MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO	Codigo:	Apo.4.1.4Fr002
	Fecha	31/01/2023
Apo.414 Fr.002 Cumplido para Pago	Versiòn	6

PARA: SUBDIRECCION FINANCIERA Y GRUPO DE CONTRATOS RADICADO No.: CP - CONS 1

DATOS GENERALES DEL CONTRATO

CONTRATO, ORDEN O CONVENIO No. 2 . 005 - 2022

NIT O DOCUMENTO DE IDENTIFICACION DEL CONTRATISTA 830060020

Radicado: 2-2023-015315
Bogotá D.C., 30 de marzo de 2023 11:00

OBJETO DEL CONTRATO, ORDEN O CONVENIO: CONTRATAR LA ACTUALIZACIÓN TECNOLOGÍA PARA REDES INALÁMBRICAS

No.Compromiso 140022

FECHA DE SUSCRIPCION DEL CONTRATO, ORDEN O CONVENIO: 25/10/2022

NOMBRE CONTRATISTA: GLOBAL TECHNOLOGY SERVICES GTS S.A.

VALOR DEL CONTRATO: 1,257,411,913.00 ADICIONALES: .00 VR CONTRATO MAS ADICIONES: 1,257,411,913.00

FECHA DE INICIO: 08/11/2022

FECHA DE TERMINACION: 31/03/2023

Adiciones y/o Cesiones del Contrato

Adicion No. 1	Fecha Adicion 19/12/2022	Desde 27/12/2022 Hasta 31/03/2023	Tiempo Adicion 0 anos - 3 meses y 5 dias	Objeto: OTROSÍ 1 DEL CONTRATO 2.005-2022. MEDIANTE EL CUAL SE MODIFICA PARCIALMENTE LA CLÁUSULA SEGUNDA ¿PLAZO¿, EN EL SENTIDO DE PRORROGAR LOS PLAZOS DE ENTREGA Y EJECUCIÓN HASTA EL 19 DE MARZO Y 31 DE MARZO DE 2023, RESPECTIVAMENTE.

DATOS ESPECIFICOS DEL PAGO

Tipo de Pago	No.	Condicion de Pago	Aclaracion	Vr.Pago	Iva Aplicado	Valor Iva	Amortizacion Anticipada	Total a Pagar
FACTURA NO.	11971	UNICO PAGO	CONTRATAR LA ACTUALIZACIÓN TECNOLOGÍA PARA REDES INALÁMBRICAS	1,056,648,666.38	19 %	200,763,246.61		1,257,411,912.99
					%			
			TOTALES	1,056,648,666.38		200,763,246.61		

TOTAL A PAGAR: 1,257,411,912.99

Anexos y No. de Folios

Factura	1	Cuenta de Cobro		Declaracion juramentada Seguridad Social	
Otros Anexos o Folios	27	Entrada a Almacen		Constancias de pago de la seguridad social	2
				Total de Folios Anexos	30

EXPEDIENTE 239/2023/FACTELEC CTO. 2.005-2022 - GLOBAL TECHNOLOGY SERVICES GTS S.A.

En calidad de Supervisor/Interventor del contrato enunciado, certifico que he verificado el cumplimiento a satisfaccion de las obligaciones que emanan del contrato, la acreditacion del pago de obligaciones con el sistema de seguridad social integral y las cifras y valores corresondientes al periodo certificado para el reconocimiento del pago que por este instrumento se acredita

SUPERVISORES Y/O INTERVENTORES

FIRMA: _____
NOMBRE: JAIME ALBERTO MOLINA SUAREZ
CARGO: SUBDIRECTOR ENCARGADO
CEDULA: 79279559

FIRMA: _____
NOMBRE: JUAN PABLO ROJAS MESA
CARGO: ASESOR
CEDULA: 80227517

FIRMA: _____
NOMBRE: JHOAN MANUEL ESPINOSA MONTILLA
CARGO: ASESOR
CEDULA: 93453561

Firmado digitalmente por:JAIME ALBERTO MOLINA SUAREZ
Asesor

Firmado digitalmente por:JUAN PABLO ROJAS MESA
ASESOR CODIGO 1020 GRADO 4

Firmado digitalmente por:JUAN PABLO ROJAS MESA
ASESOR CODIGO 1020 GRADO 4

Firmado digitalmente por:JHOAN MANUEL ESPINOSA MONTILLA
Profesional Especializado

MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO

SIED

1. Recepción Facturas Electrónicas y demás documentos para pago

Número de Radicado	Fecha de Radicado	Fecha de Presentación
1-2023-025353	27/03/2023 17:02	27/03/2023 17:02

Interesado - Facturas Electrónicas

º Tipo Documento : **NIT** º Identificación del Contratista : **830060020**

º Nombre del Contratista : **GLOBAL TECHNOLOGY SERVICES GTS SA** º Dirección del Contratista : **Calle 33 Bis N° 13 A 54**

º Correo Electrónico donde desea recibir la respuesta : **infofinanciera@gtscolombia.com**

º Digite su correo nuevamente : **infofinanciera@gtscolombia.com**

RECEPCIÓN FACTURAS ELECTRÓNICAS

º ¿Está corrigiendo una factura ya radicada anteriormente? : **NO**

º Nro. Contrato : **2.005** º Nro. Factura : **11969** º Fecha Factura : **27/03/2023**

º Concepto de la factura : **Suministro y configuración de AP y licenciamiento.**

Periodo del Servicio:

º Año : **2023** º Mes : **03**

º Nombre del Supervisor en el Ministerio de Hacienda : **Jaime Molina-Noe Hernandez**

[X] Mención Legal: La responsabilidad por la recolección, entrega y validez de la información requerida es responsabilidad exclusiva del Contratista

Expone / Solicita

Observaciones

Suministro y configuración de AP y licenciamiento en la nube con sus aditamentos y herrajes.

Asunto

Contratista: GLOBAL TECHNOLOGY SERVICES GTS SA - Nro. contrato: 2.005 - Concepto factura: Suministro y configuración de AP y licenciamiento. - Supervisor: Jaime Molina-Noe Hernandez

Casos seleccionados

º A) DOCUMENTOS AL PRESENTAR FACTURA ELECTRÓNICA:

Es obligatorio presentar la Representación Gráfica de la Factura Electrónica, los demás documentos son opcionales.

Documentos requeridos adjuntados

º 1. Representación gráfica de la factura electrónica (Archivo en PDF): Documento adjuntado Fra. 11969 Minhacienda Cto. 2005-2022.pdf

Identificador: WnlW1Jni7Jjzx5TN6NBmIgI7U/Q=

Documentos requeridos opcionales adjuntados

º 2. Factura Electrónica en formato de generación (Archivo en XML en estándar DIAN): Documento adjuntado Fra. 11969 Minhacienda Cto. 2005-2022.xml

Identificador: HefCASzYnxOSh25b2zy6NQ3n2Oo=

º 3. Reporte Olimpia Factura Electrónica (Archivo en PDF): Documento adjuntado Soporte Recibido Olimpia Fra. 11969.pdf

Identificador: JgYgm8NoSQR0dkGTLJJVl1axd9A=

º 4. Certificación del pago de Seguridad Social y Aportes Parafiscales (Archivo PDF): Documento adjuntado Parafiscales y pago SS Feb-Mar 23.pdf

Identificador: IWwWWUc+LpEMWxYmuYdaSdDcL4c=

º 5. Informe de ejecución o acta de entrega (Archivo en PDF): Documento adjuntado Apo.4.1.Fr.16 Informe de Ejecución Supervisión de Contrato 2005-2022firmado GTS.pdf

Identificador: gCAx54l4GTxYWJWPEFtJHEwQU18=

Avisos legales

Datos Personales

(*) Los datos facilitados por usted en este formulario pasarán a formar parte de bases de datos personales del Ministerio de Hacienda y Crédito Público obtenidas con ocasión del desarrollo de las funciones legales y constitucionales, y podrán ser utilizados para el ejercicio de las funciones propias en el ámbito de sus competencias. Así mismo y de conformidad con la Ley 1581 de 2012, reglamentada por el Decreto 1377 de 2013, de Protección de Datos de Carácter Personal, o las que hagan sus veces, usted podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición mediante comunicación presentada ante el Ministerio de Hacienda y Crédito Público, de igual manera podrá descargar y consultar nuestra Política de Tratamiento de Datos Personales disponible en el link : www.minhacienda.gov.co/webcenter/wccproxy/d?dDocName=WCC_CLUSTER-104160

GLOBAL TECHNOLOGY SERVICES
GTS S.A.

CALLE 33 BIS # 13A – 54

Bogotá, D.C,Bogotá, Colombia

NIT 830060020 - 5
Autorización de numeración de facturación electrónica
No. 18764039018563 del 03/11/2022 al 03/05/2023
Habilita numeración de:
11822 al 12000
Régimen: Impuesto sobre las ventas - IVA
Responsabilidad fiscal:
R-99-PN No Aplica - Otros

RESPONSABLE DE IVA - ACTIVIDAD ECONÓMICA 4651
NO SOMOS GRANDES CONTRIBUYENTES NI AUTORRETENEDORES
Correo electrónico: infofinanciera@gtscolombia.com

Cliente: MINISTERIO DE HACIENDA Y CREDITO PUBLICO
NIT 899999090 - 2
Dirección: CR 8 6 64
Codigo Cliente 04
Teléfono: 343 3000
Dirección Despacho:
Contacto:
Ciudad: Bogotá, D.C
Departamento: Bogotá
País: Colombia

Factura Electronica de Venta No. 11969
Fecha de emisión: 27/03/2023 04:00:00 PM
Fecha de validación DIAN: 27/03/2023 03:55:56 PM
Fecha de vencimiento: 06/04/2023
Plazo (Días): 10
Codigo de Moneda COP
Tasa de Cambio
Orden de Compra
Remisión
Pedido
Asesor
Aviso de Recibo

Item	Referencia	Descripción	Cant.	Unidad de Medida	Precio Unitario	Cargos y Descuentos	Impuestos	Rte Fte	Valor Total
1	1	ELEMENTO 1: Suministro y configuración de AP con sus aditamentos y herrajes de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No.1 del presente Contrato.	122,00	unidad	COP 5,036,731.09	COP 0.00	IVA(19%)		COP 614,481,193.28
2	2	ELEMENTO 2: Suministro y configuración de AP Tipo 2 con sus aditamentos y herrajes de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No. 1 del presente Contrato.	4,00	unidad	COP 6,896,754.62	COP 0.00	IVA(19%)		COP 27,587,018.49
3	3	ELEMENTO 3: Suministro y configuración de licenciamiento en nube para GESTIÓN Y CONTROL DE AP´S de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No. 1 del presente Contrato.	126,00	unidad	COP 1,181,494.12	COP 0.00	IVA(19%)		COP 148,868,258.82
4	4	ELEMENTO 4: Suministro y configuración de licenciamiento sobre control de acceso en red NAC 1000 usuarios, 100 BYOD de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No. 1 del presente Contrato.	1.000,00	unidad	COP 123,025.21	COP 0.00	IVA(19%)		COP 123,025,210.08
5	5	INSTALACION de todos los equipos - de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No. 1 del presente Contrato.	1,00	unidad	COP 79,692,846.22	COP 0.00	IVA(19%)		COP 79,692,846.22
6	6	TRANSFERENCIA DE CONOCIMIENTO CERTIFICADA - de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No. 1 del presente Contrato.	3,00	unidad	COP 16,557,215.97	COP 0.00	IVA(19%)		COP 49,671,647.90

Este documento corresponde a la representación gráfica de una factura electrónica de venta. Confirme el CUFE mediante lectura de este código bidimensional:

CUFE f78e83ed52d189023102b1c1e2a844e44a60d20e8fc7ad90586937713bea64eb244ef8245f3a47b0e8e44b0c07c2208b

Proveedor tecnológico: Comercio Electrónico en Internet CENET S.A. NIT 830057860 Software: misfacturas

GLOBAL TECHNOLOGY SERVICES
GTS S.A.

CALLE 33 BIS # 13A – 54

Bogotá, D.C,Bogotá, Colombia

NIT 830060020 - 5
Autorización de numeración de facturación electrónica
No. 18764039018563 del 03/11/2022 al 03/05/2023
Habilita numeración de:
11822 al 12000
Régimen: Impuesto sobre las ventas - IVA
Responsabilidad fiscal:
R-99-PN No Aplica - Otros

7	7	TRANSFERENCIA DE CONOCIMIENTO NO CERTIFICADA - de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No. 1 del presente Contrato.	5,00	unidad	COP 2,664,498.32	COP 0.00	IVA(19%)		COP 13,322,491.60

Total de items: 7
Observaciones
#$13-01-01-000;2.005-2022;Jaime.Molina@minhacienda.gov.co#$

Forma de pago: Crédito
Medio de pago: Consignación bancaria

RECOMENDACIÓN: Favor reportar el pago de esta factura al e-mail infofinanciera@gtscolombia.com
Transferir a la cuenta ahorros Banco AV Villas No.382012748
Cuenta corriente Banco AV Villas No. 382012706

Subtotal:	COP 1,056,648,666.38

IVA(19%)	COP 200,763,246.61

Impuestos:	COP 200,763,246.61
Retenciones:	COP 0.00
Cargos de la factura:	COP 0.00
Descuentos de la factura:	COP 0.00
Anticipos:	COP 0.00
Total	COP 1,257,411,913.00
Neto a pagar	COP 1,257,411,913.00

Este documento corresponde a la representación gráfica de una factura electrónica de venta. Confirme el CUFE mediante lectura de este código bidimensional:

CUFE f78e83ed52d189023102b1c1e2a844e44a60d20e8fc7ad90586937713bea64eb244ef8245f3a47b0e8e44b0c07c2208b

Ingresa documento correctamente

Factura Electrónica <factura.electronica@olimpiait.com>

Lun 27/03/2023 16:30

Para: Ginna Leandra Carranza Vargas <auxiliarcontable2@gtscolombia.com>

MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO

Bogotá,03/27/2023 04:30 PM

Reciba un cordial saludo:

Factura Electrónica de Olimpia IT, informa que se generaron los siguientes:
Ingresa documento correctamente **11969**

CONTENIDO DEL INFORME

1. CONDICIONES DEL CONTRATO

Número de Contrato:	2.005-2022
Nombre del Contratista:	GLOBAL TECHNOLOGY SERVICES GTS S.A.
Periodo informe:	MARZO 2023
Supervisores:	NOE HERNANDEZ RODRIGUEZ, JUAN PABLO ROJAS MESA JHOAN MANUEL ESPINOSA MONTILLA
Área perteneciente:	Dirección Tecnología

2. **OBJETO DEL CONTRATO**: Contratar la actualización tecnología para redes inalámbricas.

3. OBLIGACIONES DEL CONTRATO, ACTIVIDADES EJECUTADAS Y PRODUCTOS ENTREGADOS

Las obligaciones del contratista son las siguientes:

OBLIGACIONES ESPECÍFICAS: El contratista deberá ejecutar las actividades descritas a continuación:
El contratista deberá suministrar los componentes con las características, cantidades requeridas y con las condiciones de funcionalidad que se describen a continuación:
…"

1.1.1. Los equipos y elementos que conforman la actualización tecnológica deberán quedar totalmente implementados y operando correctamente, para lo cual se deberá entregar el hardware, software, licenciamiento, certificados públicos y privados y demás componentes que sean necesarios.

1.1.2. Los equipos y elementos que conforman la actualización tecnológica se deben entregar integrados y estabilizados con la infraestructura de red LAN y directorio activo que posee actualmente el Ministerio.

1.1.3. Todos los equipos y elementos ofertados deberán ser nuevos de última tecnología, contar con el licenciamiento y las últimas versiones de software generadas por el fabricante que se encuentren estables y en funcionamiento al momento de la implementación en el MHCP.

1.1.4. Los equipos y elementos entregados deberán ser de un mismo fabricante tanto en los componentes de hardware como de software.

1.1.5. Se deberá contemplar por parte del contratista la reubicación física de los equipos, de tal manera que se garantice para los nuevos AP´s su correcto funcionamiento y cobertura en cada una de las áreas proyectadas.

1.1.6. El contratista deberá realizar la instalación de los equipos AP de tal manera que haya una total cobertura de conexión inalámbrica en los lugares designados por el MHCP, para ello el contratista previo a la instalación deberá entregar una propuesta de ubicación de equipos con su respectivo mapa de Calor el cual será aprobado por el Supervisor del contrato.

1.1.7. La red inalámbrica deberá estar en capacidad de correr pruebas en tiempo real de usuarios y equipos, para determinar fallas y causas raíz.

1.1.8. Los equipos y elementos deberán tener compatibilidad con sistemas operativos de equipos fijos o móviles (Mac, Windows, IOS, Android).

1.1.9. La red inalámbrica deberá estar en capacidad de identificar los dispositivos que se conecten de la red, adicionalmente deberá estar en capacidad de aplicar inteligencia artificial para perfilar los dispositivos que conformaran la red Wifi del MHCP.

1.1.10. La red inalámbrica deberá estar en capacidad de generar reportes y estadísticas, adicionalmente extraer información de

conexiones, usuarios, aplicaciones, dispositivos e integrarse vía APIs a otros sistemas de seguridad como SIEMs, Firewalls, syslogs sin costo para la Entidad.

1.1.11. La red inalámbrica deberá estar en capacidad de generar múltiples informes sobre el funcionamiento de la red enfocados a su funcionamiento.

1.1.12. La plataforma de gestión deberá ser amigable e intuitiva para configurar y personalizar la red.

1.1.13. La red inalámbrica deberá permitir la integración de directorio activo, de tal manera que permita el acceso a equipos y usuarios registrados el acceso automático a la red. En caso de que un dispositivo no se encuentre registrado la solución deberá permitir el ingreso de los usuarios como un BYOD a través delportal de visitantes.

1.1.14. La red inalámbrica deberá permitir la posibilidad de tener diferentes perfiles, para administradores del sistema. Adicionalmente la solución deberá permitir que los administradores sean integrados por medio de RADIUS o TACACS de tal manera que usen sus credenciales de directorio activo.

1.1.15. La configuración de red para usuarios deberá ser intuitiva de fácil acceso y segura.

1.1.16. El Portal cautivo de la red inalámbrica deberá permitir la inclusión de los logos del MHCP bajo previa aprobación del Supervisor del contrato. Adicionalmente el Portal deberá ser altamente configurable de tal manera que los campos puedan ser elegidos de una lista de opciones incluyendo la inclusión de logos.

1.1.17. La solución deberá permitir el ingreso por medio de redes sociales mínimo cinco (5) en caso de que el MHCP así lo requiera.

1.1.18. La solución deberá permitir el ingreso de un usuario invitado por medio de autenticación mediante un portal cautivo personalizado para visitantes elaborado por el contratista y aprobado previamente por el supervisor del contrato.

1.1.19. La plataforma deberá permitir el monitoreo y en caso de ser necesario, el bloqueo de un visitante.

1.1.20. La plataforma deberá permitir la creación de categorías de usuarios, de tal manera que se puedan asignar roles y perfiles con funcionalidades específicas para cada perfil.

1.1.21. La plataforma deberá permitir la asignación, gestión, modificación y actualización de contraseñas en caso de que el MHCP así lo requiera.

1.1.22. Se deberá ejecutar por parte del contratista todas las labores de instalación, configuración, estabilización y demás elementos que sean necesarios para cumplir con los requerimientos técnicos y funcionales especificados, de tal forma que se conforme un sistema completo, integrado y enteramente operacional.

1.1.23. La red inalámbrica deberá tener la capacidad de identificar dispositivos o clientes inalámbricos (Ipad, Iphone, Mac, SmarthPhone Android, etc.) y permitir aplicar políticas de seguridad y de control de tráfico por tipo o grupo de dispositivos.

1.1.24. La red inalámbrica deberá tener la capacidad de aplicar políticas de seguridad y control de tráfico por tipo o grupo de perfiles de usuario definidos por el MHCP.

1.1.25. La red inalámbrica deberá contar con todos los certificados vigentes durante el tiempo de soporte, los cuales serán generados por el proveedor y emitidos por una entidad certificadora sin incluir ningún costo adicional.

1.1.26. La red inalámbrica deberá ser escalable en todos sus componentes, tanto en software para actualizaciones de acuerdo con la versión emitida por el fabricante, y hardware para adición de nuevos dispositivos de acuerdo con las especificaciones técnicas.

1.1.27. Se deberá implementar una solución de Control de Acceso a la Red- NAC en alta disponibilidad para la red inalámbrica.

1.1.28. El ministerio proveerá los servidores que requiera la solución NAC siempre y cuando sean máquinas virtuales (VMWARE) con sistema operativo Windows Server 2016 o superior.

1.1.29. El Contratista deberá realizar el diseño y las Configuraciones que sean necesarias del portal cautivo incluyendo parametrizaciones hasta la correspondiente aprobación del supervisor del Contrato.

1.1.30. El contratista deberá realizar las Configuraciones de automatización de todos los procesos que requieran funcionamientos automáticos de uso según las necesidades específicas del MHCP estas serán indicadas y aprobadas por el Supervisor del contrato

1.1.31. El contratista deberá realizar la Configuración y puesta en funcionamiento de los códigos SSID según los perfiles designados por el MHCP, esta se deberá realizar usando las mejores prácticas y recomendaciones exigidas por el supervisor del contrato.

1.1.32. El contratista deberá suministrar, en caso que se requiera, los dispositivos power injector para alimentar eléctricamente los equipos Access point. Para esto deberá tener en cuenta que los equipos Access point se conectaran en switches marca Cisco modelo WS-C2960X-48FPD-L, los cuales cumplen con los standares IEEE 802.3 af y IEEE 802.3 at, donde los puertos son PoE+ de 30Watts.

ELEMENTO 1: ACCESS POINT Tipo 1	
CANTIDAD	122
Tecnologia Inalámbrica	• Los APs deben incluir como mínimo: • Doble radio. • Soporte para doble banda 802.11ax con OFDMA y MU-MIMO. • Data rates mínimo de 4.8 Gbps en 5Ghz y 575Mbps en 2.4ghz. • Tecnología two spatial stream. • MU-MIMO 4x4:4 (5GHz) y 2x2:2 (2.4Ghz) • Mínimo 5.3 Gbps desempeño agregado • Soporte Wi-Fi Multimedia (WMM). • Soporte Bluetooth 5 para casos de usos de IOT y servicios de localización. • mínimo 16 SSID por radio. • soporte de asociación de hasta 500 clientes por radio. • Asignación y selección de canal de manera automática, así como los niveles depotencia del AP. • mínimo de 500 clientes asociados por radio. • Debe contar con mecanismos automáticos que migren a los clientes hacia el punto de acceso que puede prestar el mejor nivel de servicio en todo momento, basado en información de ubicación del cliente, capacidades del dispositivo cliente, condiciones del entorno RF y congestión de los puntos de acceso, sin que requiera intervención del usuario y que aplique a las distintas marcas y modelos de dispositivos presentes en el mercado. Esto para evitar problemas asociado a sticky clients. • Para garantizar la protección de inversión, alineación con las tendencias tecnológicas de la industria, soporte y vigencia tecnológica y estar preparados para los requerimientos futuros, confirmar que los equipos de comunicación ofertadosdeben corresponder a una marca o fabricante que figure como líder en el cuadrante de Cuadrante Mágico Gartner para soluciones de acceso LAN Wired and Wireless durante los últimos tres años (2019, 2020 y 2021 y para su acreditación deberá presentar el informe correspondiente a cada año. • Los modelos de AP's ofertados deben ser capaces de trabajar sin controlador, con Controlador y en la nube. No se aceptarán soluciones OEM, los AP's, Controladora y Software deberán ser nativos fabricados por la marca. La controladora debe ser en nube.
Estándares IEEE	Los AP's deben soportar como mínimo los siguientes estándares de la industria: - IEEE 802.11a - IEEE 802.11b - IEEE 802.11g - IEEE 802.11i - IEEE 802.11n - IEEE 802.11ac - IEEE 802.11ax - 802.11ac very high throughput (VHT) support: VHT20/40/80/160 - IEEE 802.1X - IEEE 802.3af/at/ clase 4 o superior - IEEE 802.3 az - IEEE 802.3 bz. - Wi-FI Certified a, b, g, n, ac, ax - WPA, WPA2, WPA3
Interfaces	Incluir como mínimo dos (2) interfaces RJ45 con:

	• Un interfaz RJ-45 100/1000/2500BASE-T autosensing con capacidad de soportar alimentación eléctrica vía estándar PoE 802.3af/at clase 4 o superior. Otra • interface mínima RJ45 10/100/1000Base T autosensing • Soporte de LACP entre las interfaces del equipo • Interface USB 2.0 (Conector Tipo A) • Una interfaz de administración serial • Radio Bluethoot 5 • Radio Zigbee
Controlador inalámbrico	El AP deben estar en capacidad de operar como mínimo en los siguientes modos: • Como equipo AP stand-alone. • Como equipo AP controlado al integrarse a un Wireless Access Controller físico (tipo apliance) o gestionado desde nube • Los APs deberán tener la capacidad de operar en modo controlado usando su propio sistema operativo, sin necesidad de una controladora física, ni licencias adicionales. Permitiendo crecer al menos 128 AP´s por clúster • Operar en modo Air monitor o su equivalente según lo denomine cada fabricante y de ser necesario incluir el licenciamiento para habilitar dicha funcionalidad • Operar como analizador de espectro. • Debe contar con mecanismos que permitan Zero Touch Provisioning para implementación automática al contar con una conexión a Internet sin intervención de servicio técnico especializado.
Seguridad	El AP debe incluir como mínimo soporte para: • IEEE 802.11i. • Algoritmo de cifrado: AES, TLS, EAP, TTLS, TKIP, WPA, WPA2 y WPA3. • Integración de Wireless Intrusion Prevention (WIP) para ofrecer protección ymitigación en contra de amenazas. • Servicios de seguridad para identificación, clasificación y bloqueo de ips, archivos o URLs maliciosos. • Debe contar con un statefull firewall en capa 7, con Deep packet inspector que facilite la visibilidad de más de 2000 aplicaciones de uso común, y permita aplicar políticas granulares de seguridad, QoS, control de ancho de banda y filtrado web. • Capacidad de manejar roles por usuario y políticas basadas en identidad. • WMM o WMM-PS. • Debe incluir un modulo Trust Anchor o Trust Platform (TPM) en el equipo, componente fisico, (no se admite software) para asegurar la integridad de la plataforma para un almacenamiento seguro de credenciales y llaves de comunicación. También para un boot seguro del equipo asegurando que el hardware y software es de propiedad del fabricante y no está corrupto.
Funciones adicionales de seguridad	El AP debe tener como mínimo las siguientes funcionalidades: • Detección y protección contra intrusiones. • Integración con solución de NAC. El fabricante deberá contar con solución decontrol de acceso Enterprise de la misma marca. • Coexistencias Avanzada Celular (Advanced Cellular Coexistence ACC) o tecnología homologa para evitar interferencias causadas por redes celulares. • Proteccion de intrusion inalambrica Integrada para proteger, mitigar y eliminar riesgos y equipos externos que eliminen la necesidad de

	sensores de RF y equipos de seguridad externos . • Integración con solución para BYOD. • Transmit Beamforming (TxBF), Passpoint (Hotspot 2.0), Dynamic Frecuency • Selection (DFS), Maximum Ratio Combining (MRC), Low-Density Parity Check(LDPC).
Calidad del servicio	Calidad del servicio para Aplicaciones de comunicaciones unificadas, que incluyan skype for business y Teams, con videoconferencia encriptada, voz, chat y escritorios compartidos. Para esta funcionalidad no deben usarse UTM´s adicionales o externos
Acceso	• Se debe incluir una funcionalidad que se integre en los radios de las bandas de 2.4GHz y 5GHz que activamente optimice el ambiente RF incluyendo ancho de canal, selección de canal y potencia de transmisión. • Funcionalidad para habilitar al AP para monitorear y reportar el consumo de potencia del equipo y opcionalmente hacer ajustes de habilitación o deshabilitacion de funciones según la potencia disponible, opción de personalizar las funciones a desactivar. - Autenticación por EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS, PEAP. - Autenticación por MAC con configuración local o RADIUS. - Aislamiento de usuario inalámbrico directo en Capa 2. • RADIUS
Administración	Minino soporte para: - SNMP v2c y v3. - HTML con SSL. - Consola serial.
Alimentación Eléctrica	Debe incluir alimentación PoE basada en el standard IEEE 802.3 af/at/ y/o bt.
Certificaciones	Incluir mínimo las siguientes: • UL2043 plenum rating • Wi-Fi Alliance: - • Wi-Fi CERTIFIED a, b, g, n, ac, ax • WPA • WPA2 • WPA3 • Enterprise with CNSA option • Personal(SAE), Enhnced Open (OWE) • WMM, WMM-PS, Wi-Fi Vantage, W-Fi Agile Multiband • Passpoint (release 2) • Bluetooth SIG • Ethernet Alliance (PoE, PD device, class 4) • ETS 300 019 class 3.2 environments
Regulaciones	• FCC/ISED • CE Marked RED Directive 2014/53/EU, Low Voltage Directive 2014/35/EU o certificaciones internacionales equivalentes tales como EN 55022/CISPR22, FCC part 15 y demás que apliquen para emisión y compatibilidad electromagnética • RED Directive 2014/53/EU • EMC Directive 2014/30/EU • Low Voltage Directive 2014/35/EU • UL/IEC/EN 60950

	• EN 60601-1-1, EN60601-1-2
Garantía de fábrica	• *Se debe proveer una garantía mínima de tres (3) años contados a partir del recibo a satisfacción por parte del MHCP.* • *No deben tener anuncio de EOS (fin de venta) ni EOL (fin de vida) a la fecha del cierre del proceso.*
Servicios para el HW	Servicios de reposición de partes y piezas (Hardware): • *Duración: 3 años, contados a partir del recibo a satisfacción por parte del MHCP.* • *Nivel: Siguiente día laborable (NBD)*
Servicios para el SW	Servicios de actualización del sistema operativo y atención a casos: • Duración: 3 años, contados a partir del recibo a satisfacción por parte del MHCP. • Nivel: 24x7
ELEMENTO 2: ACCESS POINT Tipo 2	
CANTIDAD	4
Tecnología Inalámbrica	Los APs deben incluir como mínimo: • Doble radio. • Debe contar con antenas internas omnidireccionales. • Soporte para doble banda 802.11ax con OFDMA y MU-MIMO. • Tecnología two spatial stream. • Mínimo 4x4:4 (5GHz y 2.4GHz) • Mínimo 2.9 Gbps desempeño agregado en mundo real • Soporte Wi-Fi Multimedia (WMM). • Soporte Bluetooth 5 para casos de usos de IOT y servicios de localización. • mínimo 16 SSID por radio. • soporte de asociación de hasta 1000 clientes por radio. • Asignación y selección de canal de manera automática, así como los niveles de potencia del AP. • Debe contar con mecanismos automáticos que migren a los clientes hacia el punto de acceso que puede prestar el mejor nivel de servicio en todo momento, basado en información de ubicación del cliente, capacidades del dispositivo cliente, condiciones del entorno RF y congestión de los puntos de acceso, sin que requiera intervención del usuario y que aplique a las distintas marcas y modelos de dispositivos presentes en el mercado. Esto para evitar problemas asociado a sticky clients. • Para garantizar la protección de inversión, alineación con las tendencias tecnológicas de la industria, soporte y vigencia tecnológica y estar preparados para los requerimientos futuros, confirmar que los equipos de comunicación ofertados deben corresponder a una marca o fabricante que figure como líder en el cuadrante de Cuadrante Mágico Gartner para soluciones de acceso LAN Wired and Wireless durante los últimos tres años (2019, 2020 y 2021 y para su acreditación deberá presentar el informe correspondiente a cada año. • Los modelo de AP's ofertados deben ser capaces de trabajar sin controlador, con Controlador y en la nube. No se aceptarán soluciones OEM, los AP's, Controladora y Software deberán ser nativos fabricados por la marca. La controladora debe ser en nube. • Debe incluir power injector
Estándares IEEE	Los AP's deben soportar mínimo los siguientes estándares de la industria: - IEEE 802.11a - IEEE 802.11b - IEEE 802.11g - IEEE 802.11i - IEEE 802.11n

	- IEEE 802.11ac - IEEE 802.11ax - 802.11ac very high throughput (VHT) support: VHT20/40/80/160 - IEEE 802.1X - IEEE 802.3af/at/ clase 4 o superior - IEEE 802.3 az - IEEE 802.3 bz. - Wi-FI Certified a, b, g, n, ac, ax - WPA, WPA2, WPA3
Interfaces	● Incluir mínimo dos (2) interfaces RJ45 con: ● - Dos(2) interfaces RJ-45 100/1000/5000BASE-T autosensing con capacidad de soportar alimentación eléctrica vía estándar PoE 802.3af/at clase 4 o superior. ● - Soporte de LACP entre las interfaces del equipo ● - Interface USB 2.0 (Conector Tipo A) ● - Una interfaz de administración serial ● - Radio Bluethoot 5 ● - Radio Zigbee
Controlador inalámbrico	● El AP deben estar en capacidad de operar mínimo en los siguientes modos: ✓ Como equipo AP stand-alone. ✓ Como equipo AP controlado al integrarse a un Wireless Access Controller físico (tipo apliance) o gestionado desde nube ✓ Los APs deberán tener la capacidad de operar en modo controlado usando su propio sistema operativo, sin necesidad de una controladora física, ni licencias adicionales. Permitiendo crecer al menos 128 AP´s por clúster ✓ Operar en modo Air monitor o su equivalente según lo denomine cada fabricante y de ser necesario incluir el licenciamiento para habilitar dicha funcionalidad. ✓ Operar como analizador de espectro. ● Debe contar con mecanismos que permitan Zero Touch Provisioning para implementación automática al contar con una conexión a Internet sin intervención de servicio técnico especializado.
Seguridad	El AP debe incluir como mínimo soporte para: ● IEEE 802.11i. ● Algoritmo de cifrado: AES, TLS, EAP, TTLS, TKIP, WPA, WPA2 y WPA3. ● Integración de Wireless Intrusion Prevention (WIP) para ofrecer protección ymitigación en contra de amenazas. ● Servicios de seguridad para identificación, clasificación y bloqueo de ips, archivos o URLs maliciosos. ● Debe contar con un statefull firewall en capa 7, con Deep packet inspector que facilite la visibilidad de más de 2000 aplicaciones de uso común, y permita aplicar políticas granulares de seguridad, QoS, control de ancho de banda y filtrado web. ● Capacidad de manejar roles por usuario y políticas basadas en identidad. ● WMM o WMM-PS. ● Debe incluir un modulo Trust Anchor o Trust Platform (TPM) en el equipo, componente fisico, (no se admite software) para asegurar la integridad de la plataforma para un almacenamiento seguro de credenciales y llaves de comunicación. También para un boot seguro del equipo asegurando que el hardware y software es de propiedad del fabricante y no está corrupto.

Funciones adicionales de seguridad	El AP debe incluir como mínimo siguientes funcionalidades: • Detección y protección contra intrusiones. • Integración con solución de NAC. El fabricante deberá contar con solución decontrol de acceso Enterprise de la misma marca. • Coexistencias Avanzada Celular (Advanced Cellular Coexistence ACC) o tecnología homologa para evitar interferencias causadas por redes celulares. • Proteccion de intrusion inalambrica Integrada para proteger, mitigar y eliminar riesgos y equipos externos que eliminen la necesidad de sensores de RF y equipos de seguridad externos . • Integración con solución para BYOD. • Transmit Beamforming (TxBF), Passpoint (Hotspot 2.0), Dynamic Frecuency Selection (DFS), Maximum Ratio Combining (MRC), Low-Density Parity Check(LDPC).
Calidad del servicio	Calidad del servicio para Aplicaciones de comunicaciones unificadas, que incluyan skype for business y Teams, con videoconferencia encriptada, voz, chat y escritorios compartidos.Para esta funcionalidad no deben usarse UTM´s adicionales o externos
Acceso	Se debe incluir una funcionalidad que se integre en los radios de las bandas de 2.4GHz y 5GHz que activamente optimice el ambiente RF incluyendo ancho de canal, selección de canal y potencia de transmisión. -Funcionalidad para habilitar al AP para monitorear y reportar el consumo de potencia del equipo y opcionalmente hacer ajustes de habilitación o deshabilitacion de funciones según la potencia disponible, opción de personalizar las funciones a desactivar. • Autenticación por EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS, PEAP. • Autenticación por MAC con configuración local o RADIUS. • Aislamiento de usuario inalámbrico directo en Capa 2. • RADIUS
Administración	Como mínimo soporte para: • SNMP v2c y v3. • HTML con SSL. • Consola serial.
Alimentación Eléctrica	Debe incluir alimentación PoE basada en el standard IEEE 802.3 af/at/ y/o bt.
Certificaciones	Mínimo las siguientes: • UL2043 plenum rating • Wi-Fi Alliance: - • Wi-Fi CERTIFIED a, b, g, n, ac, ax • WPA • WPA2 • WPA3 • Enterprise with CNSA option • Personal(SAE), Enhnced Open (OWE) • WMM, WMM-PS, Wi-Fi Vantage, W-Fi Agile Multiband • Passpoint (release 2) • Bluetooth SIG • Ethernet Alliance (PoE, PD device, class 4) • ETS 300 019 class 3.2 environments
Regulaciones	• FCC/ISED • CE Marked, RED Directive 2014/53/EU, Low Voltage Directive 2014/35/EU o certificaciones internacionales equivalentes tales como EN 55022/CISPR22,

	FCC part 15 y demás que apliquen para emisión y compatibilidad electromagnética. • RED Directive 2014/53/EU • EMC Directive 2014/30/EU • Low Voltage Directive 2014/35/EU • UL/IEC/EN 60950 • EN 60601-1-1, EN60601-1-2
Garantía de fábrica	• *Se debe proveer una garantía mínima de tres (3) años contados a partir del recibo a satisfacción por parte del MHCP.* • *No deben tener anuncio de EOS (fin de venta) ni EOL (fin de vida) a la fecha del cierre del proceso.*
Servicios para el HW	Servicios de reposición de partes y piezas (Hardware): • Duración: 3 años, contados a partir del recibo a satisfacción por parte del MHCP. • Nivel: Siguiente día laborable (NBD)
Servicios para el SW	Servicios de actualización del sistema operativo y atención a casos: • Duración: 3 años, contados a partir del recibo a satisfacción por parte del MHCP. • Nivel: 24x7

Seguridad	
Manejo de intrusiones	Debe mínimo: • Brindar información sobre la detección de APs intrusos en la red. • Brindar información general sobre el servicio de Wireless IDS. • Informar sobre ataques a la infraestructura de la red • Informar sobre fuentes de interferencia • Ser capaz de mostrar información por horas, días y semanas.
Seguridad	• Debe tener comunicación segura mediante certificados entre el dispositivo y la gestión en Nube. • Soporte de conexiones HTTPS
Control de Aplicaciones	
Aplicaciones	Debe mínimo: • Brindar gráficas donde se muestre cuáles son las aplicaciones más usadas en la red y los principales destinos, sitios de WEB más visitados y clasificarlos en categorías de tipo y de confiabilidad • Categorizar las aplicaciones y mostrar el uso por categoría. • Categorizar e indicar los sitios WEB visitados por los clientes tanto por tipo de sitio, como por nivel de confianza - Con la información recopilada debe ser capaz de establecer políticas de control para permitir, bloquear o limitar la velocidad.
Alta Disponibilidad	
Estructura redundante	El esquema de servicio en Nube debe contar con tolerancia a fallas. La gestión no dependa de un solo servidor, sino que debe contar con una arquitectura que brindecontinuidad del servicio ante la falla de uno o más servidores.
Disponibilidad	El servicio de administración en nube debe contar con una disponibilidad al menos del 99,95%.
Servicio de Reportes	

Reportes	Debe ser capaz mínimo de: • Enviar reportes a cuentas específicas de correo electrónico. • Generar reportes que ayuden al cumplimiento de PCI • Brindar reportes de inventario de los equipos. • Generar reportes de capacidad, tráfico, clientes. • Generar reporte de las aplicaciones y los sitios más visitados. • Brindar reportes de tráfico por dispositivo y por usuario. • Generar reporte de las aplicaciones y las sesiones de los clientes. • Los reportes deben de ser generados en archivos PDF.
Servicio de Portal cautivo para Visitas	
Portal Cautivo	Debe ser capaz mínimo de: • Brindar el servicio de portal cautivo para usuarios invitados o visitantes de la red. • Permitir ajustar la pantalla del portal cautivo mediante logo y texto. • Permitir múltiples métodos de autenticación, tales como el anónimo, el autoservicio y el login vía red social como LinkedIn, Facebook, Google y Twitter • Permitir la creación de accesos temporales por parte de la recepcionista.
Servicio de análisis de Presencia	
Presencia	Debe estar en capacidad de mínimo de: • Generar gráficas e información en tiempo real e histórica de los usuarios que rondan por una determinada área del establecimiento. • Generar información del tiempo que tarda el usuario en determinado lugar. • Permitir establecer métricas de comparación entre sitios para la toma de decisiones • Permitir ajustar parámetros de tiempo y cantidad de señal según sea requerido. • - Mostrar estadísticas de usuarios que solo pasaron por el sitio, de usuarios que se conectaron por periodos cortos y de los usuarios que se mantuvieron en sitio por periodos más extensos.
Servicio de análisis de Red	
Calidad de Conexión	La solución de administración en Nube debe estar en capacidad de indicar la salud de la conexión de los usuarios, con al menos los siguientes parámetros: • Asociación de usuario. • Autenticación de usuario. • Asignación de direccionamiento vía DHCP. • Conexión al Portal Cautivo. • Información del DNS.
Licenciamiento y Suscripción	
Servicio inicial	La Solución de administración en Nube ofertada debe estar en capacidad demanejar 125 dispositivos al momento de la compra.
Escalabilidad	El crecimiento de la solución de administración ofertada debe realizarse únicamente mediante la adición de licenciamiento, con una capacidad de crecimiento en el orden de las decenas de miles de nodos.
Expiración del servicio	Si a futuro el cliente decide no renovar las licencias de servicio, al expirar la suscripción de estas toda la infraestructura de red debe seguir operando, y debe existirla opción para cambiar a un modo de operación y administración local.
Garantía y Servicios	

Servicios para el SW	• El servicio de gestión en Nube se debe brindar por un periodo mínimo de 3años. • Durante el periodo del servicio se deben brindar las actualizaciones de software de los dispositivos gestionados. • La herramienta debe contar con un soporte en modalidad 24x7 durante el periodo del servicio,

ELEMENTO 3: NAC	
Descripción	Especificaciones técnicas mínimas requeridas: • Hardware de propósito específico para habilitar Solución de Control deAcceso a la red cableada, inalámbrica y VPN. • Solución debe soportar acceso diferenciado para dispositivos corporativos, contratistas, invitados, IoT y BYOD. • Soporte para ambientes de red multi-vendor • Perfilamiento y asignación de acceso basado en roles • Soporte integrado para servicios RADIUS, TACACS+, enforcement SNMP e integraciones con soluciones de seguridad de terceros mediante APIs

	• Debe Incluir capacidades de Guest, portal cautivo, RADIUS o TACACS+, perfilamiento de dispositivos, Entidad Certificadora sin costo adicional • Capacidad de adicionar servicios de: BYOD y Postura de Seguridadagregando licenciamiento adicional
CANTIDAD	Hasta 1000 usuarios y 100 licencias para BYOD
Características generales	
Capacidad	La solución deberá manejar hasta 10.000 sesiones RADIUS activas concurrentes por cada máquina virtual en alta disponibilidad.
Servicios incluidos enlicenciamiento base	Deberá incluir en el licenciamiento base los siguientes servicios: • 802.1X • Autenticación por MAC Address • RADIUS/TACACS+ • Enforcement a través de SNMP • Perfilamiento de dispositivos • Integraciones con terceros mediante REST APIs
Seguridad contextual	La política de seguridad deberá permitir tomar en consideración elementos contextuales como: horario, ubicación, tipo de dispositivo, versión de SO y nombre del dispositivo, entre otros
Hardware/Software	Disponible en versión máquina virtual
Soporte Multivendor	Soporte para Assessment de postura, perfilamiento y autenticación web en ambientes de red multi-vendor y basado en protocolos estándar RADIUS y RADIUS CoA
Control de acceso unificado	Deberá controlar el acceso de usuarios y dispositivos a través de la red cableada (switches), inalámbrica (access points y controladores WiFi) y VPN (firewalls y concentradores VPN) de manera unificada
Servicios AAA	Deberá soportar la aplicación de políticas contextuales mediante servicios AAA: RADIUS, RADIUS CoA, TACACS+ y SNMP
Reportería	Deberá incluir sin costo adicional un componente de monitoreo y reportería con información en tiempo real e histórica sobre usuarios y dispositivos conectados, alertas, detalle de autenticación y autorización, consumo de anchos de banda

		Métodos de Perfilamiento	Deberá soportar los siguientes métodos de perfilamiento: • Activo: Nmap, WMI, SSH, SNMP • Pasivo: MAC OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFLOW, Puerto 'SPAN', HTTP User-Agent, IF-MAP • Integrados y de terceros: Desde la solucion de BYOD y de chequeo de postura, EMM/MDM, Rapid7, Cisco device sensor.
		Certificados digitales	La solución deberá ser capaz de actuar como entidad certificadora Root o Intermediaria
		Acceso de externos via Portal Cautivo (Invitados, contratistas, clientes)	
		Funcionalidades clave	• Deberá proveer la opción de autoregistro con confirmación de cuenta vía impresión de ticket, SMS o e-mail, para asegurar que los datos ingresadospor los usuarios seran válidos • Deberá permitir que antes de que un usuario externo se pueda conectar, elacceso deba ser aprobado por un usuario corporativo (auto-registro con sponsor) • Deberá permitir que la validez de las cuentas de invitados sea configurable en base a tiempo, anchos de banda utilizados, horario de conexión, entre otros • Deberá permitir la personalización total del portal cautivo con logos, publicidad, videos, encuestas, etc • Deberá proveer la opción de acceder a la red a través de las redes sociales Facebook, Twitter, inkedin y Google • Deberá ajustar de manera automática el tamaño del portal, de acuerdo al dispositivo con el cual se conectan los usuarios • Deberá proveer encriptación del tráfico sobre una red abierta mediante el estándar PEAP-Public • Deberá permitir la asignación de políticas de acceso basadas en roles, para poder asegurar anchos de banda, acceso a recursos específicos y duración de las conexiones, de acuerdo con el tipo de invitado • Deberá permitir la integración con sistemas gestión de huéspedes, pacientes y cobro, tales como: Micros Opera PMS, Protel PMS, Silverbyte Optima PMS, Agilysis Visual One PMS, etc • Deberá permitir realizar Caching de direcciones MAC por cierta cantidad de tiempo, para evitar que los usuarios recurrentes tengan que introducir constantemente sus credenciales • Deberá permitir asignar accesos basados en roles a los operadores que crean o modifican las cuentas de usuarios
		Protocolos para losservicios AAA	La solución deberá soportar al menos los siguientes protocolos para los servicios AAA: • RADIUS, RADIUS CoA, TACACS+, autenticación web, SAML 2.0 • EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS) • PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS. EAP-PEAP-Public,EAP-PWD) • TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5,PAP, CHAP) • EAP-TLS • PAP, CHAP, MSCHAPv1 y 2, EAP-MD5 • OAuth2 • Autenticación de Máquina en dominio Windows • SMB v2/v3 • Autenticación vía MAC (para dispositivos que no soportan 802.1x) • Online Certificate Status Protocol (OCSP) • SNMP generic MIB, SNMP private MIB • Common Event Format (CEF), Log Event Extended Format (LEEF)

		Fuentes de Autenticación	La solución deberá soportar las siguientes fuentes de autenticación sin licenciamiento o plugins adicionales: • Microsoft Active Directory • RADIUS • Cualquier directorio basado en protocolo LDAP • MySQL, Microsoft SQL, PostGRES, Oracle 11g y cualquier servidor SQLODBC-compliant • Servidores de Token • Base de datos interna • Kerberos • Microsoft Azure Active Directory (viaSAML y OAuth2.0) • Google G Suite
		Estándares RFC	El sistema deberá soportar los siguientes estándares RFC: • RFC 2246 The TLS Protocol Version 1.0 • RFC 2248 Network Services Monitoring MIB • RFC 2407 Internet IP Security Domain of Interpretation for ISAKMP • RFC 2408 ISAKMP • RFC 2409 The Internet Key Exchange (IKE) • RFC 2548 Microsoft Vendor-specific RADIUS Attributes • RFC 2759 Microsoft PPP CHAP Extensions, Version 2 • RFC 2865 Remote Authentication Dial In User Service (RADIUS) • RFC 2866 RADIUS Accounting • RFC 2869 RADIUS Extensions • RFC 2882 Network Access Servers Requirements: Extended RADIUS Practices • RFC 3079 Microsoft Point to Point Encryption • RFC 3576 Dynamic Authorization Extensions to RADIUS • RFC 3579 RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP) • RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)Usage Guidelines • RFC 3748 Extensible Authentication Protocol (EAP) • RFC 3779 X.509 Extensions for IP Addresses and AS Identifiers • RFC 4017 Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs • RFC 4137 State Machines for Extensible Authentication Protocol (EAP) Peerand Authenticator • RFC 4301 Security Architecture for IP • RFC 4302 IP Authentication Header • RFC 4303 IP Encapsulating Security Payload (ESP) • RFC 4308 Cryptographic Suites for IPsec • RFC 4346 TLS Protocol • RFC 4514 Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names • RFC 4518 Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation • RFC 4809 Reqs for IPsec Certificate Mgmt Profile • RFC 4849 RADIUS Filter Rule Attribute • RFC 4851 EAP-FAST • RFC 4945 PKI Profile for IKE/ISAKMP/PKIX • RFC 5216 The EAP-TLS Authentication Protocol

			• RFC 5246 The Transport Layer Security (TLS) Protocol • RFC 5280 Internet X.509 Public Key Infrastructure • RFC 5281 EAP-TTLSv0 • RFC 5282 Authenticated Encryption and IKEv2 • RFC 5755 Internet Attribute Certificate Profile for Authorization • RFC 5759 Suite B Certificate and Certificate Revocation List (CRL) Profile • RFC 6818 Updates to the Internet X.509 Public Key • RFC 6960 X.509 Internet Public Key Infrastructure • RFC 7030 Enrollment over Secure Transport • RFC 7296 Internet Key Exchange Protocol Version 2 • RFC 7321 ESP y AH • RFC 7468 Textual Encodings of PKIX, PKCS, and CMS Structures • RFC 7815 Minimal Internet Key Exchange Version 2 (IKEv2) Initiator Implementation • RFC 8032 Edwards-Curve Digital Signature Algorithm (EdDSA) • RFC 8247 The Internet Key Exchange v2 (IKEv2)
		Servicios adicionales	Deberá tener la capacidad de adicionar de manera modular servicios de: enrolamiento de dispositivos personales en entornos corporativos (BYOD) y Postura de Seguridad sobre PCs corporativos
		Licenciamiento	El licenciamiento deberá ser perpetuo. No se admiten licencias por suscripción.
		Integración con soluciones de terceros	Deberá tener la capacidad de integración via REST-based APIs, de manera nativa y sin costo adicional de licenciamiento, con soluciones de Seguridad Perimetral (Ej: CheckPoint, Palo Anto, Fortinet, etc), MDM/EMM (Ej: Citrix, MobileIron, AirWatch), sistemas de gestión de tickets (Ej: Service Now, y multiples factores de autenticación (Ej: DUO, RSA SecurID), UEBA
		Segmentación dinámica	Se requiere que la solución aplique el control de acceso y segmentación dinámica basada en roles, para evitar el uso de múltiples VLANs para aplicar políticas de seguridad
		Perfilamiento de dispositivos	La solución deberá soportar perfilamiento para despliegues con direccionamiento IP fijo
		Social Login	La solución deberá soportar autenticación vía social login con Facebook, Linkedin, Google y Twitter
		Integraciones delportal cautivo	El portal cautivo deberá ser capaz de integrarse con soluciones de PMS, pago por uso y publicidad
		Privilegios sobre losdispositivos	Se requiere que la solución pueda aplicar políticas de acceso, perfilamiento y autenticación sin necesidad de habilitar privilegios de administración sobre los equipos
		Perfilamiento de dispositivos	Se requiere que la solución pueda perfilar y categorizar los dispositivos que se conectan a la red sin licenciamiento adicional
		Alta Disponibilidad	La Alta disponibilidad debe permitir modalidad activo/active. Se requiere que el failover en caso de fallas sea automático, sin necesidad derealizar tareas manuales
		Single Sign On	La solución deberá soportar SAML tanto como SP e IdP y el protocolo Oauth para habilitar Single Sign On con aplicaciones y portales externos

		Fuentes de Autenticación	La solución deberá soportar bases de dato SQL como fuente de autenticación sin necesidad de agregar licenciamiento o plugins adicionales
		Portal cautivo	El portal cautivo deberá ser altamente personalizable
		Certificados digitales	La solución deberá ser capaz de actuar como entidad certificadora Root o Intermediaria en el caso de certificados públicos deben ser proporcionados por el proveedor.
		Servicios para el SW	Servicios de actualización del sistema operativo y atención a casos - Duración: 3 años. - Nivel: 24x7

1.3. GARANTIA: El contratista deberá garantizar que todos los elementos y/o componentes de hardware y software operen en perfecto estado de funcionamiento mediante reemplazo y/o reparación y/o actualización y/o configuración del elemento y/o componente defectuoso, para lo cual deberá:

1.3.1. Ofrecer mínimo tres (3) años de garantía de fábrica para todos los componentes de hardware y software de los elementos instalados, con fin de mantenerlos en perfecto estado de funcionamiento mediante reemplazo y/o reparación y/o actualización y/o configuración del componente defectuoso. El tiempo de la garantía que se contabilizará a partir de la fecha de la entrega, instalación y aceptación por parte de lasupervisión del contrato.

1.3.2. Los equipos y elementos reemplazados y las reparaciones a los mismos que se requieran deberán contar con garantía del fabricante a través del contratista.

1.3.3. Cuando se realice un reemplazo de equipo, el equipo que falle deberá ser retirado de las instalaciones de la Entidad y el equipo nuevo pasará a ser propiedad del Ministerio. Al equipo nuevo le aplicará la garantía solicitada en el presente numeral hasta cumplir el plazo de la garantía del equipo que se reemplazó.

1.3.4. La garantía debe incluir todos los costos de operación, en los que debe contemplar mano de obra, transporte y los repuestos, sin que esto genere costos adicionales a la Entidad.

1.3.5. El contratista deberá realizar una (1) jornada de revisión preventiva de la solución cada año durante el tiempo mínimo de garantía requerida, dicha jornada deberá ser realizada en las instalaciones del Ministerio e incluirá como mínimo limpieza interna y externa, confirmación de funcionalidad, ajustes mecánicos y electrónicos y revisión general, además de la verificación de todas las funciones básicas y operativas del sistema y sus elementos. Esta actividad no deberá generar costos adicionales y deberá ser previamente coordinada con el supervisor del contrato.

1.3.6. Brindar asistencia técnica para la solución de incidentes frente al mal funcionamiento, fallas, des-configuraciones que se puedan presentar en las soluciones objeto del presente proceso.

1.3.7. Atender los requerimientos de garantía y asistencia técnica, sin costo adicional para el Ministerio cuantas veces lo requieran los equipos y elementos bajo las siguientes condiciones:

a. Modalidad de atención 5 x 8, cinco días a la semana 8 horas diarias.
b. Tiempo de solución no mayor a 4 horas contadas a partir del reporte del incidente.
c. Atender servicios de manera telefónica o remota a fin de determinar la falla reportada
d. Cuando se haya determinado el problema y no se encuentre solución telefónica o remota, el Contratista debe asignar un técnico para que se desplace a las oficinas de la Entidad, en un tiempono mayor de cuatro (4) horas contadas a partir de haber determinado la no solución remota otelefónica
e. Si el equipo no logra ser reparado en sitio, el Contratista podrá retirarlo de las instalaciones delMinisterio, mientras es reparado, independiente del tipo de daño presentado, deberá ser remplazado en un plazo máximo de cuatro (4) horas por otro de características iguales o 15ajor15t15v, pero con la misma funcionalidad. Si después de un (1) día calendario el 15ajor15t no ha sido reparado, éste deberá ser remplazado de manera 15ajor15t15ve por otro que posea como mínimo las mismas características, marca, modelo, licencias y funcionalidades, en un término no superior a dos (2) días calendario. Para los eventos anteriores, los días se contarán a partir del reporte del incidente. Los equipos defectuosos que se remplacen deberán ser retirados y los que se instalen en su reemplazo pasarán a ser propiedad del Ministerio. De lo anterior se suscribirá un acta por parte del Contratista y el Ministerio en la que se indique el serial, las características y funcionalidades del 15ajor15t que reemplazará al que 15ajor15t la falla.
f. Los repuestos que sean necesarios para efectuar la reparación y el correcto funcionamiento de cualquiera de los

	elementos o partes cubiertos correrán por cuenta del contratista. Los repuestos empleados para remplazar elementos defectuosos serán de la misma o 16ajor calidad al existente
1.4. TRANSFERENCIA DE CONOCIMIENTO	
1.4.1.	Durante la ejecución del contrato, brindar para 3 personas transferencia de conocimiento certificada por el fabricante en la administración e implementación de la solución Wifi-implementada, con una intensidad horaria de mínimo 24 horas
1.4.2.	Durante la ejecución del contrato, brindar transferencia de conocimiento no certificada para 5 personas en conceptos básicos, monitoreo y operación de la solución Wifi-implementada, con unaintensidad horaria de mínimo 12 horas
1.5. RECURSO HUMANO	
Para la ejecución del contrato, proponente deberá poner a disposición del Ministerio dos (2) ingenieros, con elsiguiente perfil:	
1.5.1.	Ingeniero especialista 1: • Un ingeniero cuyo núcleo básico de conocimiento sea: "Ingeniería de Sistemas, Telemática y Afines" o "Ingeniería Eléctrica y Afines" o "Ingeniería Electrónica, Telecomunicaciones y Afines". • Certificación vigente de la matrícula profesional expedida por el respectivo Consejo Profesional de Ingeniería que lo regule. • Experiencia mínima certificada de 2 años en la implementación o soporte o instalación de redes inalámbricas. • Certificación de cursos o entrenamientos en redes inalámbricas, expedida por el fabricante.
1.5.2.	Ingeniero especialista 2: • Un ingeniero cuyo núcleo básico de conocimiento sea: "Ingeniería de Sistemas, Telemática y Afines" o "Ingeniería Eléctrica y Afines" o "Ingeniería Electrónica, Telecomunicaciones y Afines". • Certificación vigente de la matrícula profesional expedida por el respectivo Consejo Profesional de Ingeniería que lo regule. • Experiencia mínima certificada de 4 años en la implementación o soporte o instalación de redes inalámbricas. • Certificación de cursos o entrenamientos en diseño o curso avanzado de redes inalámbricas, expedida por el fabricante.
1.6. INSTALACIÓN Y SOPORTE	
1.6.1.	Deberá dejar las áreas y bienes del Ministerio donde se instalen los equipos en las mismas condiciones de estética y acabados que presentaban antes de iniciar las labores de instalación.
1.6.2.	Deberá suministrar e instalar los herrajes, bases, soportes y demás elementos requeridos para la instalación del equipo ya sea en pared o techo. Es muy importante que los materiales y accesorios para su instalación correspondan a los acabados - colores de la estructura de cada sitio.
1.6.3.	Todos los componentes adicionales requeridos para la instalación y puesta en operación de los elementos solicitados con las funcionalidades descritas en el presente Anexo deberán ser asumidos por el contratista sin costo adicional para Ministerio, se excluyen el cableado lógico y el suministro eléctrico.
1.6.4.	Ejecutar todas las labores de instalación, configuración, estabilización y demás elementos que sean necesarios para cumplir con los requerimientos técnicos y funcionales especificados, de tal forma que se conforme un sistema completo, integrado y enteramente operacional
1.6.5.	El Cableado lógico y el suministro eléctrico de los equipos correrá por parte del MHCP, por lo que el contratista deberá proporcionar la ubicación exacta del Punto de Datos y Eléctrico necesario para el correcto funcionamiento del equipo AP. En caso de requerirse modificar la ubicación de un punto por error u omisión del contratista, este deberá asumir el costo y los materiales requeridos para la reubicación del cableado lógico y suministro eléctrico.
1.6.6.	El contratista deberá contar con todas las herramientas y elementos necesarios para la ejecución del contrato, tales como computadores, multímetros, andamios, gruas y escaleras, entre otros.
1.6.7.	Se deberá entregar al MHCP los planos de comunicación o conexión entre componentes y/o equipos, a escala 1:100 en papel y medio magnético en formato para Autocad 2016 y/o superior, firmados por cada uno de los responsables con su respectiva matrícula profesional dando cumplimiento a cada una de la Normativa y estándares vigentes en Colombia aplicables a la solución.
1.6.8.	Entregar los manuales técnicos de los elementos instalados y documentación de la operación, administración de la solución implementada, así como un documento con las configuraciones realizadas.
1.6.9.	El recurso humano deberá estar dotado de las herramientas necesarias para el desempeño de sus labores y elementos de seguridad industrial.
1.6.10.	El Recurso humano deberá contar Curso avanzado de trabajo seguro en alturas o reentrenamiento impartido por un ente certificador acreditado, tomado en el último año anterior a la fecha de inicio de ejecución.
1.6.11.	El contratista deberá cumplir todas las condiciones y normas de bioseguridad del Ministerio de Hacienda y Crédito Público, para lo cual deberá diligenciar los formatos correspondientes y acatar las medidas establecidas.

Avance: El contratista GLOBAL TECHNOLOGY SERVICES GTS S.A. realizó la entrega definitiva y en operación de los equipos y elementos para la actualización tecnología para redes inalámbricas del Ministerio de Hacienda y Crédito Público, así como de los planos de conexión, manuales técnicos, configuraciones realizadas de los elementos instalados y documentación de la operación, administración de la solución implementada y cumplió a satisfacción con los requerimientos técnicos mínimos especificados en el contrato en la cláusula 7) OBLIGACIONES ESPECÍFICAS.

PRODUCTOS ENTREGADOS

El contratista GLOBAL TECHNOLOGY SERVICES GTS S.A realizó la entrega en operación y a satisfacción de los siguientes elementos:

No.	DESCRIPCIÓN	CANTIDAD
1	ELEMENTO 1: Suministro y configuración de AP con sus aditamentos y herrajes de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No.1 del presente Contrato.	122
2	ELEMENTO 2: Suministro y configuración de AP Tipo 2 con sus aditamentos y herrajes de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No.1 del presente Contrato.	4
3	ELEMENTO 3: Suministro y configuración de licenciamiento en nube para GESTIÓN Y CONTROL DE AP'S de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No.1 del presente Contrato.	126
4	ELEMENTO 4: Suministro y configuración de licenciamiento sobre control de acceso en red NAC 1000 usuarios, 100 BYOD de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No.1 del presente Contrato.	1000
5	INSTALACION de todos los equipos –de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No.1 del presente Contrato.	1
6	TRANSFERENCIA DE CONOCIMIENTO CERTIFICADA –de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No.1 del presente Contrato.	3
7	TRANSFERENCIA DE CONOCIMIENTO NO CERTIFICADA –de acuerdo con los REQUERIMIENTOS TECNICOS MINIMOS, contenidos en el Anexo No.1 del presente Contrato.	5

Adicionalmente a los elementos relacionados en la anterior tabla se hizo entrega de lo siguiente:

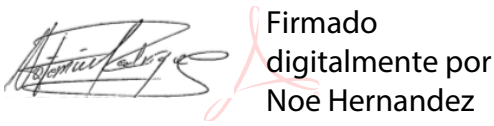
- Los planos de comunicación o conexión entre componentes y/o equipos, a escala 1:100 en papel y medio magnético en formato para Autocad 2016, firmados por cada uno de los responsables con su respectiva matrícula profesional dando cumplimiento a cada una de la Normativa y estándares vigentes en Colombia aplicables a la solución.
- Los manuales técnicos de los elementos instalados
- Documentación de la operación
- Documentación administración de la solución implementada
- Documentación con las configuraciones realizadas.

Lo anterior con de acuerdo con lo requerido en la cláusula 7) OBLIGACIONES ESPECÍFICAS del contrato.

GLOBAL TECHNOLOGY SERVICES GTS S.A
Representante Legal

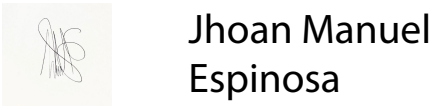
En la calidad de supervisores del contrato nos permitimos avalar el contenido del informe y el avance en la ejecución del mismo de acuerdo a lo descrito.

El contrato no presenta a la fecha dificultades en su ejecución, ni situaciones exógenas que afecten el normal desarrollo del mismo.



NOE HERNANDEZ RODRIGUEZ
Supervisor

JUAN PABLO ROJAS MESA
Supervisor



JHOAN MANUEL ESPINOSA MONTILLA
Supervisor

EL SUSCRITO REVISOR FISCAL DE

GLOBAL TECHNOLOGY SERVICES GTS S.A.
NIT. 830.060.020-5

CERTIFICO

1. Por medio del presente documento me permito certificar que la empresa GLOBAL TECHNOLOGY SERVICES GTS SA con NIT 830.060.020-5 ha cumplido con los aportes al Subsistema de la Seguridad Social en Salud durante los últimos seis (6) meses (octubre de 2022 a marzo de 2023); así como de los Aportes Parafiscales, al Subsistema de Pensiones y de Riesgos Profesionales correspondiente a los últimos seis (6) meses (septiembre de 2022 a febrero de 2023), de acuerdo con lo establecido en el artículo 50 de la Ley 789 de 2002, en el artículo 23 de la Ley 1150 de 2007, Ley 1562 de 2012 y demás normas que las adicionen, complementen o modifiquen y con la presentación del impuesto sobre la renta del año 2021. Las planillas por los periodos mencionados son:

GTS – PLANTA		
Planilla	**Fecha pago**	**Valor**
9441151050	06-10-22	$81.045.800
9442411961	03-11-22	$98.995.300
9443873119	07-12-22	$78.150.400
9445157928	05-01-23	$112.472.600
9446606448	06-02-23	$74.597.300
9446607890	06-02-23	$ 3.737.100
9447783843	03-03-23	$68.565.500
9447789361	03-03-23	$ 3.304.000

2. Que la sociedad se beneficia de la exoneración del pago de los aportes parafiscales a favor del Servicio Nacional de Aprendizaje e Instituto Colombiano de Bienestar Familiar ICBF, correspondientes a los trabajadores que devengan, individualmente considerados, menos de diez (10) salarios mínimos mensuales legales vigentes, en cumplimiento de lo dispuesto en la Ley 1819 de 2016.

3. Que la sociedad se beneficia de la exoneración del pago de los aportes al sistema de salud, correspondientes a los trabajadores que devengan, individualmente considerados, menos de diez (10) salarios mínimos mensuales legales vigentes, en cumplimiento de lo dispuesto en la Ley 1819 de 2016.

La presente certificación se expide en Bogotá, a los tres (03) días del mes de marzo de 2023, por solicitud del interesado.

MIGUEL EDUARDO VÁSQUEZ BARRERA
Revisor Fiscal
TP-109.108 - T
Por delegación de **Latin Professional S.A.S.**

Bogotá, 03 de marzo de 2023
CER-047-23
Latin Professional S.A.S.

aportes en línea

Comprobante de Pago

DATOS GENERALES DEL APORTANTE							
Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono
NIT 830060020	5	GLOBAL TECHNOLOGY SERVICES GTS S.A.	B - MENOS DE 200 COTIZANTES	842088-ADMINISTRATIVO	CL 33 BIS 13A 54	BOGOTA-BOGOTA D.E.	5932200

DATOS GENERALES DE LA LIQUIDACION			
Periodo Pensión	**2023-02**	Periodo Salud	**2023-03**
Fecha límite de pago	**2023/03/06**	Fecha de pago	**2023/03/03**
Dias de mora	**0**	Tasa de mora	**26.16%**

TOTALES	
Valor a pagar	**$68,565,500**
Intereses de mora	**$0**
Saldos e incapacidades	**$0**
Valor total	**$68,565,500**

DATOS DE LA TRANSACCIÓN	
Clave planilla	**9447783843**
Clave de pago	**1949714401**
Banco	**BANCO ITAU**

2023/03/03 12:52 PM

aportes en línea

Comprobante de Pago

DATOS GENERALES DEL APORTANTE							
Identificación	dv	Razon Social	Clase Aportante	Sucursal Principal	Direccion	Ciudad-Departamento	Teléfono
NIT 830060020	5	GLOBAL TECHNOLOGY SERVICES GTS S.A.	B - MENOS DE 200 COTIZANTES	AJUSTES	CALLE 33 BIS 13A 54	BOGOTA-BOGOTA D.E.	5932200

DATOS GENERALES DE LA LIQUIDACION			
Periodo Pensión	**2023-02**	Periodo Salud	**2023-03**
Fecha límite de pago	**2023/03/06**	Fecha de pago	**2023/03/03**
Dias de mora	**0**	Tasa de mora	**26.16%**

TOTALES	
Valor a pagar	**$3,304,000**
Intereses de mora	**$0**
Saldos e incapacidades	**$0**
Valor total	**$3,304,000**

DATOS DE LA TRANSACCIÓN	
Clave planilla	**9447789361**
Clave de pago	**1949926721**
Banco	**BANCO ITAU**

2023/03/03 12:54 PM