar LACP. • Deberá soportar Spanning Tree. • Deberá soportar Jumbo Frames. • Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex. • Deberá soportar el estandar IEEE 802.1D MAC Bridging/STP. • Deberá soportar el estandar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP). • Deberá soportar el estandar IEEE 802.1s Multiple Spanning Tree Protocol (MSTP). • Deberá soportar la funcionalidad STP Root Guard. • Deberá soportar STP BPDU Guard. • Deberá soportar Edge Port / Port Fast. • Deberá soportar el estandar IEEE 802.1Q VLAN Tagging. • Deberá soportar Private VLAN. • Deberá soportar el estandar IEEE 802.3ad Link Aggregation con LACP. • Deberá poder balancear trafico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac). • Deberá soportar el estandar IEEE 802.1AX Link Aggregation. • Deberá soportar instancias de Spanning Tree (MSTP/CST). • Deberá contar con la funcionalidad de Control de Tormentas (Storm Control).		

	• Deberá soportar la creacion de VLANs por MAC, IP y Ethertype-based. • Deberá soportar la funcionalidad de Virtual-Wire. • Deberá soportar Time-Domain Reflectometer (TDR). • Deberá soportar 4094 VLANs simultáneas. • Deberá soportar IGMP Snooping. • Deberá soportar IGMP proxy y querier. • Deberá soportar emgency location identifier numbers (ELINs) en LLDP-MED. • Deberá permitir la negociación de POE en LLDP-MED. • Deberá permitir limitar la cantidad de MACs aprendidas por puerto. • Deberá permitir un mínimo de 15 instancias de MSTP. • Deberá permitir controlar tormentas de broadcast independientemente en cada puerto. • Deberá soportar un mecanismo de detección y prevención de loops. • Deberá soportar VLAN Stacking (QinQ). • Deberá soportar SPAN. • Deberá soportar RSPAN y ERSPAN. **Licenciamiento** EL LICITANTE deberá considerar licenciamiento que incluya las funcionalidades de seguridad avanzadas, así como la descarga de firmas de seguridad y actualizaciones de Firmware. Dicho licenciamiento deberá garantizar la operación continua del sistema, contemplando actualizaciones y soporte, por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.		
14	**1.7.4 13 (TRECE) SWITCHES DE 24 PUERTOS DE RJ45 CON LAS SIGUIENTES CARACTERÍSTICAS:** **Característica / Valor** Puertos GBE: 24 puertos GE RJ45 Puertos SFP: 4x 10GE SFP+ Factor de Forma: 1 RU Rack Mount Capacidad de Switching: 128 Gbps Paquetes por Segundo: 190 Mbps Almacenamiento de MAC Addresss: 32 K PoE: 24 puertos PoE+ (802.3 af/at) VLANs Soportadas (Máximo): 4 K (4000) **CARACTERÍSTICAS:** **1 Administración.**	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 333 - 334

	• El switch deberá poder aceptar actualizaciones de firmware. • Los switches con PoE deberán tener la capacidad de habilitar o deshabilitar la función de PoE. • Deberá soportar detección y notificación de conflictos de direcciones IP. • Deberá soportar administración en la nube. • Deberá soportar administración por IPv4 e IPv6. • Deberá soportar Telnet / SSH para acceso a la consola. • Deberá soportar HTTP / HTTPS. • Deberá soportar SNMP v1/v2c/v3. • Deberá poder configurar su reloj mediante un NTP Server. • Deberá contar con una línea de comandos estándar y con interface para configurar vía Web. • Deberá soportar actualizaciones de Software por: TFTP/FTP/GUI. • Deberá soportar HTTP REST APIs para Configuración y monitoreo. • Quality of Service. • Deberá soportar priorización de tráfico basada en 802.1p. • Deberá soportar priorización de tráfico basada en IP TOS/DSCP. • Deberá soportar marcado de tráfico con 802.1p y/o IP TOS/DSCP.		
2	**Layer 2.** • Deberá soportar Link Aggregation estático. • Deberá soportar LACP. • Deberá soportar Spanning Tree. • Deberá soportar Jumbo Frames. • Deberá soportar Auto-negociacion para la velocidad de los puertos y para Duplex. • Deberá soportar el estándar IEEE 802.1D MAC Bridging/STP. • Deberá soportar el estándar IEEE 802.1w Rapid Spanning Tree Protocol (RSTP). • Deberá soportar el estándar IEEE 802.1s Múltiple Spanning Tree Protocol (MSTP). • Deberá soportar la funcionalidad STP Root Guard. • Deberá soportar STP BPDU Guard. • Deberá soportar Edge Port / Port Fast • Deberá soportar el estándar IEEE 802.1Q VLAN Tagging. • Deberá soportar Private VLAN. • Deberá soportar el estándar IEEE 802.3ad Link Aggregation con LACP. • Deberá poder balancear tráfico Unicast/Multicast sobre un puerto trunk (dst-ip, dst-mac, src-dst-ip, src-dst-mac, src-ip, src-mac). • Deberá soportar el estándar IEEE 802.1AX Link Aggregation.		

	• Deberá soportar instancias de Spanning Tree (MSTP/CST). • Deberá contar con la funcionalidad de Control de Tormentas (Storm Control). • Deberá soportar la creación de VLANs por MAC, IP y Ethertype-based. • Deberá soportar la funcionalidad de Virtual-Wire. • Deberá soportar Time-Domain Reflectometer (TDR). • Deberá soportar 4094 VLANs simultáneas. • Deberá soportar IGMP Snooping. • Deberá soportar IGMP proxy y querier. • Deberá soportar emgency location identifier numbers (ELINs) en LLDP-MED. • Deberá permitir la negociación de POE en LLDP-MED. • Deberá permitir limitar la cantidad de MACs aprendidas por puerto. • Deberá permitir un mínimo de 15 instancias de MSTP. • Deberá permitir controlar tormentas de broadcast independientemente en cada puerto. • Deberá soportar un mecanismo de detección y prevención de loops. • Deberá soportar VLAN Stacking (QinQ). • Deberá soportar SPAN. • Deberá soportar RSPAN y ERSPAN. **Licenciamiento** EL LICITANTE deberá considerar licenciamiento que incluya las funcionalidades de seguridad avanzadas, así como la descarga de firmas de seguridad y actualizaciones de Firmware. Dicho licenciamiento deberá garantizar la operación continua del sistema, contemplando actualizaciones y soporte, por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.		
15	**1.7.5 25 (VEINTICINCO) PUNTOS DE ACCESO WIFI 7 CON LAS SIGUIENTES CARACTERÍSTICAS:** 	Característica	Valor
---	---
Puertos GBE	1 puertos GE RJ45
Puertos Multigiga	1 Puerto 2.5Gb
Ancho de Banda	2401 Mbps
Tecnología	802.11 a/b/g/n/ac/ax.
Frecuencias de operación.	2.4 / 5/ 6 Ghz
Tipo de Antenas	Internas
Tipo de Ap	Interior
PoE input	802.3 at/bt | **CARACTERÍSTICAS:** **1 General FAP.**	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 335 – 336

	• Punto de acceso (AP) que permita el acceso de los dispositivos a la red a través de la Wireless y que posea todas sus configuraciones centralizadas en controlador inalámbrico. • Deberá soportar el modo de operación centralizado, o sea, su operación depende del controlador inalámbrico que es responsable de gestionar las políticas de seguridad, calidad de servicio (QoS) y monitoreo de la radiofrecuencia. • Deberá identificar automáticamente el controlador inalámbrico al que se conectará. • Deberá permitir administrarse remotamente a través de links WAN. • Deberá poseer capacidad dual-band con radios 2.4GHz, 5GHz y 6GHz operando simultáneamente, además de permitir configuraciones independientes para cada radio. • Deberá poseer un radio dedicado al escaneo de radiofrecuencia. • El tráfico de los dispositivos conectados a la red inalámbrica debe realizarse de forma centralizada a través del túnel establecido entre el punto de acceso y el controlador inalámbrico. En este modo todos los paquetes deben ser encapsulados hasta el controlador inalámbrico. • Cuando sea encapsulado, el tráfico debe ser encriptado a través de DTLS o IPSEC. • Debe permitir el tráfico de los dispositivos conectados a la red inalámbrica de forma distribuida (local switching), o sea, el tráfico debe ser conmutado localmente en la interfaz LAN del punto de acceso y no necesitará ser encapsulado hasta el controlador inalámbrico. • Cuando el tráfico sea distribuido y la autenticación con PSK, en caso de fallo en la comunicación entre los puntos de acceso y el controlador inalámbrico, los usuarios asociados deben permanecer asociados a los puntos de acceso y al mismo SSID. Debe permitirse la conexión de nuevos usuarios a la red inalámbrica. • En conjunto con el controlador inalámbrico, debe optimizar el rendimiento y la cobertura inalámbrica (RF), realizando automáticamente el ajuste de potencia y la distribución adecuada de canales a ser utilizados. • Deberá soportar la funcionalidad de ajuste automático de potencia para extender la cobertura en caso de falla del punto de acceso vecino gerenciado por la misma controladora. • Debe soportar mecanismos para la detección y mitigación de puntos de acceso no autorizados, también conocidos como Rogue APs. • En conjunto con el controlador inalámbrico, debe implementar mecanismos de protección para		

	identificar ataques a la infraestructura inalámbrica (wIDS / wIPS). • En conjunto con el controlador inalámbrico, debe permitir la creación de múltiples dominios de movilidad (SSID) con configuraciones distintas de seguridad y red. • En conjunto con el controlador inalámbrico, debe implementar los siguientes métodos de autenticación: WPA (TKIP) y WPA2 (AES). • En conjunto con el controlador inalámbrico, debe implementar el protocolo IEEE 802.1X con la asociación dinámica de VLAN para los usuarios en función de los atributos proporcionados por los servidores RADIUS. • Deberá admitir los siguientes métodos de autenticación EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS y PEAP. • Deberá implementar el estándar IEEE 802.11r para acelerar el proceso de roaming de los dispositivos a través de la función conocida como Fast Roaming. • Deberá implementar el estándar IEEE 802.11k para permitir que un dispositivo conectado a la red inalámbrica identifique rápidamente otros puntos de acceso disponibles en su área para que ejecute el roaming. • Deberá implementar el estándar IEEE 802.11v para permitir que la red influya en las decisiones de roaming del cliente conectadas mediante el suministro de información complementaria, como la carga de utilización de los puntos de acceso cercanos. • Deberá implementar el estándar IEEE 802.11e; • Deberá implementar el estándar IEEE 802.11h; • El punto de acceso deberá soportar agregación de paquetes A-MPDU y A-MSDU. • El punto de acceso deberá soportar (LPDC) - Low Density Parity Check. • El punto de Acceso deberá soportar (MLD) - Maximum Likelihood Demodulation. • El Punto de Acceso deberá soportar método de diversidad (MRC) Maximum Ratio Combining. • Debe tener indicadores luminosos (LED) para indicación de estado. • Debe permitir su alimentación a través de Power Over Ethernet (PoE) conforme los estándares 802.3af o 802.3at. • El punto de acceso debe ser compatible y ser administrado por los controladores inalámbricos de este proceso. • Cualquier licencia y / o software necesario para la plena ejecución de todas las características descritas en este término de referencia deberá ser suministrada.		

<table>
<tr><td></td><td>

- Debe poseer un certificado emitido por la Wi-Fi Alliance.

Licenciamiento
EL LICITANTE deberá considerar licenciamiento que incluya las funcionalidades de seguridad avanzadas, así como la descarga de firmas de seguridad y actualizaciones de Firmware. Dicho licenciamiento deberá garantizar la operación continua del sistema, contemplando actualizaciones y soporte, por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.

</td><td></td><td></td></tr>
<tr><td>16</td><td>

1.7.6 1 (UN) FIREWALL DE NUEVA GENERACIÓN CON LAS SIGUIENTES CARACTERÍSTICAS:

Característica	Valor
FW Troughput (64 Bytes)	134Gbps
Sesiones concurrentes (TCP)	7.5 Millones
IPsec VPN Troughput	55 Gbps
Gateway to Gateway IPsec Tunnels	20,000
NGFW Troughput	15Gbps
Puertos RJ45	8x 1 GE / 2.5GE / 5GE / 10GE RJ45
Puertos SFP	16x 10GE SFP+
Puertos SFP28	8x 25GE SFP28
Puertos QSFP28	2x 100GE/ 40GE QSFP28

Características:

1. General.

- 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.
- Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.
- Las funcionalidades de protección de red que conforman la plataforma de seguridad, deberá soportar 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 de los equipos debe ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
- Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q;
- Los dispositivos de protección de red deben soportar agregación de enlaces 802.3ad y LACP.

</td><td>SI CUMPLE</td><td>El proveedor cumple con lo descrito en las páginas 337 - 340</td></tr>
</table>

	• Los dispositivos de protección de red deben soportar Policy based routing y policy based forwarding. • Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM). • 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. • Deberá ser compatible con NAT dinámica (varios-a-1). • Deberá ser compatible con NAT dinámica (muchos-a-muchos). • Deberá soportar NAT estática (1-a-1). • Deberá admitir NAT estática (muchos-a-muchos). • Deberá ser compatible con NAT estático bidireccional 1-a-1. • Deberá ser compatible con la traducción de puertos (PAT). • Deberá ser compatible con NAT Origen. • Deberá ser compatible con NAT de destino. • Deberá soportar NAT de origen y NAT de destino de forma simultánea. • Deberá soportar NAT de origen y NAT de destino en la misma política. • Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico. • Deberá ser compatible con NAT64 y NAT46. • Deberá implementar el protocolo ECMP. • Deberá soportar SD-WAN de forma nativa. • Deberá soportar el balanceo de enlace hash por IP de origen. • Deberá soportar el balanceo de enlace por hash de IP de origen y destino. • Deberá soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. • Deberá ser compatible con el balanceo en al menos tres enlaces. • Deberá implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales. • Deberá 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. • Enviará logs a sistemas de gestión externos simultáneamente.		

	• Deberá tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL. • Deberá soporta protección contra la suplantación de identidad (anti-spoofing). • Implementará la optimización del tráfico entre dos dispositivos. • Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP). • Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3). • Soportará OSPF graceful restart. • Deberá ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red. • Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico. • Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico. • Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas. • Soportará la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente. • Soportará la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3. • Soportará configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster. • La configuración de alta disponibilidad debe sincronizar: Sesiones. • La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red. • La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN. • La configuración de alta disponibilidad debe sincronizar: Tablas FIB. • En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace. • Deberá soportar la creación de sistemas virtuales en el mismo equipo. • Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos. • Deberá permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales. • La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.		

	• Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos). • Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red. • El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red. • Deberá existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi. • La consola de administración debe soportar como mínimo, inglés, español y portugués. • La consola debe soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad. • La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas. **2. Firewall.** • Deberá soportar controles de zona de seguridad. • Deberá contar con políticas de control por puerto y protocolo. • Contará con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones. • Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad. • Firewall deberá poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad. • Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall. • Deberá soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública. • Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).		

	• Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes. • Deberá soportar el protocolo estándar de la industria VXLAN. • La solución deberá permitir la implementación sin asistencia de SD-WAN. • En SD-WAN deberá soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN. • la solución debe soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall. **3. VPN.** • Deberá soportar e VPN de sitio-a-sitio y cliente-a-sitio. • Deberá soportar VPN IPSec. • Deberá soportar VPN SSL. • La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512. • La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14. • La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2); • La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard). • Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec. • Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting. • Deberá permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy. • Deberá permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL. • Deberá soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local. • Deberá permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL. • Deberá mantener una conexión segura con el portal durante la sesión. • El agente de VPN SSL o IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS. **Licenciamiento** EL LICITANTE deberá considerar licenciamiento que incluya las funcionalidades de seguridad avanzadas, así		

<table>
<tr><td></td><td>como la descarga de firmas de seguridad y actualizaciones de Firmware. Dicho licenciamiento deberá garantizar la operación continua del sistema, contemplando actualizaciones y soporte, por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.</td><td></td><td></td></tr>
<tr><td>17</td><td>1.7.7 5 (CINCO) FIREWALL DE NUEVA GENERACIÓN CON LAS SIGUIENTES CARACTERÍSTICAS:
<table><tr><th>Característica</th><th>Valor</th></tr><tr><td>FW Troughput (64 Bytes)</td><td>27.9Gbps</td></tr><tr><td>Sesiones concurrentes (TCP)</td><td>3 Millones</td></tr><tr><td>IPsec VPN Troughput</td><td>25 Gbps</td></tr><tr><td>Gateway to Gateway IPsec Tunnels</td><td>200</td></tr><tr><td>NGFW Troughput</td><td>2.5Gbps</td></tr><tr><td>Puertos RJ45</td><td>8x 1 GE RJ45</td></tr><tr><td>Puertos SFP</td><td>2x 1GE / 2.5GE / 5GE / 10GE SFP+</td></tr></table>CARACTERÍSTICAS.
1. General.
• La solución deberá 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.
• Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos.
• Las funcionalidades de protección de red que conforman la plataforma de seguridad, deberá soportar ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación.
• La plataforma deberá 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 de los equipos deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red.
• Los dispositivos de protección de red deben soportar 4094 VLANs Tags 802.1q.
• Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP.
• Los dispositivos de protección de red deberán soportar Policy based routing y policy based forwarding.
• Los dispositivos de protección de red deberán soportar encaminamiento de multicast (PIM-SM y PIM-DM).
• Los dispositivos de protección de red deberán soportar DHCP Relay.</td><td>SI CUMPLE</td><td>El proveedor cumple con lo descrito en las páginas 340 - 343</td></tr>
</table>

	• Los dispositivos de protección de red deberán soportar DHCP Server. • Los dispositivos de protección de red deberán soportar sFlow. • Los dispositivos de protección de red deberán soportar Jumbo Frames. • Los dispositivos de protección de red deberán soportar sub-interfaces Ethernet lógicas. • Deberá ser compatible con NAT dinámica (varios-a-1). • Deberá ser compatible con NAT dinámica (muchos-a-muchos). • Deberá soportar NAT estática (1-a-1). • Deberá admitir NAT estática (muchos-a-muchos). • Deberá ser compatible con NAT estático bidireccional 1-a-1. • Deberá ser compatible con la traducción de puertos (PAT). • Deberá ser compatible con NAT Origen. • Deberá ser compatible con NAT de destino. • Deberá soportar NAT de origen y NAT de destino de forma simultánea. • Deberá soportar NAT de origen y NAT de destino en la misma política. • Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico. • Deberá ser compatible con NAT64 y NAT46. • Deberá implementar el protocolo ECMP. • Deberá soportar SD-WAN de forma nativa. • Deberá soportar el balanceo de enlace hash por IP de origen. • Deberá soportar el balanceo de enlace por hash de IP de origen y destino. • Deberá soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. • Deberá ser compatible con el balanceo en al menos tres enlaces. • Debe implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales. • Deberá 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. • Enviará logs a sistemas de gestión externos simultáneamente. • Deberá tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL. • Deberá soporta protección contra la suplantación de identidad (anti-spoofing). • Implementará la optimización del tráfico entre dos dispositivos.		

	• Para IPv4, soportar enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP). • Para IPv6, soportar enrutamiento estático y dinámico (OSPFv3). • Soportará OSPF graceful restart. • Deberá ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red. • Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico. • Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico. • Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas; • Soportará la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente. • Soportará la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3. • Soportar configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster. • La configuración de alta disponibilidad debe sincronizar: Sesiones. • La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red. • La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN. • La configuración de alta disponibilidad debe sincronizar: Tablas FIB. • En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace. • Deberá soportar la creación de sistemas virtuales en el mismo equipo. • Para una alta disponibilidad, el uso de clusters virtuales debe de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos. • Deberá permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales. • La solución de gestión debe ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso. • Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), debe soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de		

	los certificados directamente en los sistemas virtuales (contextos). • Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red. • El tejido de seguridad debe identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red. • Debe existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi. • La consola de administración debe soportar como mínimo, inglés, español y portugués. • La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad. • La solución debe soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas. **2. Firewall.** • Deberá soportar controles de zona de seguridad. • Deberá contar con políticas de control por puerto y protocolo. • Contará con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones. • Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad. • El Firewall deberá poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad. • Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall. • Deberá soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública. • Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF). • Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes.		

- Deberá soportar el protocolo estándar de la industria VXLAN.
- La solución debe permitir la implementación sin asistencia de SD-WAN.
- En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN.
- la solución deberá soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall.

3. VPN.

- Deberá soportar VPN de sitio-a-sitio y cliente-a-sitio.
- Deberá soportar VPN IPSec.
- Deberá soportar VPN SSL.
- La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512.
- La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14.
- La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2).
- La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard).
- Deberá tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.
- Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec.
- Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting.
- Deberá permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy.
- Deberá permitir la creación de políticas de control de aplicaciones, IPS, antivirus, filtrado de URL y AntiSpyware para el tráfico de clientes remotos conectados a la VPN SSL.
- Deberá soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local.
- Permitirá la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de túneles SSL.
- Deberá mantener una conexión segura con el portal durante la sesión.
- El agente de VPN SSL o IPSEC cliente-a-sitio deberá ser compatible con al menos Windows y Mac OS.

Licenciamiento

EL LICITANTE deberá considerar licenciamiento que incluya las funcionalidades de seguridad avanzadas, así como la descarga de firmas de seguridad y actualizaciones

	de Firmware. Dicho licenciamiento deberá garantizar la operación continua del sistema, contemplando actualizaciones y soporte, por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.		
18	**1.7.8 1 (UN) FIREWALL DE NUEVA GENERACIÓN CON LAS SIGUIENTES CARACTERÍSTICAS:** **CARACTERÍSTICAS.** **1. General.** • La solución deberá 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. • Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos. • Las funcionalidades de protección de red que conforman la plataforma de seguridad, deberán soportar ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación. • La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7. • La gestión de los equipos deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red. • Los dispositivos de protección de red deberán soportar 4094 VLANs Tags 802.1q. • Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP. • Los dispositivos de protección de red deberán soportar Policy based routing y policy based forwarding. • Los dispositivos de protección de red deberán soportar encaminamiento de multicast (PIM-SM y PIM-DM). • Los dispositivos de protección de red deberán soportar DHCP Relay. • Los dispositivos de protección de red deberán soportar DHCP Server. • Los dispositivos de protección de red deberán soportar sFlow.	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 343 - 347

Característica	Valor
FW Troughput (64 Bytes)	10Gbps
Sesiones concurrentes (TCP)	1.4 Millones
IPsec VPN Troughput	7.1 Gbps
Gateway to Gateway IPsec Tunnels	200
NGFW Troughput	1.5Gbps
Puertos RJ45	10x 1 GE RJ45

	• Los dispositivos de protección de red deberán soportar Jumbo Frames. • Los dispositivos de protección de red deberán soportar sub-interfaces Ethernet lógicas. • Deberá ser compatible con NAT dinámica (varios-a-1). • Deberá ser compatible con NAT dinámica (muchos-a-muchos). • Deberá soportar NAT estática (1-a-1). • Deberá admitir NAT estática (muchos-a-muchos). • Deberá ser compatible con NAT estático bidireccional 1-a-1. • Deberá ser compatible con la traducción de puertos (PAT). • Deberá ser compatible con NAT Origen. • Deberá ser compatible con NAT de destino. • Deberá soportar NAT de origen y NAT de destino de forma simultánea. • Deberá soportar NAT de origen y NAT de destino en la misma política. • Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico. • Deberá ser compatible con NAT64 y NAT46. • Deberá implementar el protocolo ECMP. • Deberá soportar SD-WAN de forma nativa. • Deberá soportar el balanceo de enlace hash por IP de origen. • Deberá soportar el balanceo de enlace por hash de IP de origen y destino. • Deberá soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. • Deberá ser compatible con el balanceo en al menos tres enlaces. • Deberá implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales. • Deberá 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. • Enviará logs a sistemas de gestión externos simultáneamente. • Deberá tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL. • Deberá soporta protección contra la suplantación de identidad (anti-spoofing). • Implementará la optimización del tráfico entre dos dispositivos.		

	• Para IPv4, soportará enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP). • Para IPv6, soportará enrutamiento estático y dinámico (OSPFv3). • Soportará OSPF graceful restart. • Deberá ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red. • Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico. • Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico. • Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas. • Soportará la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente. • Soportará la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3. • Soportará configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster. • La configuración de alta disponibilidad debe sincronizar: Sesiones. • La configuración de alta disponibilidad debe sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red. • La configuración de alta disponibilidad debe sincronizar: Las asociaciones de seguridad VPN. • La configuración de alta disponibilidad debe sincronizar: Tablas FIB. • En modo HA (Modo de alta disponibilidad) debe permitir la supervisión de fallos de enlace. • Deberá soportar la creación de sistemas virtuales en el mismo equipo. • Para una alta disponibilidad, el uso de clusters virtuales deberá de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos. • Deberá permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales. • La solución de gestión deberá ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso. • Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound),		

	deberá soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos). • Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red. • El tejido de seguridad deberá identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red. • Deberá existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi. • La consola de administración deberá soportar como mínimo, inglés, español y portugués. • La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad. • La solución deberá soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas. **2. Firewall.** • Deberá soportar controles de zona de seguridad. • Deberá contar con políticas de control por puerto y protocolo. • Contará con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones. • Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad. • Firewall deberá poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad. • Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall. • Deberá soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública. • Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF).		

	• Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes. • Deberá soportar el protocolo estándar de la industria VXLAN. • La solución deberá permitir la implementación sin asistencia de SD-WAN. • En SD-WAN deberá soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN. • La solución deberá soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall. • Capacidad WiFi-Incluida. • El dispositivo deberá incorporar un punto de acceso de doble banda y doble transmisión que proporcionará el acceso inalámbrico WiFi-6 (802.11ax) de alta velocidad dentro del mismo hardware. • Deberá soportar los protocolos WiFi a/b/g/n/ac-W2/ax en el mismo dispositivo. **3. VPN.** • Deberá soportar VPN de sitio-a-sitio y cliente-a-sitio. • Deberá soportar VPN IPSec. • La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512. • La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14. • La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2). • La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard). • Deberá tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall. • Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec. • Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso throubleshooting. • Deberá permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy. • Deberá soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local. • Deberá mantener una conexión segura con el portal durante la sesión. • El agente de VPN IPSEC cliente-a-sitio debe ser compatible con al menos Windows y Mac OS. **Licenciamiento**		

	EL LICITANTE deberá considerar licenciamiento que incluya las funcionalidades de seguridad avanzadas, así como la descarga de firmas de seguridad y actualizaciones de Firmware. Dicho licenciamiento deberá garantizar la operación continua del sistema, contemplando actualizaciones y soporte, por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.		
19	**1.7.9 26 (VEINTISEIS) FIREWALL DE NUEVA GENERACIÓN CON LAS SIGUIENTES CARACTERÍSTICAS:** **CARACTERÍSTICAS.** **1. General.** • La solución deberá 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. • Por funcionalidades de NGFW se entiende: Reconocimiento de aplicaciones, prevención de amenazas, identificación de usuarios y control granular de permisos. • Las funcionalidades de protección de red que conforman la plataforma de seguridad, deberá soportar ejecutarse en múltiples dispositivos siempre que cumplan todos los requisitos de esta especificación. • La plataforma deberá estar optimizada para análisis de contenido de aplicaciones en capa 7. • La gestión de los equipos deberá ser compatible a través de la interfaz de administración Web en el mismo dispositivo de protección de la red. • Los dispositivos de protección de red deberán soportar 4094 VLANs Tags 802.1q; • Los dispositivos de protección de red deberán soportar agregación de enlaces 802.3ad y LACP. • Los dispositivos de protección de red deberán soportar Policy based routing y policy based forwarding. • Los dispositivos de protección de red deben soportar encaminamiento de multicast (PIM-SM y PIM-DM). • Los dispositivos de protección de red deberán soportar DHCP Relay.	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 347 – 350.

Característica	Valor
FW Troughput (64 Bytes)	3.9Gbps
Sesiones concurrentes (TCP)	600 Mil
IPsec VPN Troughput	3.5 Gbps
Gateway to Gateway IPsec Tunnels	200
NGFW Troughput	570 Mbps
Puertos RJ45	4x 1 GE RJ45

	• Los dispositivos de protección de red deberán soportar DHCP Server. • Los dispositivos de protección de red deberán soportar sFlow. • Los dispositivos de protección de red deberán soportar Jumbo Frames. • Los dispositivos de protección de red deberán soportar sub-interfaces Ethernet lógicas. • Deberá ser compatible con NAT dinámica (varios-a-1). • Deberá ser compatible con NAT dinámica (muchos-a-muchos). • Deberá soportar NAT estática (1-a-1). • Deberá admitir NAT estática (muchos-a-muchos). • Deberá ser compatible con NAT estático bidireccional 1-a-1. • Deberá ser compatible con la traducción de puertos (PAT). • Deberá ser compatible con NAT Origen. • Deberá ser compatible con NAT de destino. • Deberá soportar NAT de origen y NAT de destino de forma simultánea. • Deberá soportar NAT de origen y NAT de destino en la misma política. • Deberá soportar Traducción de Prefijos de Red (NPTv6) o NAT66, para evitar problemas de enrutamiento asimétrico. • Deberá ser compatible con NAT64 y NAT46. • Deberá implementar el protocolo ECMP. • Deberá soportar SD-WAN de forma nativa. • Deberá soportar el balanceo de enlace hash por IP de origen. • Deberá soportar el balanceo de enlace por hash de IP de origen y destino. • Deberá soportar balanceo de enlace por peso. En esta opción debe ser posible definir el porcentaje de tráfico que fluirá a través de cada uno de los enlaces. Debe ser compatible con el balanceo en al menos tres enlaces. • Deberá implementar balanceo de enlaces sin la necesidad de crear zonas o uso de instancias virtuales. • Deberá 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. • Enviará logs a sistemas de gestión externos simultáneamente. • Deberá tener la opción de enviar logs a los sistemas de control externo a través de TCP y SSL. • Deberá soportar protección contra la suplantación de identidad (anti-spoofing).		

	• Implementará la optimización del tráfico entre dos dispositivos. • Para IPv4, soportará enrutamiento estático y dinámico (RIPv2, OSPFv2 y BGP). • Para IPv6, soportará enrutamiento estático y dinámico (OSPFv3). • Soportará OSPF graceful restart. • Deberá ser compatible con el modo Sniffer para la inspección a través del puerto espejo del tráfico de datos de la red. • Deberá soportar modo capa - 2 (L2) para la inspección de datos y visibilidad en línea del tráfico. • Deberá soportar modo capa - 3 (L3) para la inspección de datos y visibilidad en línea del tráfico. • Deberá soportar el modo mixto de Sniffer, L2 y L3 en diferentes interfaces físicas; • Soportar la configuración de alta disponibilidad activo / pasivo y activo / activo: En modo transparente. • Soportará la configuración de alta disponibilidad activo / pasivo y activo / activo: En capa 3. • Soportará configuración de alta disponibilidad activo / pasivo y activo / activo: En la capa 3 y con al menos 3 dispositivos en el cluster. • La configuración de alta disponibilidad deberá sincronizar: Sesiones. • La configuración de alta disponibilidad deberá sincronizar: Configuraciones, incluyendo, pero no limitando, políticas de Firewalls, NAT, QoS y objetos de la red. • La configuración de alta disponibilidad deberá sincronizar: Las asociaciones de seguridad VPN. • La configuración de alta disponibilidad deberá sincronizar: Tablas FIB. • En modo HA (Modo de alta disponibilidad) deberá permitir la supervisión de fallos de enlace. • Deberá soportar la creación de sistemas virtuales en el mismo equipo. • Para una alta disponibilidad, el uso de clusters virtuales deberá de ser posible, ya sea activo-activo o activo-pasivo, que permita la distribución de la carga entre los diferentes contextos. • Deberá permitir la creación de administradores independientes para cada uno de los sistemas virtuales existentes, con el fin de permitir la creación de contextos virtuales que se pueden administrar por diferentes áreas funcionales. • La solución de gestión deberá ser compatible con el acceso a través de SSH y la interfaz web (HTTPS), incluyendo, pero no limitado a, la exportación de configuración de sistemas virtuales (contextos) por ambos tipos de acceso.		

	• Control, inspección y descifrado de SSL para tráfico entrante (Inbound) y saliente (Outbound), deberá soportar el control de los certificados individualmente dentro de cada sistema virtual, o sea, aislamiento de las operaciones de adición, remoción y utilización de los certificados directamente en los sistemas virtuales (contextos). • Deberá soportar una malla de seguridad para proporcionar una solución de seguridad integral que abarque toda la red. • El tejido de seguridad deberá identificar potenciales vulnerabilidades y destacar las mejores prácticas que podrían ser usadas para mejorar la seguridad general y el rendimiento de una red. • Deberá existir la opción de un Servicio de Soporte que ofrezca a los clientes un chequeo de salud periódico con un informe de auditoría mensual personalizado de sus appliances NGFW y WiFi. • La consola de administración deber soportar como mínimo, inglés, español y portugués. • La consola deberá soportar la administración de switches y puntos de acceso para mejorar el nivel de seguridad. • La solución deberá soportar integración nativa de equipos de protección de correo electrónico, firewall de aplicaciones, proxy, cache y amenazas avanzadas. **2. Firewall.** • Deberá soportar controles de zona de seguridad. • Deberá contar con políticas de control por puerto y protocolo. • Contará con políticas por aplicación, grupos estáticos de aplicaciones, grupos dinámicos de aplicaciones (en base a las características y comportamiento de las aplicaciones) y categorías de aplicaciones. • Control de políticas por usuarios, grupos de usuarios, direcciones IP, redes y zonas de seguridad. • Firewall deberá poder aplicar la inspección de control de aplicaciones, antivirus, filtrado web, filtrado DNS, IPS directamente a las políticas de seguridad. • Además de las direcciones y servicios de destino, los objetos de servicio de Internet deben poder agregarse directamente a las políticas de firewall. • Deberá soportar automatización de situaciones como detección de equipos comprometidos, estado del sistema, cambios de configuración, eventos específicos, y aplicar una acción que puede ser notificación, bloqueo de un equipo, ejecución de scripts, o funciones en nube pública.		

	• Deberá soportar el protocolo de la industria 'syslog' para el almacenamiento usando formato Common Event Format (CEF). • Deberá soportar integración de nubes públicas e integración SDN como AWS, Azure, GCP, OCI, AliCloud, Vmware ESXi, NSX, OpenStack, Cisco ACI, Nuage y Kubernetes. • Deberá soportar el protocolo estándar de la industria VXLAN. • La solución deberá permitir la implementación sin asistencia de SD-WAN. • En SD-WAN debe soportar, QoS, modelado de tráfico, ruteo por políticas, IPSEC VPN. • la solución deberá soportar la integración nativa con solución de sandboxing, protección de correo electrónico, cache y Web application firewall. • Capacidad WiFi-Incluida. • El dispositivo deberá incorporar un punto de acceso de doble banda y doble transmisión que proporciona el acceso inalámbrico WiFi-6 (802.11ax) de alta velocidad. • Deberá soportar los protocolos WiFi a/b/g/n/ac-W2/ax en el mismo dispositivo. **3. VPN.** • Deberá soportar VPN de sitio-a-sitio y cliente-a-sitio. • Deberá soportar VPN IPSec. • La VPN IPSec deberá ser compatible con la autenticación MD5, SHA-1, SHA-256, SHA-512. • La VPN IPSec deberá ser compatible con Diffie-Hellman Grupo 1, Grupo 2, Grupo 5 y Grupo 14. • La VPN IPSec deberá ser compatible con Internet Key Exchange (IKEv1 y v2); • La VPN IPSec deberá ser compatible con AES de 128, 192 y 256 (Advanced Encryption Standard). • Deberá tener interoperabilidad con los siguientes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall. • Deberá soportar VPN para IPv4 e IPv6, así como el tráfico IPv4 dentro de túneles IPv6 IPSec. • Deberá permitir activar y desactivar túneles IPSec VPN desde la interfaz gráfica de la solución, lo que facilita el proceso troubleshooting. • Deberá permitir que todo el tráfico de los usuarios VPN remotos fluya hacia el túnel VPN, previniendo la comunicación directa con dispositivos locales como un proxy. • Deberá soportar autenticación vía AD/LDAP, Secure id, certificado y base de usuarios local. • Deberá mantener una conexión segura con el portal durante la sesión. • El agente IPSEC cliente-a-sitio deberá ser compatible con al menos Windows y Mac OS.		

<table>
<tr><td></td><td>Licenciamiento
EL LICITANTE deberá considerar licenciamiento que incluya las funcionalidades de seguridad avanzadas, así como la descarga de firmas de seguridad y actualizaciones de Firmware. Dicho licenciamiento deberá garantizar la operación continua del sistema, contemplando actualizaciones y soporte, por un periodo que inicia a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.</td><td></td><td></td></tr>
<tr><td>20</td><td>1.7.10 TRANSCEPTORES ÓPTICOS.

EL LICITANTE deberá de considerar dentro de tu propuesta técnica los transceptores ópticos y cables prefabricados recomendados y certificados por el fabricante de la marca de los equipos de seguridad perimetral ofertados.

EL LICITANTE deberá contemplar los siguientes Transceptores y cables prefabricados:

<table>
<tr><th>Tipo de Fibra/Cable</th><th>Distancia Máxima (mts)</th><th>Velocidad</th><th>Factor de Forma</th><th>Cantidad</th></tr>
<tr><td>MMF</td><td>220</td><td>1GE</td><td>SFP</td><td>2</td></tr>
<tr><td>MMF</td><td>300</td><td>10 GE</td><td>SFP+</td><td>26</td></tr>
<tr><td>MMF</td><td>80</td><td>10 GE</td><td>SFP+</td><td>96</td></tr>
<tr><td>MMF</td><td>30</td><td>10 GE</td><td>SFP+</td><td>100</td></tr>
<tr><td>Prefabricado</td><td>3</td><td>10 GE</td><td>Direct Attach Cable</td><td>1</td></tr>
<tr><td>Prefabricado</td><td>1</td><td>10 GE</td><td>Direct Attach Cable</td><td>19</td></tr>
<tr><td>Prefabricado</td><td>3</td><td>40 GE</td><td>Direct Attach Cable</td><td>2</td></tr>
<tr><td>Prefabricado</td><td>1</td><td>40 GE</td><td>Direct Attach Cable</td><td>6</td></tr>
</table>
</td><td>SI CUMPLE</td><td>El proveedor cumple con lo descrito en las páginas 350 - 351</td></tr>
<tr><td>21</td><td>1.7.11 INSTALACIÓN, CONFIGURACIÓN Y PUESTA A PUNTO DE INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL.

EL LICITANTE deberá considerar dentro de su propuesta técnica, la instalación, configuración y puesta a punto de los equipos de seguridad perimetral mencionados anteriormente y que a continuación se resumen:</td><td>SI CUMPLE</td><td>El proveedor cumple con lo descrito en las páginas 351</td></tr>
</table>

	<table><tr><th>Equipo</th><th>Cantidad</th></tr><tr><td>Switches de alta densidad de 48 puertos de Fibra Óptica</td><td>2</td></tr><tr><td>Switches de 48 puertos de Fibra Óptica</td><td>2</td></tr><tr><td>Switches de 48 puertos RJ45</td><td>56</td></tr><tr><td>Switches de 24 puertos RJ45</td><td>13</td></tr><tr><td>Access Point</td><td>25</td></tr><tr><td>Firewall 19 Gb IPS Troughput</td><td>1</td></tr><tr><td>Firewall 4.5 Gb IPS Troughput</td><td>5</td></tr><tr><td>Firewall 2.5 Gb IPS Troughput</td><td>1</td></tr><tr><td>Firewall 800 Mbps IPS Troughput</td><td>26</td></tr></table>		
22	**1.7.12 PLATAFORMA DE SIMULACIÓN DE ATAQUES.** EL LICITANTE deberá considerar dentro de su propuesta técnica y económica, un servicio de simulación de ataques del fabricante de los equipos propuestos, la cual debe permitir la realización de pruebas realistas y proporcionar métricas detalladas para evaluar la preparación de los usuarios. La plataforma deberá considerar lo siguiente: <table><tr><th>Requisito/Funcionalidad</th><th>Descripción Detallada de la Solución</th></tr><tr><td>Realismo de Ataques</td><td>La solución debe utilizar simulaciones de phishing que repliquen técnicas del mundo real, garantizando que las campañas sean altamente creíbles.</td></tr><tr><td>Tipos de Campañas</td><td>Debe soportar campañas de phishing por correo electrónico y simulaciones de phishing mediante códigos QR.</td></tr><tr><td>Personalización de Ataques (Plantillas)</td><td>Debe incluir una biblioteca de plantillas de phishing predefinidas (globales), así como la capacidad de crear plantillas y páginas de aterrizaje personalizadas.</td></tr></table>	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 351 - 352

	Personalización de Ataques (Dificultad) — Las campañas deben poder configurarse en diferentes niveles de dificultad (Simple, Moderado, Desafiante) para ajustar la complejidad de los indicadores de phishing (errores de ortografía, coincidencia de URL/enlaces, autenticidad de la página de aterrizaje). Personalización de Ataques (Contenido Avanzado) — Soporte para la inclusión de archivos adjuntos (como PDF) y la capacidad de insertar variables de plantilla en el cuerpo del correo (como nombre del destinatario, dominio, posición) para generar datos dinámicos y convincentes. Simulación de Spear-Phishing — Capacidad para crear correos electrónicos dirigidos sin clics ni archivos adjuntos, pero que simulen un ataque real de spear-phishing, permitiendo rastrear qué usuarios responden al correo. Botón de Alerta de Phishing (PAB) — Se requiere la provisión de un add-in para clientes de correo electrónico (Outlook para Exchange Online/Microsoft 365 y Exchange Server On-premises, y Thunderbird) que permita a los destinatarios reportar correos electrónicos sospechosos, sean simulados o reales. Manejo de Falsos Positivos — La plataforma debe permitir configurar un periodo de tiempo de demora para omitir las acciones de escáneres de correo electrónico de terceros (como abrir correos o hacer clic en enlaces) que podrían registrarse incorrectamente como actividad del usuario. Validación de Dominio — El servicio debe utilizar tokens DNS (registros TXT) para verificar la propiedad de los dominios, lo cual es un paso mandatorio antes de iniciar campañas.		
23	**1.7.13 CURSO DE CONCIENTIZACIÓN SOBRE SEGURIDAD PERIMETRAL.** EL LICITANTE deberá considerar dentro de su propuesta técnica, un curso de concientización sobre la seguridad perimetral para 30 personas, que serán designadas por LA CONVOCANTE. El propósito de este curso es proporcionar a las personas los conocimientos y las habilidades esenciales para proteger los activos de información. El curso guiará a los participantes en un entorno de aprendizaje en el que adquirirán una comprensión fundamental de varias amenazas a la seguridad de la red, las computadoras e ingeniería social. Más importante aún, las habilidades aprendidas en el curso contribuirán a que los participantes puedan tomar las medidas necesarias para mitigar su exposición a la seguridad. **MÓDULOS DEL CURSO:** 1. Controles de Acceso 2. Seguridad de la Inteligencia Artificial 3. Seguridad de nube	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 352 – 353.

	4. Seguridad en las comunicaciones 5. Operación y mantenimiento seguro de los sistemas de TI 6. Seguridad de tecnología operativa 7. Cadena de suministro 8. Ingeniería social El curso deberá ser impartido por personal certificado en el tema de ciberseguridad y deberá ser impartido dentro de las instalaciones del Municipio de Tlajomulco de Zúñiga. Al concluir el curso de ciberseguridad, el Licitante deberá emitir un diploma de participación.		
24	**1.8 HERRAMIENTA DE MONITOREO DE TRÁFICO** EL LICITANTE deberá ofrecer una solución de monitoreo de tráfico, eventos, detección y orquestación de respuestas con enfoque contra las amenazas cibernéticas en el ambiente heterogéneo de las redes modernas, donde las fronteras cada vez son más difusas. El Municipio de Tlajomulco de Zúñiga requiere de una solución para proteger, asegurar y defender la infraestructura de red, así como los datos de posibles daños, acceso no autorizado y uso indebido de recursos de TI. La solución que ofrezca el LICITANTE deberá ser abierta, agnóstica y capaz de integrar cualquier fuente de información de las diferentes marcas que operan la seguridad perimetral de LA CONVOCANTE (no open source) aplicando los conceptos de Open XDR (Extended Detection and Response). La solución de monitoreo de tráfico, eventos, detección y orquestación de respuestas busca un enfoque proactivo para el manejo de ciber amenazas dentro de la infraestructura de LA CONVOCANTE, el cual brindará visibilidad de los datos a través de redes, nubes y puntos finales, mientras se aplica análisis y automatización para abordar las ciber amenazas cada vez más sofisticadas de la actualidad. La solución deberá incluir y abarcar en una sola licencia y plataforma las siguientes características: • Módulo de IDS basado en Machine Learning. • Módulo Multitenancy para diferentes campus o instancias. • Módulo de UEBA (análisis de comportamiento de usuarios y entidades). • Módulo de Network Detection and Response. • Módulo de Caza de Amenazas (Threat Hunting) • Módulo de Automatización de Respuesta. • Módulo de Sistema de información y gestión de eventos de seguridad (SIEM) • Módulo de Sandbox de Red. • Módulo de Inteligencia de Amenazas. • Módulo de Monitoreo de Integridad de Archivos.	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 353 – 354.

	Estos módulos deberán ser administrados en la misma consola de gestión y deberán ser del mismo fabricante. Se deberá considerar dentro de la solución y como parte de la misma, estas actividades de entrega: • Deberá de implementarse de manera transparente a través de sensores y/o sondas físicas o virtuales, para proporcionar telemetría. • Deberá de rastrear las amenazas en cualquier fuente o ubicación dentro de LA CONVOCANTE, incluyendo y no limitado a: redes, servidores (físicos y virtuales), aplicaciones, contenedores, nubes pública y privada. • Deberá de identificar amenazas ocultas, sigilosas y sofisticadas, en archivos o en el tráfico de red de forma pro-activa y rápida en la infraestructura tecnológica. • Deberá de realizar análisis de patrones de tráfico este-oeste (tráfico en el mismo segmento de LAN) a través de un puerto espejo o port mirror. • Deberá de correlacionar los eventos, anomalías e incidentes identificados de manera automática. • Deberá permitir la caza de amenazas en todos los ambientes de LA CONVOCANTE. • Deberá Integrarse a la infraestructura de firewalls de LA CONVOCANTE para enriquecer la información colectada, independientemente de la marca. • Deberá tener la capacidad de responder cada evento de ataques de ciberseguridad de manera orquestada y automatizada integrándose con la infraestructura tecnológica de ciberseguridad y redes presente en la Institución para tal fin. • Deberá ser una solución basada en nube, no se admitirá solución instalada en sitio. • Se deberá Aumentar la productividad de los analistas de Ciberseguridad de LA CONVOCANTE a través de un proceso de capacitación directa del fabricante. EL LICITANTE deberá considerar todo el equipamiento, licenciamiento, implementación, puesta a punto, memoria técnica y entrenamiento de los componentes tecnológicos que componen el servicio de Orquestación de Red y respuesta a Incidentes. **CARACTERÍSTICAS TÉCNICAS:** La solución propuesta por el LICITANTE deberá brindar el monitoreo de tráfico, eventos, detección y orquestación de respuestas deberá de cumplir las siguientes características de operación: • EL LICITANTE deberá proporcionar el servicio para la continuidad operativa con capacidades de analizar en el tráfico de la red: eventos de seguridad anómalos y críticos, en internet, la		

comunicación Este-Oeste y Norte-Sur la red interna, perimetral, las aplicaciones, contenedores, servidores, usuarios, entre estos elementos que representen un riesgo para LA CONVOCANTE, y que sea capaz de recolectar información de datos que cursen hacia y desde la MPLS, Internet, LAN to LAN, LAN, servidores u otros, con una amplia variedad de patrones de uso.

- Para este servicio, el sistema deberá contar con al menos las siguientes funcionalidades:

  - Proveer la habilidad de escuchar el tráfico de la red de manera transparente y descubrir elementos nuevos de infraestructura automática.
  - Visibilidad en toda la red (extremo a extremo), logrando identificar, eventos de Ciberseguridad, las anomalías críticas, correlaciones, conexiones y segmentos. Mostrando la distribución de las amenazas presentes, intentos de infiltración y riesgo, de acuerdo con los estados de MITRE ATT&CK para mejorar la postura de seguridad de LA CONVOCANTE.
  - Esta solución deberá tener la capacidad de integrar las diferentes plataformas que integran la red de LA CONVOCANTE, para correlacionar de manera automática.
  - Contar con Inteligencia Artificial para correlacionar todos los eventos de manera automática y cercano a tiempo real.

- La solución debe de contar con diversas funcionalidades que permitan maximizar la capacidad de detección a través MITRE ATT&ACK de manera automática, como mínimo:

  a. IDS basado en Machine Learning.
  b. Sandbox.
  c. Analítica de comportamiento de Usuarios y entidades (UEBA).
  d. Detección de Phishing.
  e. Network Detection and Response.
  f. Caza de Amenazas (Threat Hunting) empoderado con Graph Machine Learning.
  g. Módulo de Automatización de Respuesta.
  h. Sistema de información y gestión de eventos (SIEM).
  i. Threat Intelligence Platform (TIP) Herramienta de enriquecimiento de información automática de cada evento.
  j. Monitoreo de Integridad de Archivos.

- La solución podrá estar basada en equipos colectores que puedan conectarse vía puerto

	espejo, por medio de TAP's o packet brokers que le hagan llegar paquetes en crudo. Los colectores reportarán a un servidor central o bien, EL LICITANTE podrá llevar a cabo la configuración remota de los paquetes de red de cada localidad y envío de los mismos a un servidor central cuidando que este tráfico no represente un consumo dentro del ancho de banda de los enlaces solicitados por LA CONVOCANTE. • El sistema deberá ser capaz de integrar al monitoreo aplicaciones y desarrollos propios de LA CONVOCANTE al menos por: o Identificador de aplicaciones no limitado al puerto TCP/UDP. o Direcciones IP de los servidores. o IP Origen y Destino. • La recolección de datos de la solución no deberá afectar el rendimiento de la red de LA CONVOCANTE. Por lo que no deberá ser una solución exclusivamente basada en agentes. • La solución deberá generar información detallada de los eventos detectados, incluyendo amenazas, anomalías, comportamientos y tendencias de la red asociadas al riesgo en la red. • El sistema deberá ofrecer una solución de almacenamiento para datos históricos de seguridad que concentre todos los sitios de LA CONVOCANTE. o Datos de eventos de seguridad. o Datos de aplicación. o Datos de Sistemas operativos. o Datos de la nube pública y privada. o Datos de Trafico de Red. o Datos de fuentes de Inteligencia de amenazas. o Datos de geolocalización. o Trafico de registros (syslog). • La solución propuesta deberá ser capaz de crear reportes que permitan seleccionar el periodo (por hora, día, semana, mes, año, y personalizada es decir por fechas específicas). Este sistema almacenará los eventos de seguridad, hasta la conclusión del contrato (31 de diciembre de 2026). Toda la información deberá estar disponible, en los diversos tableros de reportes, disponibles en la plataforma, así como en el sistema de reportes, para el envío de estos de manera automatizada. • Analizar el tráfico TCP/UDP en la red de LA CONVOCANTE para detectar comportamiento y posibles amenazas, generando eventos accionables de acuerdo con el tipo de tráfico.		

	• La solución deberá ser capaz de realizar desgloses sobre las gráficas para mostrar el detalle de la información (proceso conocido en inglés como Drill Down). • La solución deberá estar disponible con los datos en gráficas que podrá filtrarse, al menos: por minutos, horas, días o meses. • Sé deberán emitir alertas cuando se detecten eventos críticos de seguridad en la red, se desvíe de los patrones establecidos (anomalías), mediante el análisis detallado de todas y cada una de las aplicaciones que corran en la red de manera nativa. • La solución deberá incluir mecanismos de sincronización como NTP (Network Time Protocol) o PTP (Precision Time Protocol) y así garantizar la correcta sincronización de la información. • La solución deberá poder integrar con métodos de autenticación vía Directorio Activo y LDAP, asimismo para identificar patrones de comportamientos anómalos de usuarios y poder deshabilitar usuarios del domino en caso de estar comprometidos o asociados a una amenaza. • La solución deberá contar con una aplicación que permita la caza de amenazas (Threat Hunting), para identificar las amenazas presentes en la red y automatizar los subsecuentes eventos de seguridad presentes en la red. • El sistema deberá contar con un visor de eventos que al menos de una vista retrospectiva de las mismas. • La herramienta deberá tener la capacidad de obtener mediciones de amenazas presentes en el tráfico y monitoreo proactivo cercano a tiempo real de todo el tráfico cursando por la red de LA CONVOCANTE, por lo menos, bajo las siguientes métricas: o Utilización de ancho de banda. o Intentos de penetración y escaneos de IPs y puertos. o Autenticaciones fallidas. o Ataques de autenticación de fuerza bruta exitosos. o Presencia de tráfico malicioso, como Ransomware, movimiento lateral, Cryptojacking, Mimikatz. o Análisis de archivos benignos y maliciosos y sus respectivas categorías. o Ataques de negación de servicio. o Conexiones de Comando y Control Presentes, internamente o hacia/desde Internet. o Hosts que representan el mayor riesgo. o Tiempos de respuesta, tráfico de entrada y de salida (inbytes/outbytes).		

	o Aplicaciones que más consumen recursos de red. o Análisis de DNS (tiempos de respuesta, time-out, errores y desempeño). o Distribución de las conexiones y su riesgo asociado. o Utilización de los servidores de Bases de Datos presentes (Top queries, usuarios, origen y destino y el detalle de uso. o Distribución de aplicaciones de capa 7. o Top de los eventos de seguridad críticos. o Tiempo de respuesta de aplicaciones. o En los sistemas virtuales cuyo tráfico atraviese la red física monitoreada, se deberán obtener al menos las siguientes métricas: Eventos de seguridad más críticos identificados en los servidores virtualizados. o Las aplicaciones que más se usan. o Top de eventos de seguridad entre las máquinas virtuales. o Riesgo asociado entre las máquinas virtuales. • Deberá ser capaz de realizar análisis retrospectivo basado en el análisis de la ingesta del tráfico TCP/UDP (análisis forense). • Deberá contar con una Plataforma de Inteligencia de Amenazas (TIP) integrada directamente en la solución. • Deberá proveer una capacidad de detección de ataques novedosos, conocidos como Zero Day • Deberá proveer un mecanismo para la clasificación de alertas de acuerdo al sentido del ataque (Interno o Externo) • Las capturas de paquetes que sean obtenidas por la solución deberán poder ser convertidas en metadatos para su análisis posterior. • Deberá permitir generar diagramas de las conexiones TCP mostrando cómo las amenazas asociadas, así como la comunicación entre el servidor y el cliente. Esto basado en capturas de tráfico, clasificado y normalizado de manera automática. • La solución deberá mostrar los eventos críticos y anomalías en las conversaciones TCP/UDP., así como en aplicaciones, servicios, servidores (físico y virtuales) y nubes públicas y privadas • Deberá permitir usar los paquetes almacenados en las sondas de monitoreo para crear gráficas de los eventos de seguridad entre 2 hosts que muestren dichas amenazas presentes en la conexión, con detalles que incluyan: el origen y destino, la geolocalización, reputación, evidencia de todos los eventos y que permitan una respuesta de estos.		

	• La solución de análisis y tráfico deberá graficar las anomalías de las aplicaciones dentro de la red, entregando resultados Top de al menos las siguientes variables: o Movimientos laterales. o Crónica de eventos. o Anomalías de tráfico malicioso. o Anomalías en las políticas y negaciones de los firewalls de la infraestructura de LA CONVOCANTE. o Top Aplicaciones. o Top Servidores. o Top Clientes. o Estados de las sesiones presentes. o Orígenes y destinos de países con mala reputación. • La plataforma deberá de generar KRI, tales como la cantidad de eventos generados en un día, semana o mes y compararlo con periodo similar, lo mismo, con la criticidad promedio de los eventos. • La solución de análisis de tráfico deberá integrarse con los elementos de IT presentes en la red, como FW, EDR, para enriquecer la información recopilada para su análisis • Deberá permitir inventariar los activos presentes en la red por direcciones IP y el nivel de riesgo de estos activos, con detalles y evidencia de esto sin necesidad de ejecutar análisis activos en la red para este fin. • Deberá ser capaz de monitorear el comportamiento de la red de ancho de banda por aplicación y así mismo identificar tendencias de crecimiento para poder tomar decisiones proactivas. • Deberá contar con mecanismos de control de acceso y autenticación basado en rol, para que únicamente el personal autorizado por LA CONVOCANTE, a través de la DSI tenga acceso a la información. • La plataforma deberá proporcionar tableros configurables que podrán contener diferentes paneles o gráficas de información, mostrando al menos la siguiente información: o *Eventos anómalos y críticos, los cuales incluyan:* ▪ Detecciones de seguridad. ▪ IP Origen y Destino. ▪ Panorámica de la actividad de los equipos (servidores e infraestructura, física y virtualizada). ▪ Las tácticas y técnicas asociadas al marco de MITRE ATT&ACK.		

- *Aplicación presentes o históricas en total y desglosado por:*
  - Riesgo asociado.
  - IP Origen y Destino.
  - Información de geolocalización.
  - Información de fuentes de inteligencia de amenazas.
  - Anomalías detectadas.
  - Calificación de riesgo.
  - Conversaciones entre Hosts.

- *Deberán permitir visualizar para un Host:*
  - Aplicaciones presentes.
  - Conversaciones hacia y desde el Host basadas en detecciones de seguridad y anomalías.
  - Deberá observar el estado de las aplicaciones y servicios que están corriendo en el centro de datos, como:
    - Indicar el número y severidad de las anomalías en indicadores clave de desempeño.
    - Indicar posibles problemas de seguridad en el centro de datos.

- Deberá proveer la capacidad de hacer zoom sobre la información, conocido como drill-down hacia métricas específicas que hayan causado el problema.

- La Solución deberá ser capaz de obtener datos disponibles para cada intervalo de tiempo seleccionado mostrando al menos las siguientes variables:
  - Ingesta recibida.
  - Tipos de eventos y anomalías de la ingesta recibida y normalizada.
  - Tráfico por dirección IP asociado con el puerto, aplicación.
  - Tráfico por puerto asociado con el protocolo IP.
  - Conversaciones entre estaciones IP.
  - Mostrar eventos de alta fidelidad.

- Deberá permitir la creación de filtros personalizados para búsquedas de eventos en específico.
- Deberá soportar diagnósticos en las diferentes capas del modelo OSI, las cuales deben incluir:
  - Análisis de anomalías de Red desde capa 2 hasta capa 7.
    - Direcciones IP.
    - Aplicaciones y/o puertos (TCP/UDP).
    - Servicios asociados.
    - Origen y destino.

	• Deberá contar con filtros de post-captura, independientes de los filtros de pre-captura, al menos por: o Filtro por errores. o Filtro de patrones de datos (Filtros por conversación entre dos estaciones a través de la selección del nombre o la dirección IP). o Filtro por protocolos. o Geolocalización. o Severidad y fidelidad. o Dirección IP. • La solución deberá proveer una consola unificada para toda la solución de análisis de tráfico de aseguramiento del servicio desde la cual pueden ser lanzadas las interfaces de alerta, monitoreo, troubleshooting. • Gestión proactiva que permita resolver problemas de seguridad antes de que afecten a los servicios solicitados. • Presentará la información referente a los servicios solicitados para LA CONVOCANTE. • De los sensores virtuales o Deberá soportar al menos 2 interfaces de 1Gbps para administración y otra para monitoreo. o Deberá de monitorear Ethernet, logrando identificar tráfico desde capa 2 hasta capa 7. o Contará con la capacidad de realizar Deep Packet Inspection (DPI) a los paquetes de red. o Contará con la capacidad de analizar +100 protocolos de OT. o Contará con la capacidad de reconocer +3500 aplicaciones web. o Contará con la capacidad de habilitar un Sensor de Nessus para integrarse a la consola centralizada de LA CONVOCANTE. o Contará con la capacidad de reenviar logs a la consola central. o Data Buffering. • Capacidad de ingesta de syslog o similar, siendo capaz de generar alarmas para los eventos identificados en estos medios. • Generación de reportes del estado actual de los elementos, su riesgo asociado y tendencias. • Configuración de umbrales para la generación de alarmas y envío de las mismas vía correo electrónico, u otro mecanismo automatizado. • Contar con una API restful para integración con diversos servicios para ingesta de tráfico y respuesta a eventos de seguridad. • Deberá contar con la funcionalidad de automatización de respuestas a los eventos		

	detectados, integrándose con la infraestructura de Ciberseguridad de LA CONVOCANTE, incluyendo Firewall, EDR Directorio Activo, entre otros. • Colectar las siguientes métricas cercano a tiempo real: o Puertos no estándar y anomalías asociadas. o IP/host de origen y destino. o Conexiones a/o desde IPs con mala reputación. o Conexiones a/o de países de alto riesgo. o Identificación de aplicaciones. • El sistema deberá ser compatible con las plataformas Windows y Linux. • Deberá permitir al personal que designe LA CONVOCANTE la generación de reportes explotando todas las variables y funcionalidades de la herramienta de Análisis de Tráfico de red, con la opción de parametrizar dichos reportes y consultarlos vía Web. • Deberá ser administrada vía una interface segura (https) en WEB por todos y cada uno de los usuarios encargados del monitoreo y buen funcionamiento de la red, de acuerdo a la función que estos desempeñen. Por lo tanto, no debe de haber límite de usuarios para monitoreo y deberá contar con la capacidad de crear permisos basados en roles (RBAC). • El monitoreo cercano a tiempo real para la detección de eventos y anomalías se realizará al menos cada minuto, este mismo intervalo de tiempo será utilizado para la medición de los niveles de servicio. • La plataforma deberá de tener la capacidad, de manera nativa de correlacionar vulnerabilidades reportadas por herramientas de terceros, con firmas de ataques identificados y mostrar un dashboard desde el cual se generen reportes. • El sistema deberá de contar con la funcionalidad de Automatización y Respuesta de la Ciberseguridad con el cual se pueda: o Generar alertas en base a incidentes identificados por consultas. o Contar con +240 plantillas con detecciones para casos de uso, como Ransomware, Command & Control, DGA, Cryptojacking, phishing, scripts maliciosos de power shell, UBA, ataques de día cero, como mínimo. o Debe tener la capacidad de crear reglas de caza de amenazas automática con respuesta en dispositivos perimetrales o de punto final. o La plataforma debe de tener la capacidad de mandar las instrucciones de respuesta a través de los mismos sensores de ingesta.		

	• La solución deberá de tener la capacidad de ejecutar una respuesta a cada evento identificado, como ejecutar una regla en el Firewall, deshabilitar un usuario, como mínimo. • Generar alertas que sean creadas con base a la correlación de al menos 2 consultas en campos distintos con extracción de información de al menos 5 campos. • Las condiciones para generar eventos deberán de integrar al menos la capacidad de señalar la cantidad de veces que se registre un evento en al menos 50 campos distintos de los eventos. • Las acciones de respuesta deben ser al menos las siguientes: o Enviar un correo electrónico. o Enviar mensajes a medios de comunicación tipo Slack. o Realizar una acción por medio de HTTP POST/PUT a un servidor. o Bloquear en el firewall. o Deshabilitar el usuario. o Ejecutar scripts. o Ejecutar una acción de contención hacia una herramienta de EDR. • La solución deberá de tener la capacidad de auditar el estado las acciones tomadas o pendientes. • Deberá tener la capacidad de generar reportes ejecutivos, de operación de LA CONVOCANTE, basado en plantillas preconfiguradas, personalizables, basados en tableros, etc. • Que proporcione visibilidad operativa sobre los eventos de seguridad detectados, sus resoluciones y los datos de los respectivos analistas. • La plataforma deberá de incluir una plataforma de gestión de casos e incidentes integrado. • Deberá contar con un módulo de gestión de incidentes, con el cual se proporcionará una representación visual de un incidente de seguridad, mostrado en orden cronológico o de acuerdo con los artefactos y/o indicadores de compromiso asociados a dicho incidente. • La plataforma deberá contar con un mecanismo de Machine Learning basado en Grafos para la detección y muestra de incidentes de seguridad. • La solución deberá contar con capacidades de multi inquilino (Multitenant), la cual permitirá la segmentación del sistema en instancias, con las siguientes características: o Segmentación de roles o Segmentación de datos o Procesos de aprendizaje automatizado independientes		

	• La capacidad multi inquilino o "multitenant" deberá ser nativa en la solución, por lo cual no deberá representar un licenciamiento extra o equipamiento adicional. • La solución deberá contar con herramienta que brinde prevención y visibilidad con detección y respuesta automatizadas en el endpoint: o Prevención de ataques inigualable. Múltiples tecnologías y modelos de Machine Learning para identificar y detener más ataques a lo largo de todo el ciclo de vida de la amenaza. o Investigación forense y visualización de los ciberataques. Obtenga información sobre el entorno de amenazas y realice análisis forense de los ataques dirigidos contra la organización. Permite la visualización de la cadena de ataque y detener la amenaza. o Endurecimiento basado en el análisis. Evalúe continuamente, priorice y endurezca los ajustes y configuraciones erróneas de la seguridad de endpoints y las vulnerabilidades ocasionadas por los usuarios con una lista priorizada fácil de entender. o Protección frente a ataques informáticos sofisticados, como las amenazas persistentes avanzadas (APT) y el ransomware, mediante más de treinta capas de tecnologías de seguridad respaldadas por Machine Learning. **Periodo de suscripción.** • La solución deberá de contar con la suscripción de licenciamiento por un periodo que inicie a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.		
25	**1.9 SERVICIO DE COUBICACIÓN DE SERVIDORES.** El licitante deberá de contemplar dentro de su propuesta técnica y económica la coubicación de servidores propiedad del Municipio de Tlajomulco de Zúñiga, para lo cual se deberá de ofertar 1 (un) gabinete exclusivo para el uso de los equipos del municipio, el cual deberá de contar por lo menos con las siguientes características: **Característica** / **Valor** Unidades de Rack: 42 Unidades de Rack totales Altura: 1,991mm Ancho: 600mm Profundidad: 1070mm PDU's: 2 Smart Rack PDU Horizontales Tierra Física: 1 Kit de tierra Física Energía: 3 Kilo Watts de energía en corriente alterna	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 361 – 362.

	EL LICITANTE deberá de incluir 6 eventos de manos y ojos remotos al mes por gabinete (no mayores a 30 minutos). Estos eventos consisten en: • Encendidos, apagado y/o reinicio de equipos. • Comprobación de estado y tecleado de un listado de comandos por solicitud escrita de LA CONVOCANTE en una consola preinstalada disponible. • Intercambio/conexión de medios para copias de seguridad (cintas, USB, CDs, DVDs, etc. • Verificación visual para ayudar en la solución remota de problemas por LA CONVOCANTE. • Instalación y Montaje de nuevos equipos de LA CONVOCANTE. • Conexión, desconexión e intercambio de cableado de red y/o eléctrico. • Etiquetado de los equipos. • Identificación, diagnóstico y testeo de circuitos. • Realización y envío de fotografías. EL LICITANTE además deberá incluir dentro de su propuesta de coubicacion 1 (un) servicio de internet dedicado de 100Mbps, para satisfacer las necesidades de conectividad de los equipos coubicados por LA CONVOCANTE. El servicio de coubicación deberá tener una vigencia, a partir del fallo de la licitación y hasta el 31 de diciembre de 2026.		
26	**1.10 MESA DE SERVICIO** EL LICITANTE deberá contar con una Mesa de Servicio, donde se podrá solicitar la atención a incidentes o fallas, un cambio y/o solicitar un requerimiento como asesorías, análisis de tráfico entre otros y/o servicios de mantenimiento preventivo que no se encuentren previamente programados. **La mesa de servicio es responsable de:** ▪ Registrar los requerimientos de LA REQUIRIENTE. ▪ Atención de primer nivel. ▪ Supervisar el ciclo de vida de los incidentes y requerimientos. ▪ Escalamiento de incidentes a niveles superiores cuando sea requerido. ▪ Retroalimentar al cliente con el estatus de atención por # de Reporte cuando así sea requerido. ▪ Mantener comunicación constante con el cliente. **Para solicitar un número de reporte es necesario contar con la siguiente información:** 1. Nombre de la empresa. 2. Nombre del responsable o quien reporta. 3. Número telefónico del responsable o quien reporta.	SI CUMPLE	El proveedor cumple con lo descrito en las páginas 362, 363.

C. HIGUERA 70, CENTRO • C.P. 45640 • TLAJOMULCO DE ZÚÑIGA, JAL. TELÉFONO: 33 3283 4400

<table>
<tr><td></td><td>
4. Nodo o sitio.
5. Tecnología que reporta.
6. Descripción de la falla, funcionalidad afectada o requerimiento.

Medios de Contacto a Mesa de Servicio:
1. TELEFONICA.
EL LICITANTE deberá de contar con una línea telefónica 800 para que LA REQUIRIENTE pueda levantar reportes y/o incidencias desde cualquier punto de la República Mexicana y esta deberá funcionar 24/7.
2. WEB.
EL LICITANTE deberá contar con una plataforma web en la que se pueda realizar el alta de solicitudes de LA REQUIRIENTE.
3. CORREO ELECTRONICO.
EL LICITANTE deberá de contar con una dirección de correo electrónico en el que LA REQUIRIENTE podrá hacer el alta de reportes que no cuenten con una cobertura por contrato de 7x24.
</td><td></td><td></td></tr>
<tr><td>27</td><td>
1.10.1 SLA

Cuando LA CONVOCANTE reporte un incidente relacionado a la infraestructura descrita en el presente anexo; el LICITANTE deberá atender dicho incidente acorde a la siguiente tabla de niveles de servicio.
<table>
<tr><th colspan="7">SERVICE LEVEL AGREEMENTS (SLA)</th></tr>
<tr><th>Soporte</th><th>Prioridad</th><th>Tiempo de Atención
Mesa De Servicio</th><th>Tiempo de Respuesta</th><th>Tiempo Total Restauración</th><th>SLA's</th><th>Cantidad Incluida</th></tr>
<tr><td>Incidentes.</td><td>Inmediata</td><td>5x8</td><td>30 min</td><td>6 hrs</td><td>90.00%</td><td>Ilimitado</td></tr>
<tr><td></td><td>Alta</td><td>5x8</td><td>60 min</td><td>12 hrs</td><td>90.00%</td><td>Ilimitado</td></tr>
<tr><td></td><td>Media</td><td>5x8</td><td>90 min</td><td>24 hrs</td><td>90.00%</td><td>Ilimitado</td></tr>
<tr><td></td><td>Baja</td><td>5x8</td><td>120 min</td><td>36 hrs</td><td>90.00%</td><td>Ilimitado</td></tr>
<tr><td>Cambios.</td><td>Estándar</td><td>5x8</td><td>180 min</td><td>6 hrs</td><td>90.00%</td><td>Ilimitado</td></tr>
</table>
</td><td>SI CUMPLE</td><td>El proveedor cumple con lo descrito en las páginas 363.</td></tr>
<tr><td>28</td><td>
1.10.2 MATRIZ DE ESCALAMIENTO

EL LICITANTE deberá proporcionar una matriz de escalamiento de mínimo 4 niveles, especificando datos de contacto de cada responsable del nivel, en caso de que los incidentes no sean resueltos en el tiempo establecido. Deberá sujetarse a los siguientes parámetros:
• 1er nivel de escalamiento: 30 minutos sin respuesta después de haber levantado el reporte en la mesa de ayuda.
• 2º nivel de escalamiento: 60 minutos sin respuesta después de haber levantado el reporte en la mesa de ayuda.
</td><td>SI CUMPLE</td><td>El proveedor cumple con lo descrito en las páginas 363</td></tr>
</table>

	• 3er nivel de escalamiento:1.5 horas sin respuesta después de haber levantado el reporte en la mesa de ayuda. • 4º nivel de escalamiento: 2 horas sin respuesta después de haber levantado el reporte en la mesa de ayuda.		

El Dictamen fue elaborado por, Cesar Osvaldo Flores Reynoso.

Tercero. Bajo dicho contexto, y de conformidad con el artículo 71, numeral 1 de la Ley Compras Gubernamentales, Enajenaciones y Contratación de Servicios del Estado de Jalisco y sus Municipios, el Comité de Adquisiciones. procede a **declarar desierta** la licitación **debido a que el licitante no cumple con los requisitos técnicos.** Así mismo, en virtud de que persiste la necesidad de adquirir el servicio, se emitirá una **segunda convocatoria.**

Cuarto. Publíquese el contenido del presente fallo en el Portal de Transparencia del Municipio de Tlajomulco de Zúñiga, haciendo este evento, las veces de notificación personal del mismo a los participantes. Lo anterior sin perjuicio de que puedan acudir personalmente para que se les entregue copia del mismo en el piso 3, Centro Administrativo Tlajomulco (CAT), Calle Higuera número 70 colonia Centro, Tlajomulco de Zúñiga, Jalisco, ubicación de la convocante.

Se hace constar que el acto fue celebrado en la séptima sesión ordinaria del 7 de mayo de 2026 dos mil veintiséis.

ING. JOSÉ RAFAEL MARTÍNEZ VALENCIA **Presidente Suplente de Comité de Adquisiciones**	**FIRMA**

LIC. MARCOS EDUARDO PADILLA DÍAZ **Representante de la Sindicatura Municipal**	**FIRMA**

La presente hoja de firmas corresponde al fallo de la adjudicación de la licitación LPL 05/2026

MTRA. ELIZABETH BUGARÍN GONZÁLEZ **Representante Oficialia Mayor**	**FIRMA**

LIC. ADRIANA SANTIAGO GONZÁLEZ **Representante de Tesorería Municipal**	**FIRMA**

LIC. EDGAR FERNANDO FLORES MORA **Representante de Cámara Nacional de Comercio, Servicios y Turismo de Guadalajara**	**FIRMA**

ING. OMAR PALAFOX SAENZ **Representante de Consejo de Desarrollo Agropecuario y Agroindustrial de Jalisco A.C.**	**FIRMA**

La presente hoja de firmas corresponde al fallo de la adjudicación de la licitación LPL 05/2026

ING. LUIS ALFONSO DE SANTIAGO GARCÍA **Representante de Consejo de Camara Industrial de Jalisco**	**FIRMA**
MTRO. GERARDO ESTEBAN SÁNCHEZ GONZÁLEZ **Representante de Coordinación General de Potencia Economica**	**FIRMA**
ING. MANUEL LEDEZMA ESPARZA **Representante de Director de Desarrollo Rural**	**FIRMA**
LIC. DANIEL CORTÉS FLORES **Órgano Interno de Control Con Voz**	**FIRMA**
PERLA YOLANDA URZUA VIRGEN **Secretaria Técnica Con Voz**	**FIRMA**

La presente hoja de firmas corresponde al fallo de la adjudicación de la licitación LPL 05/2026