F02 – ANEXO – CONDICIONES TÉCNICAS ESENCIALES PARA LA PRESTACIÓN DEL SERVICIO Y/O ENTREGA DE BIEN	Fecha	09/10/13

1. DENOMINACIÓN DEL BIEN O SERVICIO

Adquisición de licenciamiento y equipos necesarios para la implementación y balanceo de una solución de virtualización de escritorios.

2. DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO

No aplica

3. UNIDAD DE MEDIDA

- Para las licencias: Licencias entregadas.
- Para los equipos de balanceo de cargas: Equipo entregado y aceptado.

4. NORMATIVIDAD APLICABLE (específica para el servicio y/o bien)

No aplica

5. DESCRIPCIÓN GENERAL

La Entidad requiere adquirir una solución de virtualización de escritorios (licenciamiento y equipos para entrega de aplicaciones con balanceo de cargas) que soporte y brinde servicio a 200 usuarios inicialmente y con capacidad de ampliar en el futuro hasta 5000 usuarios con la infraestructura adquirida.

La solución deberá incluir los siguientes requerimientos mínimos:

- Tecnologías de virtualización de escritorios y aplicaciones
- Tecnologías de control de acceso seguro
- Tecnologías de balanceo de cargas

La implementación de la solución, así como la infraestructura de servidores y almacenamiento requerida será suministrada por el ICBF, por lo cual no se deberá contemplar esto dentro de la propuesta. El ICBF posee 2 enclosures HP C7000 en el cual se encuentra instalada toda la infraestructura de servidores virtuales de la entidad, en esta infraestructura residirá la solución de requerida. El ICBF cuenta con los recursos necesarios para aprovisionar 3 servidores de 64GB RAM con 2 CPU de 8 núcleos cada uno, los cuáles deberían soportar la solución requerida. En consecuencia, no se requiere cotizar componente alguno de la infraestructura de servidores y almacenamiento SAN a utilizar.

Teniendo en cuenta lo anterior, la solución deberá incluir:

- Licenciamiento para doscientos (200) escritorios virtualizados.
- Dos (2) unidades para entrega de aplicaciones virtualizadas con balanceo de cargas con capacidad para 5000 conexiones concurrentes.

6. ESPECIFICACIONES TÉCNICAS DE LOS INSUMOS, BIENES, PRODUCTOS, OBRAS O SERVICIOS A ENTREGAR

El contratista deberá suministrar los siguientes elementos, cumpliendo con los siguientes requisitos técnicos mínimos:

6.1. SUMINISTRO DE AL MENOS DOSCIENTAS (200) LICENCIAS PARA VIRTUALIZACIÓN DE ESCRITORIOS.

TECNOLOGÍAS DE VIRTUALIZACION DE ESCRITORIOS Y APLICACIONES
La solución propuesta debe integrarse, con todos los siguientes hypervisores para alojar los escritorios y aplicaciones virtuales: • VMware ESX 3/ VMware vSphere 4 • Microsoft HYPER-V - Microsoft System Center Virtual Machine Manager 2008 y Microsoft System Center Virtual Machine Manager 2008 R2 o superior. • Citrix XenServer 5 o 5.5 o 5.6 o superior La solución debe poder integrarse con todos los hypervisores anteriores como mínimo e incluso integrar varios hypervisores para la virtualización de los escritorios y aplicaciones virtuales en la misma granja de escritorios.
Se debe incluir el licenciamiento requerido de uso a perpetuidad de al menos uno de los hypervisores mencionados anteriormente, el cual será usado para virtualizar los componentes de la solución ofrecida únicamente.
El hypervisor incluido en la solución debe contener mínimo las siguientes características de funcionalidad: • Hypervisor nativo de 64-bits de tipo bare metal. • Habilitado para virtualización asistida por hardware en arquitecturas de virtualización AMD-V o INTEL-VT. • Soporte a la creación de granjas/arreglos (pools/clusters) de servidores físicos con hypervisor. • Servidores virtuales ilimitados por servidor físico. • Soporte para todo tipo de máquinas virtuales con sistema operativo Windows de Servidor (Windows Server 2008 32/64bits, Windows Server 2012) y con sistema operativo Windows de escritorio (Windows XP Professional, Windows VISTA Professional, Windows 7 Professional, Windows 8 Professional). • Conectividad con sistemas de almacenamiento compartidos comunes en el mercado

como NAS, DAS y SAN (iSCSI o FC) para ofrecer compatibilidad integrada con una amplia gama de plataformas de hardware de almacenamiento. • Herramienta de administración integrada de almacenamiento que permita presentar hypervisores a las plataformas de almacenamiento y viceversa, reduciendo la complejidad de creación y administración de áreas de almacenamiento y la presentación de las mismas a los hypervisores y permitiendo desde la consola el uso de características propias del almacenamiento como creación de instantáneas (snapshot), clonación, deduplicación y aprovisionamiento eficiente (thin provisioning) siempre que los sistemas de almacenamiento las provean. • Migración en vivo de máquinas virtuales entre servidores físicos de la granja sin suspensión de servicio (Live migration). • Alta disponibilidad (HA) para el reinicio de cargas de trabajo de forma automática ante falla o caída de uno de los servidores físicos de la granja, en los demás servidores físicos que la conformen. • Consola de administración grafica centralizada, que permita la administración de múltiples servidores o granjas. • Balanceo de cargas de trabajo (máquinas virtuales) entre los servidores de la granja, al momento de inicio de la máquina virtual y en ejecución por sugerencia al administrador. • Reporte en tiempo real e histórico de rendimiento de los hypervisores o las granjas a través de la consola, soportada en datos históricos almacenados en base de datos. • Reporte de problemas de rendimiento de los servidores de la granja vía E-mail. • Servicios de aprovisionamiento para equipos virtuales (múltiples servidores desde una sola imagen, inicio de máquinas virtuales por protocolos de red bootstrap vía PXE) • Herramientas para creación de flujos de trabajo (workflows) vía Windows Powershell™, que faciliten el aprovisionamiento de nuevos servidores de forma automática, o simplemente faciliten la realización de tareas repetitivas de operación en la infraestructura y lo hagan de forma automática. • Herramientas de migración y conversión de físico a virtual P2V y virtual a virtual V2V. • Integración con directorio activo para administración y operación de la infraestructura de granja e hypervisores. • Instantáneas de cargas de trabajo (snapshots) nativo.
Se debe proveer un componente de brokering de escritorios y brokering de aplicaciones, que realice la asignación del escritorio/aplicación virtual al usuario que se esté conectando, y después de autenticarlo, ejecute la conexión de los usuarios con sus escritorios virtuales o sus aplicaciones virtuales, controlando el estado de los escritorios/aplicaciones, arrancando y deteniendo los mismos en demanda basados en la configuración definida.
Se deben poder entregar las aplicaciones en los dispositivos finales de forma directa y permitir el uso de las aplicaciones virtualizadas desde estos dispositivos finales sin necesidad de entregar un escritorio virtual alojado en el Datacenter (VDI).
Se debe soportar como mínimo todas las siguientes versiones de sistema operativo de escritorio: • Windows XP Professional 32-bit y 64-bit • Windows Vista 32-bit y 64-bit Business, Ultimate, o Enterprise Editions con Service Pack 1 o superior. • Windows 7 32-bit y 64-bits Professional.

• Windows 8 32-bit y 64-bit Professional.
Los escritorios compartidos y las aplicaciones virtualizadas deben poder alojarse en servidores de aplicaciones/escritorios compartidos con todos los siguientes sistemas operativos de servidor: • Windows Server 2008 32 bits • Windows Server 2008 R2 64 bits. • Windows Server 2012, 32 y 64 bits. Ejecutando RDS o Terminal Services.
La solución deberá contemplar la posibilidad de acceder a los escritorios y aplicaciones virtuales como mínimo desde todos los siguientes dispositivos: Thin Clients, computadores personales y dispositivos móviles. Adicionalmente, debe contar con la característica de portabilidad donde la sesión de un usuario debe poder trasladarse de un dispositivo a otro sin necesidad de cerrarla, para que el usuario pueda seguir trabajando desde el mismo punto. La solución debe ser compatible y funcional como mínimo en todos los dispositivos que tengan cualquiera de los siguientes sistemas operativos: Windows XP, Windows XP Embebido, Windows Vista, Windows 7, Windows CE, Windows 8, Linux, Macintosh OS X, iOS, Android.
La solución debe proveer escritorios y/o aplicaciones virtuales tanto para ambientes de redes de telecomunicaciones LAN (cableada o inalámbrica - WLAN) como para ambientes de redes de telecomunicaciones WAN e Internet (tecnología 3G o superior).
La solución deberá poseer la inteligencia necesaria para mantener la separación y permitir el ensamblar en momento de ejecución los tres (3) componentes básicos que conforman un escritorio virtual dedicado o compartido: Sistema Operativo, Aplicaciones y Perfil de Usuario, permitiendo conservar la independencia entre estos 3 niveles generando la mayor flexibilidad posible en la arquitectura.
La personalización del escritorio dedicado o compartido que necesite cada usuario deberá ser almacenada en un repositorio dedicado, fuera de la máquina virtual o la máquina física, con una herramienta de gestión y configuración para tal fin, que administre las configuraciones de personalización de los usuarios, facilitando además el proceso de inicio o cierre de sesión de los usuarios.
La solución deberá proveer, la posibilidad de realizar streaming tanto del Sistema Operativo como las Aplicaciones (por separado de la imagen del Sistema Operativo y por demanda) a máquinas virtuales en el Datacenter y también a computadores personales físicos en la LAN (Estos sistemas operativos y/o aplicaciones, se ejecutarán en los dispositivos finales con los recursos locales del dispositivo como CPU, Memoria y Disco local, agregando la posibilidad de trabajar fuera de línea las aplicaciones que se entreguen así), utilizando la mismas licencias de la solución de virtualización de escritorios y aplicaciones.
Se requiere que la solución incluya componentes que permitan aprovisionar múltiples escritorios virtuales dedicados y múltiples servidores de aplicaciones/escritorios virtuales compartidos desde imágenes centralizadas, sin forzar la utilización de clonaciones de discos virtuales, permitiendo de esta forma optimizar la utilización de sistemas de almacenamiento.
La solución deberá contener una herramienta para administrar, centralizar, gestionar y automatizar los perfiles de usuario (Windows Profiles) y manejar las personalizaciones necesarias para los usuarios con sistemas operativos Windows tanto físicos como virtuales, facilitando y

acelerando los procesos de inicio y cierre de sesión de los mismos y permitiendo el mantenimiento de unos perfiles híbridos ajustados a las políticas de la organización tanto para los cambios permitidos a los ambientes de escritorios y aplicaciones virtuales, como al direccionamiento de los datos de los usuarios.
Se debe permitir integración con mecanismos de acceso remoto seguro tipo VPN SSL, para permitir que los usuarios tengan acceso a sus escritorios/aplicaciones virtuales a través de conexiones de redes públicas.
La solución debe contener una herramienta para creación de flujos de trabajo (workflows) vía Windows Powershell™, que facilite la realización de tareas repetitivas de administración ejecutándolas automáticamente. Conectar usuarios con aplicaciones, crear nuevos servidores o escritorios a partir de imágenes doradas aprovisionadas, sin necesidad de ejecutar scripts para ello, todo a través de una interfaz gráfica de creación de dichos flujos de trabajo. La ejecución de los flujos de trabajo deberán poderse iniciar por la ocurrencia de un evento definido.
Se debe proveer de manera integrada la posibilidad de decidir en momento *de* autenticación y basada en políticas cuál es la mejor forma de entregarle la aplicación a cada usuario dependiendo del cumplimiento de las políticas definidas por la organización. La entrega de aplicaciones deberá ser basada en roles de usuario y deberá permitir asignar nuevas aplicaciones o quitarle aplicaciones existentes a un usuario de manera dinámica, sin intervención del usuario y sin que esto requiera instalación o desinstalación de software ni en los escritorios virtuales ni en los físicos, más allá del agente de conectividad a las mismas, el cual se instala solo una sola vez y no se cambia al asignar o desasignar aplicaciones.
La plataforma de virtualización de aplicaciones debe permitir almacenar de forma centralizada las aplicaciones, en ambientes aislados (isolation), y que sean entregadas desde estos centros de almacenamiento tanto a los servidores que las ejecutaran para entregarlas virtualizadas a los usuarios, como a los escritorios virtuales y a los dispositivos finales físicos. Facilitando la actualización, administración y la entrega de dichas aplicaciones y reduciendo el conflicto entre aplicaciones o versiones de aplicaciones.
Se debe proveer aplicaciones virtuales tanto para ambientes de redes LAN como para ambientes de redes WAN e internet.
La solución debe incluir una interface de acceso a las aplicaciones tipo web vía html como mínimo desde navegadores, incluyendo Internet Explorer 7 o superior, Mozilla Firefox 3.x o superior, Safari 4.x o superior, Google Chrome versión 27 o superior, teniendo presente que la solución debe soportar plenamente las versiones más recientes de cada navegador al momento del cierre del presente proceso.
La solución debe incluir mecanismos que ayuden a administrar la utilización de CPU, para mejorar su uso por las aplicaciones publicadas.
Se deben incluir herramientas de administración centralizada de las granjas de servidores de aplicaciones que permitan: • Monitorear los recursos de los servidores de aplicaciones vía contadores de rendimiento de sesiones, alertas multivariables y permitiendo reportes personalizados. • Administrar la instalación de aplicaciones en múltiples servidores del mismo tipo. • Optimizar el uso de CPU y memoria en los servidores que alojan las aplicaciones • Monitorear el estado de los servidores que alojan las aplicaciones, permitiendo subir de forma automática servicios de la plataforma críticos para su funcionamiento, sin intervención humana de forma automática o programada.

La solución debe incluir una herramienta que se instale en los dispositivos finales que accederán a las aplicaciones virtualizadas, y que opcionalmente permita a los usuarios subscribirse a las aplicaciones que van a utilizar, previamente aprobadas por el administrador de la plataforma.
En el caso de los escritorios virtualizados, estos deberán poder estar encendidos de antemano, para que el usuario no tenga que esperar el tiempo de inicio de la máquina virtual, con lo cual cuando el usuario inicie sesión en la plataforma el escritorio deberá presentarse automáticamente ante él.
En caso de una desconexión del dispositivo, por motivos de corte en la comunicación, la solución deberá permitir al usuario tanto la reconexión automática cuando la comunicación se restablezca como la posibilidad de continuar su trabajo desde el mismo lugar previo a la desconexión.
La solución deberá permitir portabilidad donde las sesiones de escritorios o aplicaciones virtualizadas puedan ser pausadas por usuarios en un dispositivo y ser retomadas en otro dispositivo físico diferente exactamente en el mismo punto donde quedo pausada o suspendida la sesión cuando abandono el dispositivo inicial.
La solución deberá soportar múltiples factores de autenticación y autenticación robusta con Smartcards incluyendo Common Access Card (CAC) y USB smart card tokens, los cuales son compatibles con Microsoft. La autenticación vía smartcard deberá estar disponible para escritorios virtuales dedicados que corran Windows XP, Windows Vista, Windows 7 o Windows 8. Múltiples smartcards y múltiples lectores deberán poder usarse en el mismo dispositivo final de usuario. Los usuarios podrán moverse entre dispositivos finales con diferentes smart card readers, reconectando su sesión después de autenticarse con la plataforma de virtualización de escritorios.
La solución debe proveer integración y soporte a periféricos locales, de forma transparente para el usuario. Los usuarios deberán poder insertar un dispositivo USB localmente y usarlos desde su escritorio virtual y aplicaciones virtuales como si estuvieran en su máquina local. Los dispositivos USB soportados deben incluir: Flash drives, smartphones, PDAs, impresoras, scanners, MP3 players, y tablets (caso de table PCs), y dispositivos asincrónicos como Webcams, microphones, speakers y headsets.
La solución debe proveer el manejo de un driver universal de impresión (evitando la instalación de los drivers de cada tipo de impresora que tengan los usuarios y además ser independientes de los drivers de impresión que tenga el dispositivo de conexión).
La solución debe contener una tecnología desarrollada para proveer una calidad aceptable tanto de audio como de video (retardos no significativos, no congelamientos y no pixelación, suave sin fisuras) cuando se reproducen contenido multimedia LAN como en ambientes WAN, sin impactar en gran medida el ancho de banda usado por la aplicación.
La solución debe proveer soporte nativo (vía códecs desarrollados para tal fin) para audio bi-direccional en escritorios virtualizados dedicados Windows.
La solución debe proveer una calidad buena virtualizando la herramienta de comunicación Microsoft Lync con una calidad buena tanto de audio como de video.
La solución debe proveer soporte a los protocolos de VoIP en el entorno LAN, de al menos las marcas conocidas proveedoras de este software de VoIP, entre ellas la del proveedor NEC, solución con la que actualmente cuenta el ICBF. Los aplicativos propios de la Solución de Telefonía IP utilizados en el ICBF como softphone son el SP350 y SP30.
La solución debe proveer soporte para que la sesión de escritorio virtual del usuario pueda verse

en múltiples monitores a la vez que estén conectados al dispositivo cliente final. La configuración para múltiples monitores debe soportar L/T/U/X-shaped o con monitores de diferentes tamaños y resoluciones.
Todos los componentes de la solución deberán contar con mecanismos de alta disponibilidad y recuperación ante fallas. La sesión de los usuarios deberá permanecer activa incluso si el broker de conexión sufre una caída.
La solución debe permitir que las conexiones a escritorios virtuales activas e inactivas puedan ser administradas, permitiendo al administrador obtener información del servidor en el cual está corriendo el escritorio virtual, el usuario que tiene en uso dicho escritorio y en caso de ser requerido, que pueda hacer cerrar dicha sesión, desde la herramienta de administración.
La solución debe ejercer el control de políticas de gestión de perfiles, software y uso de forma centralizada.
La solución debe proveer mecanismos para permitir la delegación de administración entre usuarios y/o grupos
La solución debe proveer soporte para autenticación con directorio activo de Windows.
La solución debe ofrecer interfaces gráficas para el personal que administre y de soporte a la solución.
La solución deberá poderse administrar desde un sitio central, el cual estará conectado por medio de enlaces de telecomunicaciones WAN con los diferentes sitios donde resida esta infraestructura.
Las configuraciones deberán poder realizarse mediante asistentes (wizards) y también por línea de comandos o a través de una o varias consolas dependiendo de las tareas a realizar. La solución deberá contar mínimo con herramientas de administración gráficas para los siguientes componentes:
Infraestructura de Virtualización ofrecida dentro de la solución (Hypervisor) • No deberá requerir un servidor adicional para brindar las funcionalidades de administración centralizada de todos los servidores (hypervisores) de la plataforma ofrecida dentro del licenciamiento, el catálogo de todas las máquinas virtuales, ni para las funcionalidades migración en vivo (live motion) de las máquinas virtuales de un servidor físico a otro, tampoco para la funcionalidad de alta disponibilidad (HA) ni para la localización óptima (en los servidores físicos con más recursos disponibles) de las máquinas virtuales cuando éstas se inician. • No deberá requerir una base de datos externa o de terceras partes para almacenar la información persistente de la configuración de la granja o grupo de servidores de virtualización. • La administración de toda la infraestructura de virtualización se deberá poder realizar desde una consola cliente servidor que se pueda instalar en cualquier plataforma Windows (XP, Vista, Windows7, Windows 8, Windows Server 2008, Windows Server 2012) y que pueda administrar distintas granjas o grupos de servidores desde la misma instancia de la aplicación.
• **Infraestructura de Aprovisionamiento de Imágenes de Sistema Operativo**: Esta herramienta de administración deberá poseer la capacidad de segregar por roles el manejo de máquinas virtuales o físicas, grupos de máquinas virtuales o físicas, imágenes

de Sistemas Operativos (virtual disks), distintos repositorios de imágenes, con la posibilidad de definir distintos sitios y brindar administración delegada a sitios remotos. Desde esta herramienta se deberá poder asignar los distintos virtual disks a los distintos grupos de máquinas virtuales o físicas, reiniciar los mismos, realizar cambios a las configuraciones de los virtual disks.
• **Infraestructura de Entrega de Escritorios**: Este componente deberá poder administrar tanto la granja de servidores de entrega de escritorios, como los grupos de escritorios, las políticas de asignación y encendido de los mismos, así como también las políticas de manejo y mapeo de dispositivos remotos para poder brindar un acceso granular y desempeño para cada tipo de escritorio y de usuario. Desde la misma consola se deberán poder administrar las sesiones de usuarios, los escritorios virtuales y tomar acciones de soporte. Asimismo se deberá poder configurar y administrar el portal web y el servicio web que administra el acceso de los usuarios a sus escritorios. • **Herramienta de Aprovisionamiento dinámico de escritorios**: Este componente debe poder crear, desde una sola interface y en una serie de pasos simples (asistente - wizard), la cantidad de escritorios nuevos que la organización necesite en cuestión de minutos, interconectando de manera sincronizada y automatizada todos los componentes de la solución.
• **Infraestructura de Entrega de Aplicaciones**: Este componente deberá poder administrar de manera centralizada todas las aplicaciones que deban correr en el entorno y administrar tanto las sesiones de usuario como las configuraciones de las aplicaciones a ser entregadas. • Así mismo deberá poder tener un mecanismo de registro de cambios a la configuración de los servidores de aplicaciones, con la que se pueda identificar el responsable del cambio y el momento en que se realizó, para simplificar y acelerar la solución de problemas.
TECNOLOGIAS DE CONTROL DE ACCESO REMOTO SEGURO
La solución de acceso seguro vía SSL/VPN, de tipo appliance físico debe soportar alta disponibilidad la cual debe operar en modo activo/pasivo (fail-over - unidad principal/unidad alterna). El sistema debe poseer los componentes necesarios para la interconexión a fin de llevar a cabo el manejo y control de fallos.
Los requerimientos de rendimiento mínimos esperados para esta solución es que pueda soportar a la totalidad de los usuarios de la plataforma de virtualización de aplicaciones y escritorios. Doscientos (200) inicialmente, con capacidad de crecimiento a cinco mil (5000) usuarios en la solución propuesta.
Debe estar certificada para la solución de virtualización de aplicaciones y escritorios, cuando no sean del mismo fabricante.
La funcionalidad mínima requerida del sistema de VPN SSL es: • La solución debe proveer la funcionalidad de acceso remoto seguro a través de la tecnología SSL VPN, integrado como una característica en la misma solución. • La solución debe poder manejar tráfico encriptado por SSL (Secure Session Layer) para asegurar la comunicación entre clientes y servidores de un modo seguro. La comunicación debe hacerse en forma transparente, a fin de poder descargar de estas tareas a los servidores WEB. • Soporte mínimo a los protocolos SSL: SSLv2, SSLv3 y TLSv1

- Soporte del siguiente set de cifrado:
  - Intercambio de claves (Key-Exchange): RSA, DSA, Diffie Hellman con claves de hasta 2048 bits.
  - Encripción: RC4, DES, 3DES, RC2, IDEA, SHA, SHA-1, MD5.
- Autenticación de cliente.
- Soporte de Certificate Revocation Lists (CRL), pudiendo obtenerse estas en forma automática a través de directorios LDAP.
- Soporte de Online Certificate Status Protocol (OCSP). Para validar el estado del certificado usando OSCP, obteniendo el estado de revocación de certificados digitales X.509 en vez de CRL.
- Administración centralizada de certificados / claves.
- Capacidad de definir políticas que evalúen el tráfico a través del appliance y tomar acciones en consecuencia, como evaluar las siguientes condiciones de una conexión:
- Políticas de pre autenticación o “endpoint analysis” que evalúen los siguientes parámetros del usuario final:
- Sistema Operativo
- Service Packs instalados
- Servicios / procesos que están siendo ejecutados
- Archivos
- Software de antivirus / versión.
- Software de Antispam
- Configuración del registro.
- Políticas de autenticación, que especifiquen como validar las credenciales del usuario (Local o por método externo de autenticación).
- Soporte de los siguientes métodos externos de autenticación de usuarios: LDAP, RADIUS, NTLM, TACACS+.
- Políticas de autorización, que especifiquen los usuarios y grupos que tienen acceso a recursos internos.
- Políticas de Sesión, que permitan configurar los atributos del lado del cliente una vez que la sesión está establecida después que el cliente se autentico en forma satisfactoria.
- Integración con tecnologías de autenticación de segundo factor como RSA SecurID, SafeWord products, Gemalto Protiva.
- La tecnología debe proveer opciones de AAA (autenticación, autorización, auditoria) con:
  - Opciones de autenticación flexibles
  - Autenticación en cascada
  - Autenticación de doble factor.
  - Soporte para autenticación vía smartcard o certificado de cliente en USB.
  - Autenticación por extracción de grupo
  - SSO para aplicaciones virtualizadas accedidas a través de la solución y para las aplicaciones web vía HTML form-based single sing on.
  - Registro y traza de auditoría detallada.
  - Escaneo de dispositivo final pre y post autenticación (análisis del dispositivo final).
  - Acceso basado en el escaneo del dispositivo final.

• Escaneo continuo de la sesión • Escaneos personalizables en busca de procesos, valores de registro y archivos. • Soporte a cuarentena o remediación. La solución debe contar con características de acceso a red con: • Reconexión automática del cliente ante interrupción de red. • Configuración de nivel de acceso a red granular. • No alteración de red y tabla de enrutamiento del cliente. • Soporte para que aplicaciones que utilicen protocolos como SIP y FTP puedan iniciar nuevas conexiones UDP o TCP con el cliente. • Limpieza de cache. • Asignación de direcciones de red. • Conexión vía VPN requerida y opcional
• El sistema ofertado deberá soportar integración a redes IPv4 y/o IPv6. • Soporte de VLAN y de trunking 802.1Q • Link Aggregation Control Protocol (LACP) 802.3ad

Como mínimo la solución deberá soportar los siguientes mecanismos de acceso para su administración: Acceso por GUI (HTTP y HTTPS), Acceso por línea de comandos (CLI), Telnet y SSH.
• Contener un Tablero de visualización (dahsboard) de rendimiento del dispositivo en tiempo real.
• La solución debe permitir definir perfiles de usuarios personalizables para distintos tipos de roles, como administrador del equipo, administrador de funcionalidades específicas como Operador, y de lectura (Read-only).
• Soporte de los siguientes métodos de autenticación de usuarios: RADIUS, LDAP, TACACS+ y NT4.
• Las funciones requeridas deben ser configurables a través de una única interfaz de administración.
• El sistema debe soportar como mínimo generación de logs a un sistema centralizado como un Syslog o mediante protocolo SNMP.
• Debe proveer soporte a administración con herramientas de terceros entre ellos, como mínimo soporte a:
  • SNMPv1, SNMPv2 and SNMPv3: NetScaler MIB and MIB-II support.
  • Microsoft System Center Operations Management (SCOM) support.
  • Microsoft System Center Virtual Machine Manager (SCVMM) support.
  • XML/SOAP API for automated application-driven configuration.

La oferta debe incluir acceso a parches y actualización de software, directamente del fabricante, con acceso a un sitio web con dominio del fabricante durante el tiempo de soporte y garantía sobre el licenciamiento. El software suministrado deberá corresponder a la última versión disponible en el mercado
El licenciamiento requerido para la solución es para usuario nombrado, no para usuario concurrente

6.2. DOS (2) UNIDADES PARA ENTREGA DE APLICACIONES VIRTUALIZADAS CON BALANCEO DE CARGAS CON CAPACIDAD PARA 5000 CONEXIONES CONCURRENTES.

La solución de Balanceo de cargas debe ser presentada en appliances físicos de la última generación disponible en el mercado y debe soportar alta disponibilidad la cual debe operar en modo activo/pasivo (unidad principal/unidad alterna – fail over). El sistema debe poseer los componentes necesarios para la interconexión a fin de llevar a cabo el manejo y control de fallos.

La solución debe soportar el funcionamiento simultáneo de todas las siguientes funcionalidades, sin requerir elementos adicionales:

- Balanceo de carga a nivel de capa 4
- Conmutación y filtrado de contenidos a nivel de capa 7.
- Aceleración (compresión, optimización y multiplexación de TCP)

Característica	Capacidad Mínima
Throughput General	0.5 Gpbs
Throughput HTTP	175,000 requests/sec mpbs
Throughput SSL (certificado 1024)	7,500 transactions/sec
Throughput SSL (certificado 2048)	1,500 transactions/sec
Throughput de compresión HTTP	0.5 Gpbs
Puertos Ethernet	6x10/100/1000 BASE-T

Se requiere la funcionalidad de balanceo de carga a nivel 4, soportando como mínimo:

- Protocolos: TCP, UDP, FTP, HTTP, HTTPS, DNS, SIP y RTSP.
- Algorítmos de balanceo de carga: Least Connections, Round Robin, Least Packets, Least Bandwidth, Least Response Time, Hashing (URL, Domain, Source IP, Destination IP and CustomID), SNMP-provided metric, Server Application State Protocol (SASP)
- Persistencia de sesión por: IP de origen, Cookie Insert, Sesión SSL ID, URL Passive, Customer Server ID, IP destino, SIP CALLID.
- Métodos de monitoreo de servidor: Ping, TCP, Load, HTTP, HTTP-ECV, TCP-ECV, HTTP-INLINE, con la capacidad de cambiar los tiempos de respuesta del servidor, intervalos de los mismos, reintentos.
- Protocolos de sesión: TCP, UDP, SSL_TCP

Debe soportar conmutación de contenido a nivel 7 (layer 7 content switching) con las siguientes políticas mínimas:

- URL, URL Query, URL Wildcard, Domain, Source/Destination IP, HTTP Header, Custom, HTTP and TCP Payload Values, UDP

Debe soportar la capacidad de realizar filtrado de contenidos (content filtering), inspeccionando cada requerimiento de HTTP y su respuesta con las reglas definidas por el usuario, basadas en el encabezamiento ó URL de HTTP.

Debe permitir tomar acciones específicas, tales como redirección de contenido a una URL específica o envío de una respuesta a un cliente, basado en la respuesta del Web Server (funcionalidad de Responder).

• Reescritura bidireccional del header y el payload de HTTP basada en políticas. • Reescritura del cuerpo de URL+
La solución debe soportar como mínimo las siguientes técnicas de optimización de TCP: • Multiplexación de conexiones TCP • Buffering de TCP • Connexión “keep-alive” • Acknowledgement selectivo • Se requiere que el sistema soporte compresión basada en el algoritmo GZIP para el tráfico HTTP.
La solución de balanceadores deberá presentar las opciones de caché de contenido dinámico y estático.
Se debe suministrar un paquete de soporte del fabricante en modalidad 5x8 durante el período de garantía.

6.3. OTROS SEVICIOS REQUERIDOS

Capacitación

Se requiere que el contratista realice una capacitación, acerca de la solución adquirida, de al menos 8 horas totales, para 3 ingenieros de la Subdirección de Recursos Tecnológicos (SRT) encargados de la administración y operación de la solución, sobre los elementos adquiridos. La capacitación podrá ser impartida por personal del fabricante o del contratista debidamente certificado en soluciones de virtualización por el fabricante. La capacitación se dictará en la Sede de la Dirección General del ICBF en Bogotá de manera presencial o virtual o mixta, lo cual deberá manifestar en su propuesta.

La capacitación deberá cubrir al menos los siguientes aspectos:

- Instalación, configuración, operación y mantenimiento del hardware y software adquirido.

Todos los equipos y materiales necesarios para el curso de capacitación serán proporcionados por el contratista. El material didáctico e informativo que se proporcione para este fin deberá estar en idioma español y/o inglés.

Documentación técnica a entregar por el Contratista

El contratista deberá entregar al supervisor del contrato la documentación técnica de todos los equipos y software suministrados, en al menos una (1) copia en medio magnético (CD o DVD). La documentación técnica deberá ser en idioma español y/o inglés de edición original del fabricante o del contratista en caso que el fabricante no cuente con esta información.

Esta documentación debe contener como mínimo:

- Composición del sistema.
- Descripción de alarmas utilizadas por los equipos (locales y remotos), con detalles de acciones correctivas.

- Descripción de pruebas y mantenimiento preventivo, instrumentos y herramientas necesarias.
- Procedimientos operacionales para reinicio de los equipos
- Mediciones y procedimientos de administración de los equipos
- Métodos de diagnóstico, detección y eliminación de defectos.
- Guía de comandos operacionales
- Guía de mensajes del sistema

Provisión de soporte para equipos

Por parte del fabricante

De acuerdo con la certificación aportada junto con la propuesta para efectos de lo acá relacionado se deberá garantizar el suministro de soporte en modalidad 5X8 durante el período de garantía (36 meses, contados a partir de la fecha de aceptación de la solución), con tiempo de respuesta máxima para el cambio de partes de 10 días hábiles, contados a partir de la notificación realizada por el líder de servicio en la Subdirección de Recursos Tecnológicos, sobre la falla en el dispositivo o equipo. Las notificaciones se podrán hacer vía telefónica, correo electrónico y/o directamente en la página web del fabricante (si éste cuenta con el servicio).

Por parte del contratista

El soporte por parte del contratista cobija el caso de recambios y reemplazos ante la falla de componentes que afecta a uno de los dos balanceadores para no tener afectación en el servicio (esto no se incluye en el soporte del fabricante).

El tiempo de respuesta a los requerimientos de la Entidad deberá ser de máximo de cuatro (4) horas hábiles o inhábiles, en modalidad 7x24 durante el período de garantía (36 meses, contados a partir de la fecha de aceptación de la solución), contados a partir de la notificación realizada por el líder de servicio en la Subdirección de Recursos Tecnológicos, sobre la falla en el dispositivo o equipo. A efectos de acreditar lo anterior, se deberá incluir en la propuesta certificación expedida por el representante legal del contratista.

El contratista deberá reparar o reemplazar las partes requeridas en garantía, realizar la instalación y configuración, y dejar los equipos en perfecto estado de funcionamiento de la siguiente forma:

- Si hay daño en uno (1) de los dispositivos, el contratista tendrá máximo hasta 30 días calendario para solucionar el problema, contados a partir de la notificación realizada por el líder de servicio en la Subdirección de Recursos Tecnológicos, sobre la falla en el dispositivo o equipo

- Si hay daño sobre los dos (2) dispositivos, el proveedor deberá garantizar el funcionamiento de la solución por medio de la puesta de una solución de forma provisional de elementos o equipos de iguales o superiores características, no

necesariamente en clúster, hasta el reemplazo o reparación definitiva de los elementos defectuosos. En cualquier caso el tiempo de reemplazo o reparación definitiva del elemento no podrá superar los 30 días calendario a partir de la notificación de ICBF de la falla del dispositivo o equipo al contratista. El tiempo máximo para la adecuación de la solución provisional y la puesta en funcionamiento no podrá ser superior a 8 horas hábiles o inhábiles contadas a partir de la notificación de ICBF de la falla del dispositivo o equipo al contratista.

Para tal fin se debe proveer un balanceador en modalidad 'cold spare' para lograr el cumplimiento de los tiempos y condiciones aquí solicitadas o garantizar mediante certificación suscrita por el fabricante de la solución que el proponente cuenta con un stock de repuestos en las instalaciones de este último, por lo que podría cumplir con los tiempos y condiciones de servicio especificadas.

El envío, instalación y configuración de los repuestos y equipos a la Sede de la Dirección General será responsabilidad del contratista y no implicará costo adicional para el ICBF.

Provisión de soporte para licenciamiento

Certificación suscrita por el fabricante y el representante legal del proponente donde se certifique el soporte y garantía sobre el licenciamiento adquirido (entiéndase este cómo derechos de actualización o suscripción y la asistencia técnica sobre el producto adquirido en software), durante el período de garantía (36 meses, contados a partir de la fecha de aceptación de la solución) suministrado por el fabricante de la solución.

Provisión de repuestos para equipos:

Certificación suscrita por el fabricante y el representante legal del proponente a través del cual se garantice el suministro de repuestos y partes para los equipos proporcionados, de la misma marca y de iguales o superiores características a las requeridas en el presente documento, durante el período de garantía (36 meses, contados a partir de la finalización de la ejecución del objeto contractual).

7. OBLIGACIONES DEL CONTRATISTA

7.1. Obligaciones específicas

7.1.1. Cumplir con la totalidad de especificaciones técnicas en cuanto a productos y servicios requeridos, señaladas en el presente documento.

7.1.2. Entregar en perfecto estado de funcionamiento los elementos de acuerdo con las especificaciones definidas en el presente documento y en la propuesta que hacen parte integral del contrato, empacados en sus respectivas cajas individuales, incluyendo manuales técnicos y de operación (Español o Inglés), cables, software de configuración (drivers) en medio magnético originales (si aplica), para cada uno de los componentes de los equipos.

7.1.3. Hacer entrega del certificado de garantía sobre el software y hardware adquiridos, remitido por el fabricante (36 meses).
7.1.4. Garantizar mediante las certificaciones arriba solicitadas, el suministro de repuestos y partes en las condiciones establecidas en el presente documento, durante el período de garantía, así como del soporte sobre el licenciamiento adquirido.
7.1.5. Garantizar que las partes y componentes de los equipos que se entreguen por requerimientos de garantía, sean fabricados por el mismo fabricante de los equipos ofertados.
7.1.6. Entregar productos originales, nuevos, no re manufacturados, de primera calidad de conformidad con las especificaciones técnicas solicitadas por el Instituto de acuerdo con el artículo 4° numeral 5° de la ley 80 de 1993.
7.1.7. Presentar y facturar el detalle del valor unitario de los productos adquiridos desglosando el IVA para efecto de ingreso al almacén.
7.1.8. Asumir los costos derivados del transporte y seguros de los equipos para la entrega en el lugar definido por el ICBF.

7.2. Obligaciones generales

7.2.1. Reportar por escrito al supervisor del contrato cualquier sugerencia que contribuya a la obtención de mejores resultados con respecto a la solución adquirida.
7.2.2. Guardar debida y completa reserva y confidencialidad sobre la información y los documentos del ICBF que tenga conocimiento o a los que tenga acceso en virtud del objeto del contrato.
7.2.3. Presentar los amparos requeridos para el cumplimiento del contrato.
7.2.4. Mantener los precios presentados en la oferta durante el tiempo de la ejecución del contrato.
7.2.5. Cumplir con las obligaciones derivadas del contrato actuando con alto grado de profesionalismo responsabilidad y eficacia en la ejecución de las tareas correspondientes.
7.2.6. Cumplir con el objeto del contrato con plena autonomía técnica y administrativa y bajo su propia responsabilidad, por lo tanto no existe ni existirá ningún tipo de subordinación, ni vínculo laboral alguno entre el contratista y el ICBF.
7.2.7. Constituir la Garantía Única de Cumplimiento establecida en el presente documento.
7.2.8. Entregar al supervisor del control de ejecución del contrato los informes que se soliciten sobre cualquier aspecto y/o resultados obtenidos en cada actividad encomendada cuando así se requiera.
7.2.9. Atender los requerimientos, instrucciones y/o recomendaciones que durante el desarrollo del contrato le imparta EL ICBF, a través del supervisor del mismo, para una correcta ejecución y cumplimiento de sus obligaciones.
7.2.10. Mantener los precios resultantes del proceso de selección, durante el tiempo de la ejecución del contrato.
7.2.11. Presentar los recibos de pago al sistema de seguridad social (salud, pensiones y riesgos profesionales) y parafiscales (Caja de Compensación, SENA, ICBF), cuando haya lugar a ellos para cada uno de los respectivos desembolsos.

7.2.12. Encontrarse a paz y salvo por el pago de los aportes de sus empleados a los sistemas de salud, riesgos profesionales, pensiones y aportes a Caja de Compensación Familiar, al Instituto Colombiano de Bienestar Familiar y al Servicio nacional de Aprendizaje, cuando a ello haya lugar, mediante certificación a la fecha, expedida por el Revisor Fiscal o el Representante Legal – de conformidad con lo establecido en el artículo 50 de la ley 789 de 2002.

7.2.13. Ejecutar las demás actividades que sean necesarias para lograr un total y fiel cumplimiento del objeto, el alcance y las obligaciones contratadas, aunque no estén específicamente señaladas en el presente documento, siempre y cuando las mismas correspondan a la naturaleza y objeto del contrato.

7.2.14. Entregar al Grupo Financiero de la Dirección General el formato de autorización para abono directo en cuenta de ahorros o corriente, debidamente diligenciado y firmado, anexando certificación bancaria de la titularidad de la cuenta.

7.2.15. Sin perjuicio de la autonomía técnica y administrativa, atender las instrucciones y lineamientos que durante la ejecución del contrato se le impartan por parte de Instituto Colombiano de Bienestar Familiar - ICBF.

7.2.16. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y en trabamientos.

7.2.17. Corregir de forma inmediata cualquier falla o error que se cometa en la ejecución del objeto contractual.

7.2.18. Conocer a cabalidad las condiciones del proceso estipuladas en el estudio previo, ANEXO tecnico y pliego de condiciones, con sus respectivas adendas (si las hubiere), la propuesta y el contrato, para realizar la ejecución del mismo con eficiencia y eficacia.

7.2.19. Mantener vigentes las garantías por el tiempo pactado en el contrato.

7.2.20. Presentar al momento de la iniciación del contrato los documentos necesarios para su ejecución.

7.3. Obligaciones del sistema de gestión de calidad

7.3.1. Durante la ejecución del contrato el contratista deberá cumplir con las normas reglamentarias sobre seguridad y salud en el trabajo, medicina preventiva, higiene y seguridad industrial y los demás aspectos inherentes que han sido establecidos o establezca la ley y los organismos de control.

7.3.2. El contratista es responsable del reporte a la ARL y EPS, atención en salud e investigación de los incidentes y accidentes de trabajo presentados durante el desarrollo de las actividades objeto del contrato.

8. LUGAR DE EJECUCIÓN DEL CONTRATO

El lugar de ejecución del contrato será la ciudad de Bogotá – Colombia.

El contratista deberá entregar los elementos adquiridos en el Almacén General de la Sede de la Dirección General del ICBF, ubicado en la Av. Cra. 68 No. 64C-75, de la ciudad de Bogotá.

9. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de **cuarenta (40) días calendario** contados a partir del cumplimiento de los requisitos de perfeccionamiento, ejecución y legalización del contrato, sin que en ningún caso se supere el 31 de diciembre de 2013.

10. VALOR Y FORMA DE PAGO

El valor del contrato a suscribir será hasta por el valor resultante de la adjudicación, incluidos todos los costos directos e indirectos asociados al suministro de los bienes, el IVA, demás impuestos de ley.

Se pagará al contratista un único pago equivalente al **cien por ciento (100%) del valor total del contrato** a la finalización de la ejecución del objeto contractual.

Los pagos se realizarán previa presentación de la factura correspondiente, la certificación de recibo a satisfacción por parte del supervisor y la certificación del revisor fiscal o representante legal, según corresponda, sobre el cumplimiento en el pago de los aportes parafiscales y de seguridad social de sus empleados de acuerdo con lo establecido en el artículo 50 de la Ley 789 de 2002 y artículo 23 de la Ley 1150 de 2007.

El pago se realizará dentro de los **treinta (30)** días hábiles siguientes a la radicación de la factura y la certificación de cumplimiento, previa aprobación del PAC (Programa Anual Mensualizado de Caja).

Si la(s) factura(s) no ha(n) sido correctamente elaborada(s), o no se acompañan los documentos requeridos para el pago, el término para este solo empezará a contarse desde la fecha en que se presenten debidamente corregidas, o desde que se haya aportado el último de los documentos solicitados. Las demoras que se presenten por estos conceptos serán de responsabilidad del contratista y no tendrá por ello, derecho al pago de intereses o compensación de ninguna naturaleza.

Todos los pagos se realizarán conforme al PAC del Instituto Colombiano de Bienestar Familiar.

11. ANEXOS

No aplica

12. CERTIFICACIÓN (a suscribir por parte de los oferentes)

_____ (Nombre del proponente en caso de persona natural o del Representante Legal y/o apoderado en caso de persona jurídica), identificado con C.C No. _____, en mi calidad de representante legal y/o Apoderado de _____ (Razón Social de la empresa), identificada con NIT _____, manifiesto con la presentación y firma del presente documento que he leído, entiendo y puedo garantizar el cumplimiento total de las especificaciones técnicas contenidas en el y en caso de resultar adjudicatario me comprometo a cumplirlo en su totalidad.

_____
Firma Representante Legal y/o Apoderado
Nombre: _____
C.C. _____