Bogotá D.C.,

Asunto: SOLICITUD DE INFORMACIÓN PARA ESTUDIO DE MERCADO

Respetados señores:

Atentamente solicito su colaboración, a efectos de obtener información para consolidar estudios de mercado sobre los bienes, obras y/o servicios que se citan a continuación:

<table>
<tr><td>OBJETO</td><td colspan="3">Adquirir la renovación tecnológica de las soluciones de comunicaciones y seguridad VPNSSL Ivanti del MHCP.</td></tr>
<tr><td rowspan="8">UNSPSC</td><td>CÓDIGO UNSPSC</td><td colspan="2">DESCRIPCIÓN</td></tr>
<tr><td>81111800</td><td colspan="2">Servicios de sistemas y administración de componentes de sistemas</td></tr>
<tr><td>81112200</td><td colspan="2">Mantenimiento y soporte de software</td></tr>
<tr><td>81112300</td><td colspan="2">Mantenimiento y soporte de hardware de computador</td></tr>
<tr><td>43222500</td><td colspan="2">Equipo de seguridad de red</td></tr>
<tr><td>43233200</td><td colspan="2">Software de seguridad y protección</td></tr>
<tr><td>81112500</td><td colspan="2">Servicios de alquiler o arrendamiento de licencias de software de computador</td></tr>
<tr><td colspan="3">Nota 1: Si considera que el bien o servicio está clasificado en otro UNSPSC, favor indicarlo.</td></tr>
<tr><td rowspan="2">DESCRIPCIÓN Y/O ALCANCE</td><td colspan="2">ESPECIFICACIONES TÉCNICAS MÍNIMAS</td><td>COTIZACIÓN ALTERNATIVA</td></tr>
<tr><td colspan="2">Ver anexo No. 1 No. 1 – REQUERIMIENTOS TECNICOS MINIMOS.</td><td>En caso de que aplique o se requieran</td></tr>
<tr><td rowspan="2">DURACION DEL CONTRATO</td><td>DIAS HABILES ___ CALENDARIO_____</td><td>MESES</td><td>AÑO</td></tr>
<tr><td colspan="3">El término de duración del contrato que se suscriba será hasta el 20 de diciembre del 2024 contado a partir de la expedición del correspondiente registro presupuestal y aprobación de las garantías que debe constituir el contratista.
Para el estudio de mercado, los interesados deberán cotizar los 3 periodos (1, 2 o 3 años) para el licenciamiento, con base en lo cual,</td></tr>
</table>

	el Ministerio determinará y definirá, las condiciones de la contratación.		
PLAZO PARA LA ENTREGA DE LOS BIENES Y/O SERVICIOS	**DIAS HABILES _____** **CALENDARIO _____**	**MESES**	**AÑO**
	El contratista tendrá hasta el 30 de octubre del 2024 para la entrega de los bienes objeto del contrato, así como de la instalación e implementación de las soluciones, contados a partir del registro presupuestal y aprobación de la garantía única que debe constituir el contratista.		
LUGAR DE EJECUCIÓN	La ejecución del contrato será la ciudad de Bogotá, D.C. en las instalaciones del Ministerio de Hacienda y Crédito Público y de manera virtual en el evento de requerirse, previa autorización del Supervisor del contrato, bajo herramientas tecnológicas autorizadas por el Ministerio de Hacienda y Crédito Público en la ciudad de Bogotá.		
FORMA DE PAGO	El valor del contrato a suscribir se pagará, por intermedio de la Coordinación de Pagaduría de la Subdirección Financiera de este Ministerio, al CONTRATISTA, con sujeción a la disponibilidad del P.A.C. (Programa anual mensualizado de Caja), a través de un único pago, una vez se acredite la entrega, instalación e implementación de las soluciones de VPN SSL IVANTI que hacen parte de la renovación tecnológica, de la Entidad. Dicho pago se efectuara con sujeción a la disponibilidad del PAC, dentro de los diez (10) días hábiles siguientes a la radicación en la Subdirección Financiera, del cumplido a satisfacción por parte del supervisor designado para tal efecto, previa presentación del informe respectivo sobre la ejecución del contrato, la certificación de los pagos a los sistemas de seguridad social integral por parte del CONTRATISTA, la factura correspondiente y los demás documentos que se requieran para tal efecto, así como del registro del cargue de dichos soportes en SECOP II, conforme al procedimiento e instructivos para la recepción y trámite de documentos para pago establecido por el MINISTERIO.		

VALIDEZ DE LA COTIZACIÓN	La Entidad requiere que la cotización tenga validez como mínimo de Noventa (90) días Calendario. En la cotización debe relacionar su período de validez
OFERTA ECONOMICA	Ver Anexo No.2 "COTIZACION ECONOMICA"

ESPACIO PARA DILIGENCIAR POR EL COTIZANTE O PROPONENTE			
GARANTIA DE CALIDAD DE BIENES Y/O SERVICIOS *	**En término o plazo**	**Adicional o alternativa**	**En monto o valor**

COTIZACIÓN BÁSICA		**COTIZACIÓN ALTERNATIVA ***	
Detallar CUANDO COMPRENDA VARIOS ITEMS, SE DEBE COTIZAR INIVIDUALMENTE CADA UNO	**VALOR UNITARIO**	Detallar CUANDO COMPRENDA VARIOS ÍTEMS, SE DEBE COTIZAR INDIVIDUALMENTE CADA UNO	**VALOR UNITARIO**
VALOR TOTAL (incluido IVA)		**VALOR TOTAL (incluido IVA)**	

NOTA: Si el cotizante encuentra que algo falta, no es procedente o es diferente a lo consignado en la descripción técnica de la necesidad, es importante que lo manifieste, justificando la razón que sustenta el cambio, para que el Ministerio, previo análisis, determine la procedencia de la sugerencia. Para tal fin deberá determinar los costos de la cotización alternativa.

Agradecemos se sirva remitir la información respectiva a más tardar el día 26 de julio de 2024, a través de correo electrónico invtecnologia@minhacienda.gov.co o laura.duran@minhacienda.gov.co o a la siguiente dirección: Carrera 8 No. 6C-38 de la ciudad de Bogotá a nombre de la Dirección de Tecnología del Ministerio de Hacienda y Crédito Público**.**

Cordialmente,

RICARDO FERNELIX RIOS ROSALES
Director de Tecnología

Elaboró: Laura Duran/Sandra Londoño

* No comprende las garantías propias del contrato, tales como cumplimiento, calidad, salarios y prestaciones

** Si el cotizante desea presentar una propuesta alternativa a la cotización solicitada por el Ministerio, debe cumplir con las condiciones de técnicas mínimas de la cotización básica.

ANEXO No.1
REQUERIMIENTOS TECNICOS MÍNIMOS

1.	**REQUERIMIENTOS GENERALES** La renovación tecnológica de las soluciones de comunicaciones y seguridad VPN SSL IVANTI del MHCP se refiere al cambio de las plataformas actuales, que se encuentran por fuera de soporte del fabricante, por nuevas infraestructuras las cuales deben ser entregadas, instaladas, implementadas y migradas con las siguientes características:
1.1.	Proveer las soluciones de VPN SSL IVANTI con entrega, instalación, implementación y migración de acuerdo con la siguiente descripción:

ITEM	DESCRIPCION
1. SOLUCIÓN DE VPN SSL PARA SIIF NACIÓN	Dos equipos Ivanti **ISA 8000f** (Hardware), cada uno con licenciamiento para 2.000 usuarios
2. SOLUCION VPN SSL PARA OTROS AMBIENTES Y TRABAJO REMOTO	Un equipo Ivanti Virtual Appliance **ISA 8000-VS-GLD-D** con licenciamiento para 3.500 usuarios
3. SOLUCION VPN SSL PRUEBAS DE CARGA	Un equipo Ivanti Virtual Appliance **ISA 6000-VS-GLD** con licenciamiento para 1.000 usuarios
4. SOLUCION VPN SSL NUBE AZURE DRP	Un equipo Ivanti Virtual Appliance **ISA 6000-VAZ-S-GLD** con licenciamiento para 2.000 usuarios

	 **Nota:** Solución de VPN SSL hace referencia a equipos físicos o virtuales (appliance), ya sea en sitio o en nube, licencias, software y configuraciones.
1.2.	Las actividades que resulten para la renovación de las soluciones descritas en el numeral 1.1, se deben realizar bajo las siguientes condiciones: **a)** Acompañamiento permanente por parte de expertos del fabricante IVANTI previo y durante la instalación, migración, implementación y estabilización. **b)** Soporte permanente en línea con el fabricante IVANTI, de tal forma que los eventos que se presenten sean atendidos y corregidos de forma oportuna, sin que se genere interrupción de los servicios. **c)** Realizar el levantamiento de información de los componentes y configuraciones de las de las plataformas actuales que deberán ser renovadas dentro del presente proceso. **d)** Entregar a la supervisión del contrato la documentación que contenga las configuraciones, diagramas y las actividades de migración, implementación y estabilización realizadas para cada uno de los ítems. **e)** Cada una de las soluciones de VPN SSL del numeral 1.1. deberán quedar debidamente migradas, instaladas, configuradas, puestas en producción, funcionando correctamente y licenciadas con todas las funcionalidades requeridas. **f)** El software que se instalará en las soluciones VPN SSL adquiridas deberá ser de la última versión estable recomendada por el fabricante en el momento de la instalación y que soporte las funcionalidades de los sistemas que SIIF Nación, SGPR y MHCP. **g)** El ítem 1 debe ser configurado en alta disponibilidad, para lo cual deben entregar, actualizar, licenciar, configurar e integrar los componentes o software adicional que se requieran y sus costos deben ser incluidos en la misma.
1.3.	El contratista deberá contemplar todos los elementos y los recursos necesarios para la instalación, migración implementación, integración, estabilización y funcionamiento de las soluciones de VPN SSL para los servicios y aplicaciones del

	MHCP y SIIF NACIÓN, a fin de lograr el correcto funcionamiento y operatividad sin generar costos adicionales para la Entidad. La instalación de los equipos se realizará en racks estándar de 19 pulgadas (rieles, conectores, cables de poder, entre otros). Los racks son suministrados por el Ministerio.
1.4.	Con el fin de migrar las actuales soluciones a las adquiridas, el contratista deberá: **a)** Validar y registrar las configuraciones de los servicios, conexiones, tráfico, integraciones, entre otras, que actualmente se encuentran implementadas en las soluciones de VPN SSL. **b)** Elaborar un plan de trabajo siguiendo las recomendaciones del fabricante, las mejores prácticas del mercado y las opciones de optimización, para la instalación, configuración, migración e implementación por cada una de las soluciones descritas en el numeral 1.1. Este plan de trabajo se debe presentar al supervisor del contrato dentro del primer mes posterior al inicio de la ejecución del contrato. **c)** Por cada ítem del numeral 1.1 presentar un diagrama de la infraestructura en el que incluya las soluciones adquiridas y la integración con la infraestructura del MHCP y/o SIIF NACIÓN. Estos diagramas se deben presentar al supervisor del contrato dentro de los 45 días calendario posteriores al inicio de la ejecución del contrato. **d)** Ejecutar las labores definidas en el plan de trabajo a fin de garantizar la correcta instalación, configuración, migración, implementación, optimización e integración de las soluciones VPN SSL, con las funcionalidades y servicios requeridos y aplicando las políticas, normas y procedimientos fijados por el Ministerio. La ejecución de estas labores deberá realizarse bajo la modalidad de control de cambio en ventanas de tiempo acordadas con la supervisión del contrato, de tal forma que se minimice el riesgo de afectación de los actuales servicios que tiene la Entidad y que serán objeto de migración a las nuevas soluciones.
1.5.	Realizar las pruebas pertinentes con el fin de garantizar el correcto funcionamiento de cada una de las soluciones. Como mínimo las siguientes pruebas: a) Conectividad interna y externa

	b) Alta disponibilidad c) Integración con infraestructura de firewalls Check Point, swtiches CISCO, directorio activo Microsoft. d) Funcionalidades solicitadas Las pruebas efectuadas se realizarán en horario que no interrumpan los servicios que actualmente se encuentran en operación en la Entidad. Las pruebas y la hora en la cual se efectúen serán avaladas por el Ministerio y se programarán de forma independiente para cada uno de los ítems del numeral 1.1 del presente anexo.
1.6.	El contratista deberá entregar soporte del fabricante IVANTI por el tiempo de duración establecido en el contrato contado a partir del recibo a satisfacción de la renovación de la solución, la asistencia técnica directa con el fabricante, incluyendo lo siguiente: a) Actualizaciones de software, parches y services packs liberados. b) Acceso a las bases de datos de conocimiento de soporte y foros de los productos. c) Abrir o escalar casos directamente al fabricante para casos de criticidad e impacto alto y recibir soporte remoto o telefónico 30 minutos después de abierto el caso. d) Reemplazo de los equipos por fallas recurrentes o definitivas. El contratista debe garantizar la continuidad de los servicios del equipo afectado mediante equipos físicos o virtuales de las mismas características o superiores mientras se realiza el reemplazo definitivo del equipo que presenta la falla.
2.	**ITEM 1: SOLUCIÓN DE VPN SSL PARA SIIF NACIÓN**
CARACTERISTICAS TECNICAS GENERALES DE LA SOLUCIÓN	
2.1.	La solución de VPN SSL debe tener las siguientes características: **a.** Solución de propósito específico conformada por equipos físicos denominados "*Appliance*". **b.** Licenciamiento del software requerido para la solución adquirida con su correspondiente garantía y soporte técnico cubiertos por el fabricante. El servicio de soporte debe ser prestado por el tiempo de duración del

	licenciamiento adquirido en el contrato contados a partir del recibo a satisfacción por parte de la supervisión. (Ver numeral 1.6) **c.** Equipos implementados en alta disponibilidad, de manera tal que, ante la falla de uno de los equipos, otro pueda asumir los servicios y la carga de forma automática del equipo que falla, sin restricción de tiempo, de servicio, ni recurso con relación al funcionamiento normal en producción, garantizando la continuidad de los niveles de seguridad, número de usuarios y servicios implementados de forma transparente a los usuarios. **d.** Los equipos deben ser instalados en los dos (2) Datacenter de la Entidad y garantizar la alta disponibilidad en cada Datacenter. El Ministerio proporcionará VLAN Extendida y/o enrutamiento entre Datacenters. **e.** La conmutación en caso de falla de alguno de los appliances no debe implicar la perdida de conexiones; es decir, no deben reestablecerse nuevas sesiones.
2.2.	Se debe realizar la migración de las configuraciones y funcionalidades que se tienen implementadas en la actual solución '**portal2' y 'SPGR'**. Así como la validación del funcionamiento de las mismas en la nueva infraestructura, puesta en producción y estabilización.
2.3.	Cada uno de los equipos de la solución de VPN SSL deben contar con las siguientes características: **a.** Equipo físico de propósito específico tipo "appliance" de VPN SSL Ivanti ISA 8000f. **b.** Deben contar con un sistema operativo pre-endurecido específico para seguridad que sea compatible con el equipo. **c.** Cada equipo debe inicialmente tener capacidad para **2.000 usuarios concurrentes** y poder incrementar el número de usuarios sin necesidad de realizar cambios de hardware. **d.** Debe permitir un Throughput de mínimo de 5.9 Gbps para túnel ESP. **e.** Debe permitir un Throughput de mínimo de 3.8 Gbps para túnel SSL. **f.** Debe contar con memoria RAM mínimo de 64 GB. **g.** El equipo debe incluir fuentes de poder redundantes, intercambiables en caliente (Hot-swap)

	h. Se debe proveer cuatro interfaces ópticas de 10 Gbps para manejo de tráfico y una interfaz de Gbps, con los correspondientes transceiver y cables de conexión. **i.** Debe proveer un almacenamiento interno y dedicado de 2 TB redundante y hot Swap. **j.** Debe incluir un puerto de consola DB9 **k.** El equipo debe ser de última generación. **l.** La solución debe contar con mecanismos de aceleración criptográfica y de SSL **m.** La solución propuesta deberá poder ser implementada y configurada de manera transparente, a partir de la información contenida en la infraestructura actual con que cuenta el Ministerio de Hacienda, utilizando las configuraciones existentes **'portal2' y 'SPGR'**. **n.** La solución deberá proporcionar, como mínimo, las mismas funcionalidades que ofrece la solución que se encuentra en producción para el SIIF NACION. **o.** La solución deberá contar con una gestión gráfica para la configuración, monitoreo, visualización y generación de reportes, manejo de alarmas, tanto de manera local (en el mismo dispositivo) a través de la interfaz nativa o de interfaz web. **p.** La solución deberá soportar conexiones VPN sin utilizar cliente (Clientless), por medio de soporte HTML5 Websocket, que además permitan al usuario realizar sesiones RDP (Remote Desktop Protocol), SSH (Secure Shell) por medio de cualquier navegador compatible con HTML5, no se debe incluir licencias adicionales para este servicio. **q.** Soportar rescribir sobre HTML5 WebSocket, no se debe incluir licencias adicionales para este protocolo **r.** La solución en alta disponibilidad debe poder soportar hasta **4.000 usuarios** concurrentes en un despliegue activo-activo o activo-pasivo. **s.** Al ser una solución en clúster, ésta debe permitir sumar las licencias presentes en cada equipo que conforman la solución de alta disponibilidad sin importar si está en Activo-Activo y/o Activo-Pasivo. **t.** Al presentarse una falla de uno de los equipos del clúster no debe presentarse una desconexión y/o solicitud de reintentos de autenticación. **u.** La solución debe tener la capacidad que al fallar un equipo que pertenezca al clúster se mantenga el licenciamiento del equipo en falla en el equipo que queda operativo.

	v. La solución debe soportar en la misma configuración el soporte de diferentes dispositivos clientes (Portátiles, Tablet, Smartphone entre otras); sin importar el sistema operativo. **w.** La solución debe tener el mismo agente para los sistemas operativos Windows, Windows Mobile, Linux, iOS, Android y MAC Os, entre otros. **x.** La solución debe tener acceso seguro SSL a través de exploradores WEB como Chrome, Internet Explorer, Edge, Opera, Safarí, entre otros. **y.** Debe soportar la realización de conexiones seguras por aplicación tipo SAM. **z.** La solución debe soportar la presentación de varios portales WEB de acceso con independencia en métodos de autenticación (Sign-IN-URL). **aa.** Interoperabilidad con VMware View Manager **bb.** La solución debe contar con sistemas de escaneo y cumplimiento de los equipos cliente antes y durante las conexiones seguras. **cc.** La solución debe estar en capacidad de validar la existencia de Antivirus, Personal Firewall, Antispyware, Antimalware, actualizaciones de Windows, existencia de certificados digitales y/o archivos específicos. **dd.** La solución debe estar en capacidad de realizar la validación avanzada de actualizaciones en los equipos clientes, estado de seguridad según el antivirus y la ejecución correcta de escaneo del antivirus. **ee.** La solución debe contar con herramienta para borrar datos remanentes luego de terminada una conexión y/o sesión. **ff.** Integración total con sistemas de autenticación: AD, LDAP, RAIDUS, RSA, SAML, securID, Certificados digitales, Public Key Infraestructure, OTP, Kerberos entre otras. **gg.** Debe soportar los siguientes mecanismos de autenticación hardware token, smart card, soft token y one-time passwords. **hh.** Ofrecer una integración avanzada de SAML 2.0 y soportar Single Sign On en SAML. **ii.** Debe permitir la implementación de SAML Identity Provider (IdP) como SAML Service Provider (SP). **jj.** Debe integrarse con Active Directory mínimo con Microsoft 2012 R2 y Microsoft 2016 independiente sí es IPv4 o IPv6. **kk.** La solución debe ser capaz de adquirir la identidad de los usuarios, desde un Directorio Activo Microsoft 2012 R2 y Microsoft 2016 sin la necesidad de instalar software/agentes en los controladores de dominio, basado en la lectura de los eventos de seguridad de Microsoft.

	ll. La solución debe soportar la integración de dos métodos o sistemas de autenticación sobre un usuario en el momento de acceso. **mm.** La solución debe soportar varios roles de acceso en donde se pueda parametrizar el rol en un portal de presentación. Adicional cada rol puede tener independientes sistemas o soluciones de autenticación, así como también cada rol podrá tener restricciones de acceso independientes. **nn.** La solución debe tener la capacidad de customizar los portales WEB a presentar a los usuarios acorde al perfil y/o rol. **oo.** La solución debe permitir la parametrización del tiempo específico de conexión y en caso de requerir más tiempo a la establecida, podrá ser extendida por el usuario directamente. **pp.** Soportar acceso a aplicaciones Flash, Java applets, HTML, JavaScript, DHTML, XML, entre otras. **qq.** Soportar accesos WEB seguros para conexiones SSH, Telnet y Terminal Services. **rr.** La solución debe tener la característica de poder realizar la interfaz de Terminal Service y/o RDP para dispositivos con sistemas operativos que no tengan dicha interfaz como equipos MAC. **ss.** Soportar la compartición segura de archivos Windows y Linux; a través de acceso WEB y sin utilizar un cliente o agente específico. **tt.** Debe poder parametrizar Split túnel. **uu.** Sobre VPN de nivel 3 debe tener la posibilidad de supervisar rutas y capacidad de tener una ruta superior. **vv.** Soportar VPN de nivel 3 mediante ESP. **ww.** La solución debe poder validar certificados digitales validos sobre los dispositivos cliente. **xx.** La solución debe permitir realizar troubleshooting avanzado desde la administración WEB. **yy.** La solución debe generar logs de auditoría y granularidad sobre cada usuario. **zz.** La solución debe generar reportes de conexiones concurrentes de usuarios, de tiempos de conexión por usuario, Throughput, top de sistemas operativos de dispositivos finales hasta por 30 días y portales a los que se realizan las conexiones.

	aaa. Los reportes deben generarse en tiempo real basado en una línea de tiempo, para reportes predefinidos o a la medida, permitiendo al administrador realizar análisis de contenido en tiempo real. **bbb.** La solución debe permitir exportar logs a un dispositivo final. **ccc.** Se debe configurar SNMP v3 para enviar traps hacia un equipo centralizado de monitoreo, SIEM y/o SOC. **ddd.** Los equipos deben estar en la capacidad de poder realizar un rollback de versión a una versión anterior. **eee.** Permitir y realizar configuración IPv4 e IPv6. **fff.** La solución debe permitir la generación de backup y restauración de las configuraciones, políticas y logs permitiendo al administrador programar la realización de los backups en el tiempo deseado. **ggg.** Los backups deben poderse almacenar localmente y transferir automáticamente vía FTP o SCP a un equipo que defina el Ministerio.
3.	**ITEM 2 SOLUCION VPN SSL PARA OTROS AMBIENTES Y TRABAJO REMOTO**
CARACTERISTICAS TECNICAS GENERALES DE LA SOLUCIÓN	
3.1.	El equipo de VPN SSL a proveer debe tener las siguientes características: **a.** Un equipo VPN SSL Ivanti Virtual Appliance **ISA 8000-VS-GLD-D** **b.** Licenciamiento del software requerido para la solución adquirida con su correspondiente garantía y soporte técnico cubiertos por el fabricante. El servicio de soporte debe ser prestado por el tiempo de duración establecido en el contrato contado a partir del recibo a satisfacción de la solución. (Ver numeral 1.6)
3.2.	Se debe realizar la migración de las configuraciones y funcionalidades que se tienen implementadas en las actuales soluciones: **‘portal3’, ´portal MHCP’ y ‘portal4’**. Así como la validación del funcionamiento en la nueva infraestructura, puesta en producción y estabilización.
3.3.	La solución de VPN SSL debe contar con las siguientes características: **a.** Debe contar con un sistema operativo pre-endurecido específico para seguridad que sea compatible con el equipo. **b.** Debe tener capacidad para **3.500 usuarios concurrentes.**

	c. Debe permitir un Throughput de mínimo de 4.5 Gbps para túnel ESP. **d.** Debe permitir un Throughput de mínimo de 3.3 Gbps para túnel SSL. **e.** Debe contar con memoria RAM mínimo de 32 GB. **f.** La solución debe contar con mecanismos de aceleración criptográfica y de SSL. **g.** La solución propuesta deberá ser implementada y configurada de manera transparente, a partir de la información contenida en la infraestructura actual con que cuenta el Ministerio de Hacienda, utilizando las configuraciones existentes para **'portal3', ´portal MHCP' y 'portal4'**. **h.** La solución deberá proporcionar, como mínimo, las mismas funcionalidades que ofrece la solución que se encuentran en **'portal3', ´portal MHCP' y 'portal4'.** **i.** La solución deberá contar con una gestión gráfica para la configuración, monitoreo, visualización y generación de reportes, manejo de alarmas, tanto de manera local (en el mismo dispositivo) a través de la interfaz nativa o de interfaz web. **j.** La solución deberá soportar conexiones VPN sin utilizar cliente (Clientless), por medio de soporte HTML5 Websocket, que además permitan al usuario realizar sesiones RDP (Remote Desktop Protocol), SSH (Secure Shell) por medio de cualquier navegador compatible con HTML5, no se debe incluir licencias adicionales para este servicio. **k.** Soportar rescribir sobre HTML5 WebSocket, no se debe incluir licencias adicionales para este protocolo **l.** La solución debe soportar en la misma configuración el soporte de diferentes dispositivos clientes (Portátiles, Tablet, Smartphone entre otras); sin importar el sistema operativo. **m.** La solución debe tener el mismo agente para los sistemas operativos Windows, Windows Mobile, Linux, iOS, Android y MAC Os, entre otros. **n.** La solución debe tener acceso seguro SSL a través de exploradores WEB como Chrome, Internet Explorer, Edge, Opera, Safarí, entre otros. **o.** Debe soportar la realización de conexiones seguras por aplicación tipo SAM. **p.** La solución debe soportar la presentación de varios portales WEB de acceso con independencia en métodos de autenticación (Sign-IN-URL). **q.** Interoperabilidad con VMware View Manager. **r.** La solución debe contar con sistemas de escaneo y cumplimiento de los equipos cliente antes y durante las conexiones seguras.

	s. La solución debe estar en capacidad de validar la existencia de Antivirus, Personal Firewall, Antispyware, Antimalware, actualizaciones de Windows existencia de certificados digitales y/o archivos específicos. **t.** La solución debe estar en capacidad de realizar la validación avanzada de actualizaciones en los equipos clientes, estado de seguridad según el antivirus y la ejecución correcta de escaneo del antivirus. **u.** La solución debe contar con herramienta para borrar datos remanentes luego de terminada una conexión y/o sesión. **v.** Integración total con sistemas de autenticación: AD, LDAP, RAIDUS, RSA, SAML, securID, Certificados digitales, Public Key Infraestructure, OTP, Kerberos, entre otras. **w.** La solución debe soportar los siguientes mecanismos de autenticación hardware token, smart card, soft token y one-time passwords. **x.** Ofrecer una integración avanzada de SAML 2.0 y soportar Single Sign On en SAML. **y.** Debe permitir la implementación de SAML Identity Provider (IdP) como SAML Service Provider (SP). **z.** Debe integrarse con Active Directory mínimo con Microsoft 2012 R2 y Microsoft 2016 independiente sí es IPv4 o IPv6. **aa.** La solución debe ser capaz de adquirir la identidad de los usuarios, desde un Directorio Activo Microsoft 2012 R2 y Microsoft 2016 sin la necesidad de instalar software/agentes en los controladores de dominio, basado en la lectura de los eventos de seguridad de Microsoft. **bb.** La solución debe soportar la integración de dos métodos o sistemas de autenticación sobre un usuario en el momento de acceso. **cc.** La solución debe soportar varios roles de acceso en donde se pueda parametrizar el rol en un portal de presentación. Adicional cada rol puede tener independientes sistemas o soluciones de autenticación, así como también cada rol podrá tener restricciones de acceso independientes. **dd.** La solución debe tener la capacidad de customizar los portales WEB a presentar a los usuarios acorde al perfil y/o rol. **ee.** La solución debe permitir la parametrización del tiempo específico de conexión y en caso de requerir más tiempo a la establecida, podrá ser extendida por el usuario directamente. **ff.** Soportar acceso a aplicaciones Flash, Java applets, HTML, JavaScript, DHTML, XML, entre otras. **gg.** Soportar accesos WEB seguros para conexiones SSH, Telnet y Terminal Services.

	hh. La solución debe tener la característica de poder realizar la interfaz de Terminal Service y/o RDP (Remote Desktop Protocol) para dispositivos con sistemas operativos que no tengan dicha interfaz como equipos MAC. **ii.** Soportar la compartición segura de archivos Windows y Linux; a través de acceso WEB y sin utilizar un cliente o agente específico. **jj.** Debe poder parametrizar Split túnel. **kk.** Sobre VPN de nivel 3 debe tener la posibilidad de supervisar rutas y capacidad de tener una ruta superior. **ll.** Soportar VPN de nivel 3 mediante protocolo de carga útil de seguridad encapsulada ESP (Encapsulating Security Payload). **mm.** La solución debe poder validar certificados digitales validos sobre los dispositivos cliente. **nn.** La solución debe permitir realizar troubleshooting avanzado desde la administración WEB. **oo.** La solución debe generar logs de auditoría y granularidad sobre cada usuario. **pp.** La solución debe generar reportes de conexiones concurrentes de usuarios, de tiempos de conexión por usuario, Throughput, top de sistemas operativos de dispositivos finales hasta por 30 días y portales a los que se realizan las conexiones. **qq.** Los reportes deben generarse en tiempo real basado en una línea de tiempo, para reportes predefinidos o a la medida, permitiendo al administrador realizar análisis de contenido en tiempo real. **rr.** La solución debe permitir exportar logs a un dispositivo final. **ss.** Se debe configurar SNMP v3 para enviar traps hacia un equipo centralizado de monitoreo, SIEM y/o SOC. **tt.** Los equipos deben estar en la capacidad de poder realizar un rollback de versión a una versión anterior. **uu.** Permitir y realizar configuración IPv4 e IPv6. **vv.** La solución debe permitir la generación de backup y restauración de las configuraciones, políticas y logs permitiendo al administrador programar la realización de los backups en el tiempo deseado. **ww.** Los backups deben poderse almacenar localmente y transferir automáticamente vía FTP o SCP a un equipo que defina el Ministerio.
4.	**ITEM 3 SOLUCION VPN SSL PRUEBAS DE CARGA**
CARACTERISTICAS TECNICAS GENERALES DE LA SOLUCIÓN	
4.1.	El equipo de VPN SSL debe tener las siguientes características:

	a. Un equipo VPN SSL Ivanti Virtual Appliance **ISA 6000-VS-GLD** **b.** Licenciamiento del software requerido para la solución adquirida con su correspondiente garantía y soporte técnico cubiertos por el fabricante. El servicio de soporte debe ser prestado por el tiempo de duración establecido en el contrato contado a partir del recibo a satisfacción de la solución. (Ver numeral 1.6)
4.2.	Se debe realizar la migración de las configuraciones y funcionalidades que se tienen implementadas en la actual solución del **portal de laboratorio**. Así como la validación del funcionamiento en la nueva infraestructura, puesta en producción y estabilización.
4.3.	La solución de VPN SSL debe contar con las siguientes características: **a.** Debe contar con un sistema operativo pre-endurecido específico para seguridad que sea compatible con el equipo. **b.** Debe tener capacidad para **1.000 usuarios concurrentes.** **c.** Debe permitir un Throughput de mínimo de 3.5 Gbps para túnel ESP. **d.** Debe permitir un Throughput de mínimo de 2.5 Gbps para túnel SSL. **e.** Debe contar con memoria RAM mínimo de 16 GB. **f.** La solución debe contar con mecanismos de aceleración criptográfica y de SSL. **g.** La solución propuesta deberá poder ser implementada y configurada de manera transparente, a partir de la información contenida en la infraestructura actual con que cuenta el Ministerio de Hacienda, utilizando las configuraciones existentes del **portal de laboratorio**. **h.** La solución deberá proporcionar, como mínimo, las mismas funcionalidades que ofrece la solución que se encuentra en el **portal de laboratorio.** **i.** La solución deberá contar con una gestión gráfica para la configuración, monitoreo, visualización y generación de reportes, manejo de alarmas, tanto de manera local (en el mismo dispositivo) a través de la interfaz nativa o de interfaz web. **j.** La solución deberá soportar conexiones VPN sin utilizar cliente (Clientless), por medio de soporte HTML5 Websocket, que además permitan al usuario realizar sesiones RDP (Remote Desktop Protocol), SSH (Secure Shell) por medio de cualquier navegador compatible con HTML5, no se debe incluir licencias adicionales para este servicio **k.** Soportar rescribir sobre HTML5 WebSocket, no se debe incluir licencias adicionales para este protocolo

	l. La solución debe soportar en la misma configuración el soporte de diferentes dispositivos clientes (Portátiles, Tablet, Smartphone entre otras); sin importar el sistema operativo. **m.** La solución debe tener el mismo agente para los sistemas operativos Windows, Windows Mobile, Linux, iOS, Android y MAC Os, entre otros. **n.** La solución debe tener acceso seguro SSL a través de exploradores WEB como Chrome, Internet Explorer, Edge, Opera, Safarí, entre otros. **o.** Debe soportar la realización de conexiones seguras por aplicación tipo SAM. **p.** La solución debe soportar la presentación de varios portales WEB de acceso con independencia en métodos de autenticación (Sign-IN-URL). **q.** La solución debe soportar Interoperabilidad con VMware View Manager. **r.** La solución debe contar con sistemas de escaneo y cumplimiento de los equipos cliente antes y durante las conexiones seguras. **s.** La solución debe estar en capacidad de validar la existencia de Antivirus, Personal Firewall, Antispyware, Antimalware, actualizaciones de Windows existencia de certificados digitales y/o archivos específicos. **t.** La solución debe estar en capacidad de realizar la validación avanzada de actualizaciones en los equipos clientes, estado de seguridad según el antivirus y la ejecución correcta de escaneo del antivirus. **u.** La solución debe contar con herramienta para borrar datos remanentes luego de terminada una conexión y/o sesión. **v.** Integración total con sistemas de autenticación: AD, LDAP, RAIDUS, RSA, SAML, securID, Certificados digitales, Public Key Infraestructure, OTP, Kerberos, entre otras. **w.** Debe soportar los siguientes mecanismos de autenticación hardware token, smart card, soft token y one-time passwords. **x.** Ofrecer una integración avanzada de SAML 2.0 y soportar Single Sign On en SAML. **y.** Debe permitir la implementación de SAML Identity Provider (IdP) como SAML Service Provider (SP). **z.** Debe integrarse con Active Directory mínimo con Microsoft 2012 R2 y Microsoft 2016 independiente sí es IPv4 o IPv6. **aa.** La solución debe ser capaz de adquirir la identidad de los usuarios, desde un Directorio Activo Microsoft 2012 R2 y Microsoft 2016 sin la necesidad de instalar software/agentes en los controladores de dominio, basado en la lectura de los eventos de seguridad de Microsoft. **bb.** La solución de soportar la integración de dos métodos o sistemas de autenticación sobre un usuario en el momento de acceso.

	cc. La solución debe soportar varios roles de acceso en donde se pueda parametrizar el rol en un portal de presentación. Adicional cada rol puede tener independientes sistemas o soluciones de autenticación, así como también cada rol podrá tener restricciones de acceso independientes. **dd.** La solución debe tener la capacidad de customizar los portales WEB a presentar a los usuarios acorde al perfil y/o rol. **ee.** La solución debe permitir la parametrización del tiempo específico de conexión y en caso de requerir más tiempo a la establecida, podrá ser extendida por el usuario directamente. **ff.** Soportar acceso a aplicaciones Flash, Java applets, HTML, JavaScript, DHTML, XML, entre otras. **gg.** Soportar accesos WEB seguros para conexiones SSH, Telnet y Terminal Services. **hh.** La solución debe tener la característica de poder realizar la interfaz de Terminal Service y/o RDP para dispositivos con sistemas operativos que no tengan dicha interfaz como equipos MAC. **ii.** Soportar la compartición segura de archivos Windows y Linux; a través de acceso WEB y sin utilizar un cliente o agente específico. **jj.** La solución debe poder parametrizar Split túnel. **kk.** Sobre VPN de nivel 3 debe tener la posibilidad de supervisar rutas y capacidad de tener una ruta superior. **ll.** La solución debe soportar VPN de nivel 3 mediante protocolo de carga útil de seguridad encapsulada ESP (Encapsulating Security Payload). **mm.** La solución debe poder validar certificados digitales validos sobre los dispositivos cliente. **nn.** La solución debe permitir realizar troubleshooting avanzado desde la administración WEB. **oo.** La solución debe generar logs de auditoría y granularidad sobre cada usuario. **pp.** La solución debe generar reportes de conexiones concurrentes de usuarios, de tiempos de conexión por usuario, Throughput, top de sistemas operativos de dispositivos finales hasta por 30 días y portales a los que se realizan las conexiones. **qq.** Los reportes deben generarse en tiempo real basado en una línea de tiempo, para reportes predefinidos o a la medida, permitiendo al administrador realizar análisis de contenido en tiempo real. **rr.** La solución debe permitir exportar logs a un dispositivo final. **ss.** Se debe configurar SNMP v3 para enviar traps hacia un equipo centralizado de monitoreo, SIEM y/o SOC. **tt.** Los equipos deben estar en la capacidad de poder realizar un rollback de versión a una versión anterior. **uu.** Permitir y realizar configuración IPv4 e IPv6.

	vv. La solución debe permitir la generación de backup y restauración de las configuraciones, políticas y logs permitiendo al administrador programar la realización de los backups en el tiempo deseado. **ww.** Los backups deben poderse almacenar localmente y transferir automáticamente vía FTP o SCP a un equipo que defina el Ministerio.
5.	**ITEM 4 SOLUCION VPN SSL NUBE AZURE DRP**
CARACTERISTICAS TECNICAS GENERALES DE LA SOLUCIÓN	
5.1.	El equipo de VPN SSL debe tener las siguientes características: **a.** Un equipo VPN SSL Ivanti Virtual ISA **6000-VAZ-S-GLD** **b.** Licenciamiento del software requerido para la solución adquirida con su correspondiente garantía y soporte técnico cubiertos por el fabricante. El servicio de soporte debe ser prestado por el tiempo de duración establecido en el contrato contados a partir del recibo a satisfacción de la solución. (Ver numeral 1.6)
5.2.	Se debe realizar la migración de las configuraciones y funcionalidades que se tienen implementadas en la actual solución de VPN SSL de la nube de Azure utilizada para recuperación de desastres del portal2 de producción SIIF NACION y SPGR. Así como la validación del funcionamiento en la nueva infraestructura, puesta en producción y estabilización.
5.3.	La solución de VPN SSL debe contar con las siguientes características: **a.** Debe contar con un sistema operativo pre-endurecido específico para seguridad que sea compatible con el equipo. **b.** Debe soportar **2.000 usuarios concurrentes.** **a.** Debe permitir un Throughput de mínimo de 3.5 Gbps para túnel ESP. **b.** Debe permitir un Throughput de mínimo de 2.5 Gbps para túnel SSL. **c.** Debe contar con memoria RAM mínimo de 16 GB. **d.** La solución debe contar con mecanismos de aceleración criptográfica y de SSL. **e.** La solución propuesta deberá poder ser implementada y configurada de manera transparente, a partir de la información contenida en la infraestructura actual con que cuenta el Ministerio de Hacienda y Crédito Público, utilizando las configuraciones existentes para la nube de Azure para DRP del **portal 2 y SPGR.** **f.** La solución deberá proporcionar, como mínimo, las mismas funcionalidades e integraciones que ofrece la solución que se encuentra en la nube de Azure para DRP del **portal 2 y SPGR.** **g.** La solución deberá contar con una gestión gráfica para la configuración, monitoreo, visualización y generación de reportes, manejo de alarmas,

	tanto de manera local (en el mismo dispositivo) a través de la interfaz nativa o de interfaz web. **h.** La solución deberá soportar conexiones VPN sin utilizar cliente (Clientless), por medio de soporte HTML5 Websocket, que además permitan al usuario realizar sesiones RDP (Remote Desktop Protocol), SSH (Secure Shell) por medio de cualquier navegador compatible con HTML5, no se debe incluir el licenciamiento. **i.** Soportar rescribir sobre HTML5 WebSocket, no se debe incluir el licenciamiento. **j.** La solución debe soportar en la misma configuración el soporte de diferentes dispositivos clientes (Portátiles, Tablet, Smartphone entre otras); sin importar el sistema operativo. **k.** La solución debe tener el mismo agente para los sistemas operativos Windows, Windows Mobile, Linux, iOS, Android y MAC Os, entre otros. **l.** La solución debe tener acceso seguro SSL a través de exploradores WEB como Chrome, Internet Explorer, Opera, Safarí, entre otros. **m.** Debe soportar la realización de conexiones seguras por aplicación tipo SAM. **n.** La solución debe soportar la presentación de varios portales WEB de acceso con independencia en métodos de autenticación (Sign-IN-URL). **o.** Interoperabilidad con VMware View Manager. **p.** La solución debe contar con sistemas de escaneo y cumplimiento de los equipos cliente antes y durante las conexiones seguras. **q.** La solución debe estar en capacidad de validar la existencia de Antivirus, Personal Firewall, Antispyware, Antimalware, actualizaciones de Windows existencia de certificados digitales y/o archivos específicos. **r.** La solución debe estar en capacidad de realizar la validación avanzada de actualizaciones en los equipos clientes, estado de seguridad según el antivirus y la ejecución correcta de escaneo del antivirus. **s.** La solución debe contar con herramienta para borrar datos remanentes luego de terminada una conexión y/o sesión. **t.** Integración total con sistemas de autenticación: AD, LDAP, RAIDUS, RSA, SAML, securID, Certificados digitales, Public Key Infraestructure, OTP, Kerberos entre otras. **u.** Debe soportar los siguientes mecanismos de autenticación hardware token, smart card, soft token y one-time passwords. **v.** Ofrecer una integración avanzada de SAML 2.0 y soportar Single Sign On en SAML. **w.** Debe permitir la implementación de SAML Identity Provider (IdP) como SAML Service Provider (SP). **x.** Debe integrarse con Active Directory mínimo con Microsoft 2012 R2 y Microsoft 2016 independiente sí es IPv4 o IPv6.

	y. La solución debe ser capaz de adquirir la identidad de los usuarios, desde un Directorio Activo Microsoft 2012 R2 y Microsoft 2016 sin la necesidad de instalar software/agentes en los controladores de dominio, basado en la lectura de los eventos de seguridad de Microsoft. **z.** La solución debe soportar la integración de dos métodos o sistemas de autenticación sobre un usuario en el momento de acceso. **aa.** La solución debe soportar varios roles de acceso en donde se pueda parametrizar el rol en un portal de presentación. Adicional cada rol puede tener independientes sistemas o soluciones de autenticación, así como también cada rol podrá tener restricciones de acceso independientes. **bb.** La solución debe tener la capacidad de customizar los portales WEB a presentar a los usuarios acorde al perfil y/o rol. **cc.** La solución debe permitir la parametrización del tiempo específico de conexión y en caso de requerir más tiempo a la establecida, podrá ser extendida por el usuario directamente. **dd.** Soportar acceso a aplicaciones Flash, Java applets, HTML, JavaScript, DHTML, XML, entre otras. **ee.** Soportar accesos WEB seguros para conexiones SSH, Telnet y Terminal Services. **ff.** La solución debe tener la característica de poder realizar la interfaz de Terminal Service y/o RDP para dispositivos con sistemas operativos que no tengan dicha interfaz como equipos MAC. **gg.** Soportar la compartición segura de archivos Windows y Linux; a través de acceso WEB y sin utilizar un cliente o agente específico. **hh.** La solución debe poder parametrizar Split túnel. **ii.** Sobre VPN de nivel 3 debe tener la posibilidad de supervisar rutas y capacidad de tener una ruta superior. **jj.** La solución debe soportar VPN de nivel 3 mediante ESP. **kk.** La solución debe poder validar certificados digitales validos sobre los dispositivos cliente. **ll.** La solución debe permitir realizar throubleshooting avanzado desde la administración WEB. **mm.** La solución debe generar logs de auditoría y granularidad sobre cada usuario. **nn.** La solución debe generar reportes de conexiones concurrentes de usuarios, de tiempos de conexión por usuario, Throughput, top de sistemas operativos de dispositivos finales hasta por 30 días y portales a los que se realizan las conexiones. **oo.** Los reportes deben generarse en tiempo real basado en una línea de tiempo, para reportes predefinidos o a la medida, permitiendo al administrador realizar análisis de contenido en tiempo real. **pp.** La solución debe permitir exportar logs a un dispositivo final.

	qq. Se debe configurar SNMP v3 para enviar traps hacia un equipo centralizado de monitoreo, SIEM y/o SOC. **rr.** Los equipos deben estar en la capacidad de poder realizar un rollback de versión a una versión anterior. **ss.** La solución debe ermitir y realizar configuración IPv4 e IPv6. **tt.** La solución debe permitir la generación de backup y restauración de las configuraciones, políticas y logs permitiendo al administrador programar la realización de los backups en el tiempo deseado. **uu.** Los backups deben poderse almacenar localmente y transferir automáticamente vía FTP o SCP a un equipo que defina el Ministerio.
6.	**TRANSFERENCIA DE CONOCIMIENTO** Durante la ejecución del contrato, se debe brindar una (1) transferencia de conocimiento certificada en la última versión del software de VPN SSL de acuerdo con los estándares establecidos por el fabricante IVANTI, para tres (3) ingenieros de la Dirección de Tecnología del Ministerio de Hacienda y Crédito Público, en la cual se provea conocimientos específicos de las funcionalidades requeridas en cuanto a administración, configuración, alta disponibilidad y troubleshooting. La transferencia de conocimiento deberá brindarse cumpliendo con lo siguiente: **a)** Tener una intensidad horaria de mínimo de 40 horas. **b)** Ser dictada por personal certificado por el fabricante IVANTI y en centros de entrenamiento autorizados por casa matriz. **c)** Disponer de equipos para realizar laboratorios prácticos. **d)** Entregar el correspondiente material y certificaciones de asistencia con intensidad horaria a cada uno de los asistentes.
7.	**GARANTÍA** La garantía consiste en mantener todas las soluciones y sus componentes de hardware y software en perfecto estado de funcionamiento mediante reemplazo y/o reparación y/o actualización del componente defectuoso o de la configuración que este presentado errores o fallas por parte del contratista por el tiempo de duración establecido en el contrato, contado a partir de la generación del acta de recibo a satisfacción de los ítems descritos en el numeral 1.1 del presente Anexo.

	a) Los equipos reemplazados y las reparaciones a los mismos que se requieran deberán contar con garantía del fabricante IVANTI a través del contratista durante el período de garantía ofrecido. **b)** Las partes y reparaciones que se requieran para restablecer la funcionalidad de los equipos deberán ser nuevas y originales en todos los casos y proporcionadas por el Contratista. **c)** Debe incluir, mano de obra, reemplazo de partes y actualización de versiones del software liberadas por el fabricante, previa autorización del Ministerio de Hacienda y Crédito Público. **d)** Atención a eventualidades que generen problemas técnicos como fallas, daños, degradación del desempeño, mal funcionamiento o anomalías que se presentan en las soluciones y que impidan que éstas cumplan con su óptimo desempeño. **e)** Ajuste o mejoras de las configuraciones que se encuentren implementadas en las soluciones VPN SSL y para atender nuevas necesidades. Este servicio deberá será atendido por especialistas certificados en la solución de VPN SSL IVANTI. **f)** Informar e implementar las directrices recomendadas por el fabricante IVANTI o el contratista o el entorno tecnológico, ante el surgimiento de vulnerabilidades o amenazas de seguridad detectadas. **g)** La garantía debe ser atendida 7x24, a través del cual el contratista recibirá los incidentes reportados por el Ministerio de Hacienda y Crédito Público. Para lo cual debe permitirse el registro de las eventualidades por alguno de los tres ingenieros del Ministerio, previamente registrados para este fin. **h)** Garantizar la recuperación estable de los servicios en máximo ocho (8) horas, contados a partir del registro de la eventualidad, tiempo durante el cual puede proporcionar una solución provisional siempre y cuando no se presente deterioro de la calidad de los servicios implementados en las soluciones VPN SSL.
8.	**MEJORAS CONTINUAS DEL SERVICIO** El contratista al identificar oportunidades de mejora que conlleven a operaciones más eficaces las deberá incorporar al servicio, previo acuerdo con el Ministerio, a través del supervisor del contrato.
9.	**CONFIDENCIALIDAD** Los diagramas de red, la implementación, levantamiento de información y los resultados de las migraciones y puesta en producción, la atención de soportes

<table>
<tr><td></td><td>que realicen los expertos; así como, la información que sea entregada por el Ministerio dentro de las actividades objeto del contrato serán tratados por el contratista en forma confidencial, adhiriéndose a las políticas de seguridad y de terceros de la Entidad.</td></tr>
<tr><td>10.</td><td>ACREDITACIÓN E IDENTIFICACIÓN DEL PERSONAL AUTORIZADO
El contratista, deberá acreditar e identificar previamente al personal autorizado ante el Ministerio para que le sea permitido el acceso a las instalaciones o por conexión virtual a las soluciones objeto del contrato.</td></tr>
<tr><td>11.</td><td>RECURSO HUMANO
Para la ejecución del contrato se deberá disponer del recurso humano que el oferente considere necesario; sin embargo, la Entidad requiere que se ejecuten las actividades de instalación, configuración, implementación, migración, estabilización, asistencia técnica con mínimo el recurso humano que se relaciona a continuación:
<table>
<tr><td>Rol</td><td>Ingeniero implementador</td></tr>
<tr><td>Cantidad</td><td>1</td></tr>
<tr><td>Característica</td><td>Descripción</td></tr>
<tr><td>Nivel de Educación</td><td>Un (1) ingeniero cuyo núcleo básico de conocimiento sea:
• Ingeniería de Sistemas, Telemática y Afines o
• Ingeniería Eléctrica y Afines o
• Ingeniería Electrónica, Telecomunicaciones y Afines</td></tr>
<tr><td>Certificación</td><td>Certificación expedida por el fabricante IVANTI o Pulse Secure que lo acredite como Technical Expert en soluciones de VPN SSL</td></tr>
<tr><td>Experiencia</td><td>Dos (2) años de experiencia profesional en en implementación o soporte o mantenimiento o instalación o administración de: infraestructura o soluciones o equipos VPN SSL Pulse Secure o IVANTI</td></tr>
<tr><td>Dedicación</td><td>Tiempo completo: lunes a viernes de 8:00 AM a 5:00 PM, durante la implementación y configuración de la solución</td></tr>
</table></td></tr>
</table>

ANEXO No. 2

COTIZACIÓN ECONÓMICA

	DESCRIPCION	CANTIDAD	Valor unitario incluido IVA	Valor total incluido IVA
1	**SOLUCIÓN DE VPN SSL PARA SIIF NACIÓN**			
	Equipo Ivanti **ISA 8000f** (Hardware)	2		
	Licenciamiento para cada equipo de 2.000 usuarios x 1 año (*)	4.000		
	Licenciamiento para cada equipo de 2.000 usuarios x 2 años (*)	4.000		
	Licenciamiento para cada equipo de 2.000 usuarios x 3 años (*)	4.000		
2	**SOLUCION VPN SSL PARA OTROS AMBIENTES Y TRABAJO REMOTO**			
	Un equipo Ivanti Virtual Appliance **ISA 8000-VS-GLD-D**	1		
	Un equipo Ivanti Virtual Appliance **ISA 8000-VS-GLD-D** con licenciamiento para usuarios x 1 año	3500		
	Un equipo Ivanti Virtual Appliance **ISA 8000-VS-GLD-D** con licenciamiento para usuarios x 2 años	3500		
	Un equipo Ivanti Virtual Appliance **ISA 8000-VS-GLD-D** con licenciamiento para usuarios x 3 años	3500		
3	**SOLUCION VPN SSL PRUEBAS DE CARGA**			
	Equipo Ivanti Virtual Appliance **ISA 6000-VS-GLD**	1		
	Licenciamiento para usuarios x 1 año	1000		
	Licenciamiento para usuarios x 2 años	1000		
	Licenciamiento para usuarios x 3 años	1000		
4	**SOLUCION VPN SSL NUBE AZURE DRP (No debe incluir IVA)**			
	Equipo Ivanti Virtual Appliance **ISA 6000-VAZ-S-GLD**	1		
	Licenciamiento para usuarios x 1 año	2000		
	Licenciamiento para usuarios x 2 años	2000		
	Licenciamiento para usuarios x 3 años	2000		

ANEXO No. 3
INFORMACION ADICIONAL

El cotizante, corresponde a alguna de las siguientes categorías:

	SI	NO
MICROEMPRESA		
PEQUEÑA EMPRESA		
MEDIANA EMPRESA		

Relacione contratos celebrados relacionados con el objeto cotizado, en los cinco (5) últimos años con otras Entidades Estatales y/o Privadas (número y fecha del contrato, nombre entidad contratante).

No. del Contrato	Fecha del Contrato	Objeto del Contrato	Nombre Entidad Contratante

INFORMACIÓN RELACIONADA CON EMPRENDIMIENTOS Y EMPRESAS DE MUJERES

Por favor diligenciar sí el cotizante se encuentra en alguna de las siguientes definiciones:

DEFINICIONES	SI
Cuando más del cincuenta por ciento (50%) de las acciones, partes de interés o cuotas de participación de la persona jurídica pertenezcan a mujeres y los derechos de propiedad hayan pertenecido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección	
Cuando por lo menos el cincuenta por ciento (50%) de los empleos del nivel directivo de la persona jurídica sean ejercidos por mujeres y éstas hayan estado vinculadas laboralmente a la empresa durante al menos el último año anterior a la fecha de cierre del Proceso de Selección en el mismo cargo u otro del mismo nivel. Entendiéndose como empleos del nivel directivo aquellos cuyas funciones están relacionadas con la dirección de áreas misionales de la empresa y la	

toma de decisiones a nivel estratégico. En este sentido, serán cargos de nivel directivo los que dentro de la organización de la empresa se encuentran ubicados en un nivel de mando o los que por su jerarquía desempeñan cargos encaminados al cumplimiento de funciones orientadas a representar al empleador.	
Cuando la persona natural sea una mujer y haya ejercido actividades comerciales a través de un establecimiento de comercio durante al menos el último año anterior a la fecha de cierre del proceso de selección.	
Asociaciones y cooperativas, cuando más del cincuenta por ciento (50%) de los asociados sean mujeres y la participación haya correspondido a estas durante al menos el último año anterior a la fecha de cierre del Proceso de Selección.	

INFORMACIÓN PARA EL FOMENTO DE SUJETOS EN ESPECIAL PROTECCIÓN CONSTITUCIONAL.

El cotizante cuenta con alguno de los siguientes grupos poblacionales, para la provisión de bienes o servicios para la ejecución del objeto cotizado:

GRUPOS POBLACIONALES	SI
Población en pobreza extrema	
Desplazados por la Violencia	
personas en proceso de reintegración o reincorporación	
Víctima del conflicto armado interno	
Mujeres cabeza de familia	
Adultos mayores	
Personas en condición de discapacidad	
Comunidades Indígenas, negra, afrocolombiana, raizal, palanquera, Rom o gitanas	
Otros sujetos de especial protección constitucional	

PROVEEDOR

Nombre o Razón Social del Cotizante _____
Nombre del Representante _____
Nit o Cédula de Ciudadanía No. _____ de_____
Dirección _____
Ciudad _____
Teléfono _____
Fax _____
Correo electrónico _____