

ESPECIFICACIONES TÉCNICAS

1. DEPENDENCIA SOLICITANTE:

Oficina General de Administración.

2. DENOMINACIÓN DE LA CONTRATACIÓN:

Adquisición de solución de virtualización de escritorios para el MIDAGRI.

3. FINALIDAD PÚBLICA:

La presente adquisición busca dotar al MIDAGRI, de una solución tecnológica que permita la virtualización y publicación segura de aplicaciones para los usuarios del MIDAGRI.

4. ANTECEDENTES:

El Ministerio de Desarrollo Agrario y Riego está implementando una nueva sede situada en la intersección de la Av. Salaverry (cuadra 13) y la Av. Húsares de Junín (cuadra 12) en el distrito de Jesús María. Esta nueva sede incluye la implementación de un Centro de Datos y la Red de Datos institucional basada en tecnología GPON, lo cual requiere software que permitan altas capacidades de procesamiento, almacenamiento y transmisión de información a los servidores para el uso de software especializado sobre la red GPON.

5. META DEL POI VINCULADO

Meta: 0106

Actividad: Gestión para el MEJORAMIENTO DE INFRAESTRUCTURA ADMINISTRATIVA del proyecto 2264711. MEJORAMIENTO E IMPLEMENTACION DE LA NUEVA SEDE DEL MINISTERIO DE AGRICULTURA Y RIEGO EN LA CIUDAD DE LIMA.

6. OBJETIVOS DE LA CONTRATACIÓN:

Adquirir una (01) solución de virtualización y publicación segura de aplicaciones, con la finalidad de atender usuarios que necesitan altas capacidades de procesamiento, almacenamiento y transmisión de información a los servidores para el uso de software especializado y manejo de imágenes satelitales, archivos GIS, modelamiento, imágenes de gran tamaño, videos y otros documentos de gran tamaño, asegurando la movilidad, seguridad de los datos y el rendimiento de los equipos.

7. ALCANCE Y DESCRIPCIÓN DE LA ADQUISICIÓN:

Ítem	Descripción del bien	Cantidad
1	Solución de virtualización de escritorios	Uno (01)

Requerimiento General:

- La solución ofertada debe incluir la entrega e implementación (instalación, configuración y puesta en funcionamiento); para lo cual se firmará el acta de entrega, y el acta de implementación. El acta de entrega se otorgará en señal de recepción de los bienes; según lo ofertado, y el acta de implementación se otorgará acorde al cumplimiento de las especificaciones técnicas solicitadas.
- El licenciamiento y todos los componentes a proveer como parte de la presente adquisición, debe pasar a nombre del Ministerio de Agricultura y Desarrollo.

Características Técnicas:

A SOLUCIÓN DE VIRTUALIZACIÓN DE ESCRITORIOS		
A.1 MODULO DE VIRTUALIZACIÓN		
	CARACTERÍSTICA	DESCRIPCIÓN
	Características generales	Licenciamiento de software de virtualización de escritorio de la última versión estable y liberada por el fabricante a la fecha de la presentación de la propuesta, para 70 usuarios nombrados.
		Licenciamiento debe ser del tipo OPEN, el cual: <ul style="list-style-type: none"> ○ No debe estar asociado a servidor físico. ○ Debe permitir la instalación en otro hardware de ser necesario.
		Se deben considerar: <ul style="list-style-type: none"> ○ Administración de acceso de los escritorios virtuales. ○ Sistema Operativo Windows para escritorios virtuales ○ Licenciamiento de módulo de virtualización. ○ Licenciamiento de administración de acceso a los escritorios virtuales. ○ Licenciamiento de sistema operativo Windows para escritorios virtuales. <p>Si producto de la arquitectura de su solución requiere licenciamiento adicional, este lo debe considerar con la finalidad que los 70 usuarios estén correctamente licenciados en la solución VDI y en el sistema operativo Windows cliente.¹</p>
		Licenciamiento por el periodo de 02 años, el cual debe incluir derecho a actualizaciones y soporte 24x7, provisto directamente por el fabricante.
		Licenciamiento bajo modelo de suscripción, donde el enlace de comunicación a la Consola de Administración, VDIs y/o Aplicaciones sea ON-PREMISE.
		MIDAGRI cuenta con una plataforma de virtualización compuesta por 8 nodos con un total de 16 procesadores, cada procesador cuenta con 24 cores desplegada con el siguiente software: <ul style="list-style-type: none"> • vRealize Log Insight 16 CPU • vRealize Operations 8 Enterprise - 16 CPU • vSphere 7 Enterprise Plus - 16 CPU • vCenter Server 7 Standard
		Se debe proporcionar el licenciamiento de todo el software necesario, para el funcionamiento del módulo de virtualización solicitado.
		Debe estar vigente tecnológicamente y pertenecer a la última versión o generación liberada por el

¹ Consulta N° 03 de la empresa CLIC IT S.A.C y consultas N° 09 y N° 12 de la empresa GRUPO ELECTRODATA S.A.C

		fabricante. Se debe acreditar para la presentación de la propuesta con una carta oficial del fabricante con referencia al presente proceso.²
	Administración de la solución	Debe permitir configurar, administrar y gestionar grupos de escritorios y aplicaciones virtuales a entregar, uso de licencias de escritorio, aprovisionamiento de imágenes de escritorio virtual, autenticación y control de autorizaciones.
		Debe contar con una herramienta o funcionalidad nativa de mesa de ayuda, en la que sea posible que un técnico intervenga en la sesión virtualizada.
		Debe permitir la interacción entre el administrador y el usuario mediante el envío de mensajes directamente desde la consola de monitoreo y soporte.
		Debe permitir la visualización de la imagen del escritorio virtual en varios monitores.
		Debe soportar políticas de impresión de tal manera que pueda configurarse, sin necesidad de cambios en los scripts de inicio de sesión, mediante la aplicación de GPO's y de forma nativa de la solución.
		Debe presentar un tablero con un resumen de la información de alerta para ver y remediar incidentes.
		Debe contar con una herramienta para monitorear el uso, salud y desempeño de la infraestructura, escritorios y protocolos.
		La herramienta de monitoreo debe tener registros para auditar el acceso a las máquinas virtuales.
	Gestión de recursos virtualizados	Debe ser capaz de provisionar y controlar el acceso a los recursos virtualizados (aplicaciones y escritorios) ya sea en el modelo de sesión única o multisesión cuando se encuentre disponible.
		Debe tener recursos para aprovisionar y desaprovisionar máquinas virtuales bajo demanda, independientemente de donde se asigne este recurso.
		Debe implementar el aprovisionamiento y administración de recursos virtualizados en máquinas virtuales con los sistemas operativos Microsoft Windows 10 o superior, RHEL 8 o superiores y Windows Server 2019 o superiores.
		Debe contar con una herramienta integrada a la solución que permita el aprovisionamiento de máquinas virtuales desde una sola imagen central, de manera que los administradores tengan autonomía para entregar los recursos con las actualizaciones más recientes, cada vez que se realice el inicio de sesión.
		El aprovisionamiento y desaprovisionamiento de

² Observación N° 01 de la empresa CLIC IT S.A.C

		recursos (máquinas virtuales) debe ser opcional según demanda, y compatible con cualquier Hipervisor.
		Debe permitir la creación de varias máquinas virtuales automáticamente, basadas en la misma imagen del sistema operativo.
		Debe permitir la configuración de un grupo de escritorios virtuales en standby (o aprovisionado) que pueda atender la demanda de conexión de los usuarios de forma paulatina, evitando el desperdicio de recursos físicos con escritorios virtuales encendidos y sin uso, estos escritorios en modo standby deben ser activados en cada grupo de escritorios virtuales a través de la consola de administración.
		Debe permitir la creación de varios escritorios virtuales automáticamente, basados en una imagen de sistema operativo preconfigurada, acelerando la entrega de escritorios virtuales a usuarios no persistentes.
		Debe poder crear grupos persistentes de escritorios virtuales, es decir, grupos de escritorios virtuales que se pueden aprovisionar para el usuario y que, después del primer aprovisionamiento, solo puede acceder el mismo usuario.
		Debe ofrecer una herramienta de virtualización de aplicaciones que permita a los administradores de escritorio transformar aplicaciones compatibles con Microsoft Windows en aplicaciones portátiles que puedan ejecutarse sin necesidad de un Escritorio completo.
		Deber permitir la creación y uso compartido o dedicado de escritorios virtuales sobre plataformas Windows y distribuciones Linux, sin limitar el número de Escritorios de cada tipo hasta el total de licencias adquiridas en el presente procedimiento de selección.
	Equilibrio de sesiones	A los efectos del balanceo de carga inteligente entre servidores de servicios de acceso a aplicaciones remotas, el software debe identificar y establecer la conexión del usuario con el servidor menos cargado; teniendo en cuenta factores como el uso de la CPU, el uso de la memoria y la cantidad de sesiones en ejecución.³
	Gestión de perfiles	La funcionalidad de gestión inteligente de perfiles debe ser una parte integrada de la solución, sin costo adicional.
		Debe proporcionar la funcionalidad de perfil móvil, es decir, conservar las personalizaciones del perfil de usuario y almacenarlas en un servicio de gestión

³ Observación N° 04 de la empresa CLIC IT S.A.C

		de perfiles dinámicos, aplicando las características conservadas por el usuario a los recursos virtualizados (aplicaciones o escritorios) siempre que los usuarios inicien sesión.
		Debe permitir que el administrador use perfiles de solo lectura, que se descartan al cerrar la sesión, sin depender de los servidores de archivos.
		Debe permitir que el dispositivo redirija las carpetas a los servidores de archivos especificados. Se deben redirigir las carpetas de archivos de usuario predeterminadas, como las que se enumeran a continuación: Escritorio, Documentos, Videos, Imágenes, Música, Descargas, Favoritos, Contactos, Enlaces, Búsquedas, Menú Inicio y AppData.
		Debe permitir que la sincronización de los datos del perfil de usuario sea parcial, es decir, dando la posibilidad al administrador de seleccionar lo que debe o no sincronizar en el perfil de usuario, pudiendo realizar esta configuración de forma global o específica por usuario.
		Debe poseer una solución de transmisión de perfiles para que se pueda entregar de manera escalonada siguiendo la demanda del usuario, sin que el usuario tenga que esperar a que su perfil completo comience a usarlo.
		Debe permitir la sincronización de perfiles mientras el usuario está conectado, reduciendo así la carga excesiva de datos durante el cierre de sesión, realizando solo el delta al final del uso.
	Experiencia del usuario	Debe proporcionar al usuario acceso a los recursos virtualizados desde un único portal, este portal de acceso debe estar disponible para acceso externo con alta disponibilidad en todos los Centros de Datos, sin embargo, la solución debe permitir que la sesión del usuario con el recurso virtualizado se establezca con el Centro de Datos más cercano al backend del servidor accedido por el recurso virtualizado.
		Debe proporcionar una aplicación cliente que permita al usuario a través de un dispositivo físico acceder a un escritorio virtual o aplicación publicada, compatible con los siguientes sistemas operativos Windows, MacOS, Linux, Android, iOS y Chromebook.
		Debe permitir que los usuarios marquen sus aplicaciones y escritorios favoritos, que se agregarán a una página separada en su perfil.
		Debe contar con un cliente soportado para instalación y acceso a la plataforma para los siguientes Sistemas Operativos: Windows, Linux, MacOS, Android e IOS.
		Debe soportar el uso de estaciones tipo thin client

		que utilicen sistemas operativos basados en Linux y/o Microsoft Windows Embedded.
		Debe permitir; independientemente del método de acceso (cliente instalado o navegador web), la redirección multimedia, permitiendo así reproducir las aplicaciones de sonido en el sistema de sonido del dispositivo local.
		Debe permitir al usuario utilizar un navegador web para acceder, a través del protocolo HTTPS, a un escritorio virtual o aplicación publicada, si el dispositivo físico utilizado no permite la instalación de la aplicación cliente de la solución ofrecida.
		Debe permitir a los usuarios controlar los recursos de sonido, el tamaño de la ventana y reiniciar su escritorio virtual sin necesidad de la intervención del administrador, excepto para reiniciar los escritorios virtuales que funcionan con multisesión.
		Debe permitir al usuario continuar con su trabajo, exactamente donde lo dejó, en caso de que necesite cambiar de estación de trabajo o abrir una sesión en otro tipo de equipo. Esta funcionalidad debe cerrar la sesión de usuario abierta en el dispositivo inicial y abrirla en el nuevo dispositivo, lo que permitirá que el escritorio "siga" al usuario.
		Debe admitir de forma nativa y realizar la optimización del tráfico con respecto a las herramientas de colaboración más utilizadas, como Microsoft Teams, Zoom y Cisco Webex.
		Debe permitir el uso de tokens criptográficos y tarjetas inteligentes para firmar documentos en escritorios virtuales.
		La herramienta debe ser capaz de facilitar la interacción del usuario al acceder a aplicaciones y/o escritorios a través de dispositivos táctiles, optimizando las funciones emergentes del teclado, el desplazamiento de la pantalla y el zoom automático
	Seguridad	Debe ofrecer un portal de autoservicio capaz de integrarse con la solución de virtualización de escritorio y otras aplicaciones Web, con el fin de unificar la experiencia del usuario y aumentar la seguridad en el acceso a los datos, aplicando configuraciones de autenticación de acceso condicional y de doble factor.
		Debe permitir el acceso a escritorios y aplicaciones virtualizadas a través de un portal disponible vía Web, con autenticación segura y acceso vía SSL o TLS.
		Debe controlar las acciones de "copiar y pegar" entre la máquina del usuario y el contenido accedido.
		Debe tener recursos para controlar la captura de pantalla de los recursos virtualizados (anticaptura

		de pantalla).
		Debe disponer de recursos para evitar la captura/copia de información tecleada durante el acceso a los recursos virtualizados (Anti-keylogger o similar).
		Debe restringir o permitir que el contenido disponible se imprima en impresoras conectadas al dispositivo del usuario.
		Debe permitir o bloquear la conexión de los periféricos de los usuarios con los escritorios y aplicaciones virtualizadas, tales como: discos locales, unidades de red, CD-ROM, DVD-ROM y dispositivos extraíbles (pendrive, HD externo, etc.).
		Debe poner a disposición, en la interfaz de acceso, únicamente los escritorios virtuales o aplicaciones publicadas a los que el usuario tenga acceso, observando los permisos y privilegios definidos luego del proceso de autenticación y análisis del dispositivo.
		Debe contar con recursos para controlar los cambios realizados en el entorno de virtualización de aplicaciones y escritorios, de manera que, cuando sea necesario, los administradores tengan acceso a logs con los cambios realizados en la configuración o permisos del entorno, con fecha y autor de los cambios
A.2	MODULO DE SEGURIDAD DE ACCESO	
	DESCRIPCIÓN	CARACTERÍSTICAS TÉCNICAS
	Características generales	<p>Certificado Digital SSL por el período de 02 años.</p> <p>Debe soportar acceso a los usuarios a través de un portal, que deberá contener asociado de un certificado digital de una entidad de certificados públicos de confianza, como mínimo contener algoritmo RSA Public Key SHA-2 (Funciones hash admitidas: 256, 384, 512), Compatibilidad con el cifrado de claves públicas de 2.048 bits (3.072 bits y 4.096 bits disponibles).</p>
	Seguridad de segundo factor de autenticación	La solución debe implementar una autenticación multifactor, el cual puede ser solicitado al ingresar a contenido corporativo desde redes internas y/o externas. Este sistema deberá soportar el algoritmo HMAC-Based One-time Password (HOTP) especificado en la RFC 4226 y/o el algoritmo Time-based One-time Password (TOTP) especificado en la RFC 6238.
A.3	MODULO DE SEGURIDAD DE VIRTUALIZACIÓN	
	DESCRIPCIÓN	CARACTERÍSTICAS TÉCNICAS
	Características generales	Licenciamiento de software antimalware de la última versión estable y liberada por el fabricante a la fecha de la presentación de la propuesta, para 70 escritorios virtuales.

		Licenciamiento por el periodo de 02 años, el cual debe incluir derecho a actualizaciones y soporte 24x7.
		El licenciamiento de software antimalware debe ser gestionado a través de una consola implementada en los servidores de la Entidad.
		El software debe incluir un sistema de análisis de vulnerabilidades derivadas de plataformas Windows y programas de terceros que permita la descarga centralizada de parches, la aplicabilidad, la distribución y la instalación remota de estos. Este sistema debe estar integrado al software antimalware por lo que no deberá requerir la instalación de ningún componente adicional para su normal desempeño.
		El software antimalware debe estar en idioma español.
	Gestión y gobierno centralizado	Deberá contar con un sistema de distribución y despliegue centralizado permitiendo en determinados casos generar instaladores independientes y personalizados.
		La consola de administración debe poder instalarse en sistemas operativos tales como Windows Server 2019 o posterior, o se podrá desplegar en la nube.
		La consola de administración deberá poder lanzar tareas de despliegue de clientes de forma remota.
		La consola de administración deberá poder mostrar un resumen de la instalación indicando el estado y sugiriendo una acción de refuerzo si fuese necesario.
		La consola deberá ser 100% web permitiendo implementar una nube privada a través de un componente web seguro (https), a fin de poder gestionar los escritorios virtuales de la red corporativa de forma transparente . ⁴
		La consola de administración deberá poder registrar eventos creando logs por cada uno de los eventos que realice dependiendo del ítem (exploración, actualización, bloqueos, etc.)
		La consola de administración deberá permitir implementar exclusiones en la exploración, con capacidad para excluir de la exploración archivos, directorios y/o procesos, etc.; de forma centralizada.
		La consola de administración deberá permitir la programación de tareas, capacidad para programar tareas de exploración, actualización, etc.
		La consola de administración deberá permitir la configuración de repositorios para actualización, capacidad para agregar/eliminar repositorios hacia donde se descarga la actualización de las definiciones de virus.

⁴ Consulta N° 14 de la empresa GRUPO ELECTRODATA S.A.C

		La consola de administración deberá permitir la instalación remota, pudiendo lanzar tareas de instalación en clientes de forma remota desde un servidor de administración antivirus.
		La consola de administración deberá mostrar un inventario general de todos los escritorios virtuales, logrando especificar los recursos de cómputo y almacenamiento que tienen instalado todos y cada uno de los escritorios virtuales protegidos.
		La consola de administración deberá poder programar análisis de malware en todos los escritorios virtuales sin que esto implique una saturación del procesador o memoria para realizar esta actividad, para esto se deberá poder especificar que el escaneo se realice utilizando los tiempos muertos del usuario, el objetivo es evitar saturar los recursos cuando el usuario los necesite.
		La consola de administración deberá contar con una cuarentena local capaz de aislar posibles amenazas de malware no firmadas, pudiendo liberar y limpiar programas o archivos.
		La consola de administración deberá poder reportar y enviar directamente al fabricante, software y/o amenazas no firmadas para su evaluación.
		La consola de administración deberá poder integrarse con el directorio activo a fin de llevar una sola gestión (grupos organizativos)
		La consola de administración deberá tener la capacidad de definir políticas de bloqueo de configuraciones por medio de una contraseña. Este bloqueo debe ser selectivo para configuraciones de objetos específicos (Módulos de protección). Se aceptará que el bloqueo de configuraciones se realice por medio de la aprobación de un usuario administrador.
		Este sistema deberá tener la capacidad de generar reportes locales en cada escritorio virtual, referentes a todas las transacciones o eventos de seguridad realizadas por cada producto.
		Deberá permitir la actualización independiente de productos para aquellos equipos que no puedan sincronizar con la consola.
	Tecnología antimalware	Deberá proteger sistemas operativos como Windows Server 2019 o superior y Windows 10 o superior.
		Deberá incluir un sistema de análisis basado en algoritmos heurísticos capaces de detectar malware por similitud.
		Deberá incluir un sistema que optimice la detección y eliminación de malware empaquetado usado para saturar el performance de los residentes antivirus lanzando miles de variables a partir de un malware ya conocido.

		Deberá incluir tecnología basada en el análisis del comportamiento de amenazas logrando detenerlas incluso sin estar firmadas.
		Deberá contar un módulo de protección especialmente diseñado para hacerle frente a todo tipo de amenazas de tipo RANSOMWARE cual deberá permitir poner en cuarentena la amenaza y si fuese necesario incluir una lista blanca de aplicaciones específicamente para este módulo.
		Deberá poder reconocer y bloquear amenazas de día cero basadas en vulnerabilidades del sistema operativo y programas instalados.
		Deberá incluir tecnologías de Machine Learning que le permitan automatizar el aprendizaje de nuevas amenazas de malware a través de sus diferentes sensores o tecnologías propuestas.
		Deberá contar con tecnologías de inteligencia artificial y aprendizaje automático capaz de reconocer y actuar sobre ataques de tipo malware ofuscado.
Atributos de prevención		Deberá tener un módulo que permita la implementación de políticas de seguridad para el control de aplicaciones, el mismo que deberá poder definir aplicaciones en lista negra para evitar que estas se ejecuten en los escritorios virtuales.
		El módulo de control de aplicaciones deberá poder implementar sus políticas de aplicaciones en lista negras reconociendo el hash, versiones y fabricantes específicos de las aplicaciones a bloquear.
		El módulo de control de aplicaciones deberá tener un modo que permita la implementación de políticas de seguridad para el control de aplicaciones el mismo que deberá poder definir aplicaciones en lista blanca que permitan que solo estas puedan ejecutarse en determinados escritorios virtuales.
		El módulo de control de aplicaciones deberá poder aplicar políticas de seguridad a directorios y archivos específicos.
		El módulo de control de aplicaciones deberá permitir que el usuario pueda solicitar permiso de acceso a determinada aplicación bloqueada desde su escritorio virtual, a fin de mejorar los tiempos de respuesta con el usuario.
		Deberá incluir una protección contra dispositivos USB físicos manipulados.
		Deberá tener un módulo que permita la implementación de políticas de seguridad para el control de dispositivos extraíbles, el mismo que deberá poder ser desplegado, habilitado o deshabilitado desde la consola de administración.
		El módulo de control de dispositivos deberá tener la capacidad de asignar privilegios de solo lectura a

		cualquier USB de almacenamiento externo que se conecte al escritorio virtual a fin de evitar que cualquier aplicación de peligro se escriba o ejecute desde este medio.
		El módulo de control de dispositivos deberá permitir la creación de listas blancas específicas construidas a partir del reconocimiento del ID del hardware de cada USB de almacenamiento.
		Deberá tener un módulo que permita la implementación de políticas de seguridad para la navegación web.
		Deberá incluir un módulo que proteja las transacciones bancarias.
		Deberá incluir un módulo de monitoreo de redes que permita monitorear la red permitiendo la creación y análisis de métricas de evaluación para discos duros, servicios críticos, CPUs, impresoras, enrutadores, switches, servidores web, servidores de correo y servidores de base de datos a fin de establecer semáforos que faciliten la lectura de informes y alertas de anomalías presentadas en la red, a fin de detectar oportunamente tendencias de rendimiento. Se aceptará sean capaces de exportar logs mediante syslog
		Deberá permitir implementar tareas de escaneo de malware en modo de reposo para de esta forma evitar saturar los recursos de los escritorios virtuales.
		Deberá contar con módulo de protección que permita auditar la seguridad a nivel físico de cualquier dispositivo USB que se conecte al escritorio virtual asegurándose de que de este no esté corrupto con algún tipo de keylogger físico, el sistema deberá solicitar un código de seguridad cada que se conecte un nuevo dispositivo.
Atributos de mitigación		Deberá mitigar el daño provocado por contagios; cierra los puertos, monitorea aplicaciones y motores de correo electrónico, analice archivos y carpetas, que efectúe seguimientos y bloquee las comunicaciones que generen una infección.
		Deberá incluir protección que amenace específicamente las vulnerabilidades del sistema operativo, deberá incluir protección anti-exploit capaz de proteger de esas amenazas que aprovechan las brechas de seguridad en los programas instalados, desde editores de texto hasta plugins de los navegadores.
		Deberá contar con un módulo de gestión de parches centralizado capaz de reconocer vulnerabilidades que derivan de la ausencia de parches en el sistema operativo y programas instalados en los escritorios virtuales.
		El módulo de gestión de parches deberá ser capaz

		de clasificar los parches que necesitan aplicarse en los escritorios virtuales a fin de cerrar los huecos de seguridad encontrados, así como lanzar pruebas de aplicabilidad de los mismos a fin de asegurarse de que estos no ocasionen problemas de compatibilidad.
		Deberá contar con un cortafuego administrable capaz de monitorear todo el tráfico entrante y saliente en todos y cada uno de los escritorios virtuales.
		El cortafuego deberá poder ser implementado en modo de piloto automático reconociendo todo el tráfico para luego implementar reglas específicas.
		El cortafuego deberá poder notificar cuando una aplicación sea bloqueada.
		El cortafuego deberá tener un asistente de configuración que permita implementar reglas de restricción y permiso a determinadas aplicaciones y puertos.
		Si el administrador así lo prefiere se podrá habilitar opción de desactivar cortafuego desde el cliente.
	Atributos de detección	Deberá incluir tecnología innovadora para escritorio virtual que detenga y elimine proactivamente el software malicioso, extienda la cobertura contra nuevos riesgos de seguridad y reduzca el costo de respuesta frente a epidemias.
		Deberá permitir defender los sistemas contra virus, gusanos, troyanos, phishing, adware y spyware.
		Deberá bloquear las amenazas que no escriben en el disco duro con el escaneo en memoria.
		Deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexión con servidores maliciosos de comando y detectar patrones típicos de equipos que forman parte de una Botnet.
		Deberá contar con protección contra ransomware que supervise el comportamiento de las aplicaciones y los procesos que intentan modificar los datos.
		Deberá bloquear una amplia gama de virus y amenazas de código malicioso, incluso los que están ocultos en archivos comprimidos; que descubra virus desconocidos con detección heurística y genérica.
		Deberá proteger contra exploits dirigidos a aplicaciones y servicios Microsoft, especialmente a servicios del sistema operativo Microsoft Windows, Microsoft Word, Microsoft Excel, Microsoft Outlook.
		Deberá incluir un antivirus residente capaz de analizar diferentes protocolos de comunicación como HTTP, HTTPS, SMPT, POP, IMAP y otros.
		El residente antivirus deberá poder tomar diversas

		acciones en caso de una infección, bloquear el acceso al archivo, desinfectar y copiar en cuarentena para su análisis, mandar a cuarentena o eliminar el archivo.
		El residente antivirus deberá poder tomar diversas acciones en caso de analizar archivos comprimidos, bloquear el acceso al archivo, desinfectar y copiar en cuarentena para su análisis, mandar a cuarentena o eliminar el archivo.
		El residente de antivirus deberá poder comprobar la existencia de virus informáticos en correos recibidos / enviados en el cliente de correo. Adicionalmente se podrá realizar la comprobación solo en los correos no leídos. El postor puede considerar otra consola para gestionar la protección de correo electrónico.
		El residente de antivirus deberá poder adjuntar un informe de ante un correo electrónico infectado.
		El residente deberá detectar y neutralizar amenazas de los programas maliciosos en los correos masivos antes incluso de que estén disponibles las actualizaciones de las firmas de virus correspondientes.
		Deberá contar con un módulo de copias de seguridad de información sensible que permita programar y ejecutar copias de seguridad de los archivos y carpetas más críticas en los clientes de forma diferencial y automática.
		El módulo de copias de seguridad debe escanear la data respaldada garantizando de esta manera de que se resguarden copias sin virus.
		El módulo de copias de seguridad debe permitir definir el destino de la información a respaldar.

ALCANCES PARA LA IMPLEMENTACIÓN

- El Contratista deberá presentar dentro de los 10 días posteriores a la suscripción del contrato, el Plan de Trabajo de la implementación.
- El Contratista asumirá todos los daños y perjuicios ocasionados por su personal o por trabajos defectuosos realizados por ellos mismos, a las instalaciones, equipos y demás bienes del Ministerio de Desarrollo Agrario y Riego y de terceros, durante la ejecución de la implementación.
- La instalación y puesta en funcionamiento deberá ser realizado por el especialista presentado en la propuesta del Postor detallado en el numeral 9 .C
- La ejecución de la implementación no deberá afectar el funcionamiento del equipamiento preexistente ni alterar las labores del personal, por lo que los trabajos de instalación, configuración y puesta en funcionamiento se realizarán en horarios que disponga el Ministerio de Desarrollo Agrario y Riego.
- El Contratista será el responsable de la implementación (instalación, configuración y puesta en funcionamiento) de la solución ofertada, para lo cual deberá incluir todo el licenciamiento necesario que; aunque no se hubiesen incluido en las presentes especificaciones técnicas, sean necesarios para cumplir las características técnicas solicitadas, sin que ello implique costo

adicional al Ministerio de Desarrollo Agrario y Riego. ~~La Entidad brindará la infraestructura física de cómputo, almacenamiento y redes, los espacios físicos, ambientales, eléctricos y de cableado estructurado para la correcta instalación y puesta en funcionamiento de los bienes solicitados.~~ MIDAGRI brindará al contratista, todos los recursos (hardware, licenciamiento de los nodos con VMware vSphere 7 Enterprise Plus, almacenamiento y redes, espacios físicos, ambientales, eléctricos y de cableado estructurado) que sean necesarios para la correcta instalación y puesta en funcionamiento de la solución ofertada.⁵

- La solución ofertada deberá ser instalada y configurada en la infraestructura tecnológica alojada en el Data Center del Ministerio de Desarrollo Agrario y Riego, el cual cuenta con las condiciones de energía estabilizada y climatización para el correcto funcionamiento.

PRESENTACION OBLIGATORIA DENTRO DE LA PROPUESTA

- El Postor para la admisión de su propuesta, deberá incluir al lado de cada una de las especificaciones técnicas solicitadas (ver Anexo 01); contenidas en el numeral CARACTERÍSTICAS TÉCNICAS, la captura de pantalla y Link del fabricante de donde se obtuvo la captura (como: catálogos y/o brouchure y/o folletería y/o datasheet y/o instructivos y/o ficha técnica y/o manual y/o consola – [en idioma español o inglés](#)⁶); lo cual permitirá al MIDAGRI, verificar fehacientemente que la solución propuesta por el Postor cumple todas las características técnicas solicitadas, [o carta del fabricante con referencia al presente proceso que acredite el cumplimiento de las especificaciones técnicas solicitadas.](#)⁷
- **NOTA:** La presente exigencia no es obligatoria para el caso de las características generales del módulo de virtualización, características generales del módulo de seguridad de acceso y características generales del módulo de seguridad de virtualización.⁸

GARANTIA DE LOS BIENES

Dos (02) años de garantía

8. PRESTACIÓN ACCESORIAS A LA PRESTACIÓN PRINCIPAL:

a) SOPORTE TÉCNICO ESPECIALIZADO

El CONTRATISTA, deberá contar con un servicio de soporte técnico especializado para realizar la atención de incidentes, requerimientos, y asesoría técnica sobre la solución implementada. Dicho servicio deberá estar a disposición 24x7x365 por un periodo de dos (02) años iniciado desde la conformidad final de la solución implementada al MIDAGRI.

El soporte técnico incluye el derecho a actualizaciones de firmware y otros componentes. Las actualizaciones se realizarán a demanda, previa coordinación con el CONTRATISTA, y deberá contar con el apoyo presencial

⁵ Consulta N° 03 de la empresa CLIC IT S.A.C

⁶ Consulta N° 24 de la empresa GRUPO ELECTRODATA S.A.C

⁷ Consulta N° 23 de la empresa GRUPO ELECTRODATA S.A.C

⁸ Observación N° 01 de la empresa CLIC IT S.A.C

y/o remoto del socio local de **software hardware**.⁹

La responsabilidad de resolver cualquier incidente, requerimiento o consulta será íntegramente del CONTRATISTA.

- **Tiempo de atención de Incidentes**

El CONTRATISTA tendrá un plazo máximo de ciento veinte (120) minutos para atender un problema o incidente reportado. Dicho plazo será contabilizado a partir de la recepción del reporte de falla por parte del CONTRATISTA hasta que un especialista del Contratista se ponga en contacto con el área de TI del MIDAGRI para dar inicio al procedimiento de diagnóstico y solución. El reporte podrá realizarse a través de correo electrónico o vía telefónica. Para tal fin, el CONTRATISTA deberá entregar las cuentas de correo electrónico y números telefónicos, los mismos que estarán a disposición de la Entidad las 24 horas del día, los 7 días de la semana, durante el periodo de vigencia del contrato. Ante el reporte de alguna falla por parte de la Entidad, el CONTRATISTA asignará un número de registro de atención a dicho reporte.

- **Tiempo de solución de Incidentes**

Ante un fallo parcial del sistema, El CONTRATISTA tendrá un plazo máximo de ciento ochenta minutos (180) minutos para solucionar el incidente. Dicho plazo será contabilizado a partir de que el especialista asignado ha contactado al área de TI del MIDAGRI para iniciar el diagnóstico.

- **Tiempo de atención de requerimientos**

- El CONTRATISTA tendrá un plazo máximo de ciento veinte (120) minutos para atender los requerimientos y/o solicitudes de asesoría técnica.
- El CONTRATISTA deberá considerar en su propuesta una bolsa anual de 15 horas para la atención de requerimientos.
- El CONTRATISTA deberá entregar un reporte anual detallando los incidentes y requerimientos atendidos durante el año. Dicho reporte deberá incluir como mínimo:
 - Número de reporte.
 - Fecha de registro.
 - Descripción del caso.
 - Estado.
 - Fecha de solución.
 - Detalle de horas utilizadas por requerimiento, y el total acumulado de horas a la fecha.
 - Personal asignado.

b) CAPACITACIÓN

El CONTRATISTA deberá efectuar un taller de capacitación para un mínimo de cuatro (04) personas de la OFICINA GENERAL DE TECNOLOGÍA DE LA

⁹ Consulta N° 05 de la empresa CLIC IT S.A.C

INFORMACIÓN.

El taller de capacitación será dictado en las instalaciones del CONTRATISTA o en el Ministerio de Desarrollo Agrario y Riego o de manera remota, previa coordinación con la OFICINA GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN, estará dirigido a cuatro (04) personas, con una duración mínima de 12 horas. Los certificados del curso deben contener las horas lectivas y las fechas que se realizó la capacitación.

El CONTRATISTA al inicio de cada curso debe entregar al personal asistente, todo el material necesario para el desarrollo de este tales como: syllabus, guías o separatas del curso, entre otros. Asimismo, debe contar con todos los recursos informáticos para desarrollar el temario del curso dictado.

El CONTRATISTA entregará los certificados de participación del taller de capacitación dentro del plazo máximo, asimismo estos formarán parte del entregable para la conformidad de la prestación principal.

El CONTRATISTA al finalizar Capacitación en conjunto con la OFICINA GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN emitirá las actas de conformidad por la capacitación.

9. REQUISITOS DE CALIFICACIÓN

B	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	<p><u>Requisitos:</u></p> <p>El postor debe acreditar un monto facturado acumulado equivalente a S/. 500,000.00 (Quinientos mil con 00/100 Soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.</p> <p>En el caso de postores que declaren en el Anexo N° 1 tener la condición de micro y pequeña empresa, se acredita una experiencia de S/. 99,500.00 (noventa y nueve mil quinientos con 00/100 Soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. En el caso de consorcios, todos los integrantes deben contar con la condición de micro y pequeña empresa.</p> <p>Se consideran bienes similares a los siguientes: Software de virtualización o solución de virtualización de escritorio o software de virtualización de aplicaciones.</p> <p><u>Acreditación:</u></p> <p>La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago¹⁰, correspondientes a un máximo de veinte (20) contrataciones.</p>

¹⁰ Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

"... el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"

(...)

"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia"

	<p>En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p> <p>En el caso de suministro, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los ocho (8) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.</p> <p>En los casos que se acredite experiencia adquirida en consorcio, debe presentarse la promesa de consorcio o el contrato de consorcio del cual se desprenda fehacientemente el porcentaje de las obligaciones que se asumió en el contrato presentado; de lo contrario, no se computará la experiencia proveniente de dicho contrato.</p> <p>Asimismo, cuando se presenten contratos derivados de procesos de selección convocados antes del 20.09.2012, la calificación se ceñirá al método descrito en la Directiva "Participación de Proveedores en Consorcio en las Contrataciones del Estado", debiendo presumirse que el porcentaje de las obligaciones equivale al porcentaje de participación de la promesa de consorcio o del contrato de consorcio. En caso que en dichos documentos no se consigne el porcentaje de participación se presumirá que las obligaciones se ejecutaron en partes iguales.</p> <p>Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.</p> <p>Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el Anexo N° 9.</p> <p>Cuando en los contratos, órdenes de compra o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de compra o de cancelación del comprobante de pago, según corresponda.</p> <p>Sin perjuicio de lo anterior, los postores deben llenar y presentar el Anexo N° 8 referido a la Experiencia del Postor en la Especialidad.</p>
--	--

C	CAPACIDAD TÉCNICA Y PROFESIONAL
C.1	FORMACION ACADEMICA
	<p><u>Requisitos:</u></p> <p>Un (01) especialista en virtualización de escritorio- Título o Bachiller en: Ingeniería Electrónica y/o Informática y/o Sistemas y/o Computación e Informática y/o Computación y Sistemas y/o Estadística e Informática y/o Redes y Comunicaciones de Datos y/o Telecomunicaciones.</p> <p><u>Acreditación:</u> El GRADO O TÍTULO PROFESIONAL REQUERIDO será verificado por el comité de selección en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria – SUNEDU a través del siguiente enlace: https://onlinea.sunedu.gob.pe/ // o en el Registro Nacional de Certificados, Grados y Títulos a cargo del Ministerio de Educación a través del siguiente enlace: http://www.titulosinstitutos.pe/, según corresponda.</p> <p>En caso DEL GRADO O TÍTULO PROFESIONAL REQUERIDO no se encuentre inscrito en el referido registro, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.</p>
C.2	EXPERIENCIA DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>Un (01) especialista en virtualización de escritorio:</p>

	<p>Experiencia mínima de cuatro (04) años como especialista en virtualización contabilizado a partir de la obtención del grado de bachiller.</p> <p><u>Acreditación:</u> La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.</p>
C.3	CAPACITACIÓN DEL PERSONAL CLAVE
	<p><u>Requisitos:</u></p> <p>Un (01) especialista en virtualización de escritorio: Contar con certificación oficial técnica a nivel profesional en software de virtualización emitida por la marca del software de virtualización ofertado.</p> <p><u>Acreditación:</u> La certificación oficial técnica a nivel profesional se acreditará con copia simple del CERTIFICADOS emitido por el fabricante.¹¹</p>

10. PLAZO DE ENTREGA DE LA PRESTACIÓN PRICIPAL

PLAZO DE ENTREGA, INSTALACIÓN Y PRUEBAS DE LOS BIENES

El plazo para la entrega, instalación y pruebas de los bienes **será máximo de veinte (20) días calendario**, contabilizados a partir del día siguiente de suscrito el contrato.

11. PLAZO DE ENTREGA DE LA PRESTACIÓN ACCESORIA

11.1 PLAZO DE EJECUCIÓN DEL SOPORTE TÉCNICO ESPECIALIZADO

El soporte técnico inicia desde el día siguiente de emitida la conformidad de la instalación y configuración de los bienes y se extiende por un plazo de dos (02) años, este puede realizarse de manera presencial o remota.

11.2 PLAZO DE EJECUCIÓN DE LA CAPACITACIÓN

Dentro del periodo de los 20 días calendario contabilizado a partir del día siguiente de suscrito el contrato, este puede realizarse de manera presencial o remota previa coordinación con la Oficina General de Tecnología de la Información.

12. ENTREGABLES

Al finalizar la implementación, el contratista deberá presentar el informe final a través de la mesa de partes digital (<https://www.gob.pe/9247>) mediante una carta dirigida a la Oficina General de Tecnología de la Información.

El informe final, debe contener como mínimo la siguiente documentación:

- Acta de entrega
- Acta de Implementación
- Certificados de participación del Taller de Capacitación
- Informe del servicio realizado, el cual debe contener como mínimo lo siguiente:
 - Acciones y configuraciones realizadas.

¹¹ Observación N° 07 de la empresa CLIC IT S.A.C

- Imágenes Fotográficas.
- Manuales.
- Declaración jurada de asistencia técnica.
- Certificado de participación a la inducción.
- Guía de remisión del Contratista.
- Comprobante de pago del Contratista.
- Carta de autorización de pago mediante CCI – Código de Cuenta Interbancario.

El único entregable debe ser entregado hasta los veinte (20) días calendarios, contabilizados desde el día siguiente de la firma del contrato.

13. CONFORMIDAD DE LA RECEPCION

La conformidad estará a cargo de la Oficina General de Tecnologías de la Información del MIDAGRI.

14. LUGAR DE ENTREGA

El lugar de entrega e instalación es: Av. General Felipe Salaverry cera. 13 esquina con Av. Húsares de Junín y JR. Cahuide, Urb. Escuela de la Agricultura - Jesús María.

15. FORMAS Y CONDICIONES DE PAGOS

15.1 PRESTACIÓN PRINCIPAL

De conformidad con el Art. 171° del Reglamento de la Ley de contrataciones del Estado, se realizará pago único, luego de ejecutado la compra y otorgada la conformidad respectiva por la Oficina General de Tecnologías de la Información del MIDAGRI.

15.2 PRESTACIÓN ACCESORIA

Soporte Técnico Especializado:

De conformidad con el Art. 171° del Reglamento de la Ley de contrataciones del Estado, el pago se realizará en dos (02) armadas anuales (uno por año), finalizado el periodo anual, después de emitida la conformidad por parte de la OFICINA GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN.

Capacitación:

De conformidad con el Art. 171° del Reglamento de la Ley de contrataciones del Estado, el pago se realizará en una sola armada, después de emitida la conformidad por parte de la OFICINA GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN.

16. PENALIDADES

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso, de conformidad con el artículo 162 del Reglamento.

16.1 OTRAS PENALIDADES

Se aplicarán otras penalidades de incumplimiento en el caso siguiente:
Por no cumplir con la atención a los incidentes dentro de los tiempos especificados.

N°	Descripción	Detalle	Tiempo máximo de resolución	Monto de penalidad
1	Tiempo de atención de incidentes	Tiempo empleado por el CONTRATISTA para atender un problema o incidente.	Ciento veinte (120) minutos	1% por incidente de la UIT
		El tiempo se contabiliza a partir de la recepción del reporte de falla por parte del CONTRATISTA hasta que un especialista del Contratista se ponga en contacto con la OGTI del MIDAGRI para dar inicio al procedimiento de diagnóstico y solución. El reporte podrá realizarse a través de correo electrónico o vía telefónica.		
2	Tiempo de solución de incidentes	Tiempo empleado por el CONTRATISTA para solucionar el incidente.	Ciento ochenta (180) minutos	3% por incidente de la UIT
		Dicho plazo será contabilizado a partir de que el especialista asignado ha contactado a la OGTI del MIDAGRI para iniciar el diagnóstico.		
3	Tiempo de atención de requerimientos	Tiempo empleado por el CONTRATISTA para atender los requerimientos y/o solicitudes de asesoría técnica.	Ciento veinte (120) minutos	10% por requerimiento de la UIT
		Dicho plazo será contabilizado a partir de que el especialista de OGTI ha contactado al contratista.		

Por no terminar la capacitación durante los 20 días computados a partir del día siguiente de la firma del contrato.

N°	Descripción	Detalle	Tiempo máximo de ejecución	Monto de penalidad
1	Capacitación	Tiempo empleado por el CONTRATISTA para terminar la capacitación.	veinte (20) días	10% de la UIT

La Oficina General de Tecnología de Información, informará a la oficina de administración, para las acciones correspondientes.

17. CLAUSULA ANTICORRUPCIÓN

"EL CONTRATISTA declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado, ofrecido, negociado o efectuado, cualquier pago o, en general, cualquier beneficio o incentivo ilegal en relación al contrato.

Asimismo, EL CONTRATISTA se obliga a conducirse en todo momento con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participantes, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas a las que se refiere el artículo 7 del Reglamento de la Ley de Contrataciones del Estado.

Además, EL CONTRATISTA se compromete a i) comunicar a las autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento; y ii) adoptar medidas técnicas, organizativas y/o de personal apropiadas para evitar los referidos actos o prácticas".

Finalmente, EL CONTRATISTA se compromete a no colocar a los funcionarios públicos con los que deba interactuar, en situaciones reñidas con la ética. En tal sentido, reconoce y acepta la prohibición de ofrecerles a éstos cualquier tipo de obsequio, donación, beneficio y/o gratificación, ya sea de bienes o servicios, cualquiera sea la finalidad con la que se lo haga.

18. RESPONSABILIDAD POR VICIOS OCULTOS

El contratista será responsable por la calidad ofrecida y los vicios ocultos del servicio ofertado, conforme a lo indicado en el numeral 40.2 del artículo 40º de la Ley de Contrataciones, por un plazo de un año (01) año, contados a partir de la conformidad otorgada por parte del Ministerio de Desarrollo Agrario y Riego.

El Ministerio de Desarrollo Agrario y Riego. se reserva el derecho de comprobar la veracidad, originalidad y cumplimiento, de toda la información incluida en la propuesta del Postor, a fin de aceptar o desestimar su propuesta.

19. CONFIDENCIALIDAD

El contratista tiene la obligación de guardar absoluta confidencialidad y reserva respecto a los documentos relacionados con la actual presentación y/o aquellos que deriven de esta (documentos, informes, fotografías, planos, en formato digital y/o físico) quedando prohibido revelar dicha información a terceros.

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año de la unidad, la paz y el desarrollo”

Anexo 01

A	SOLUCIÓN DE VIRTUALIZACION DE ESCRITORIOS			
A.1	MODULO DE VIRTUALIZACIÓN			
	CARACTERÍSTICA	DESCRIPCIÓN	Captura de Pantalla	Link del fabricante
	Características generales	Licenciamiento de software de virtualización de escritorio de la última versión estable y liberada por el fabricante a la fecha de la presentación de la propuesta, para 70 usuarios nombrados.		
		Licenciamiento debe ser del tipo OPEN, el cual:		
		o No debe estar asociado a servidor físico.		
		o Debe permitir la instalación en otro hardware de ser necesario.		
		Licenciamiento por el periodo de 02 años, el cual debe incluir derecho a actualizaciones y soporte 24x7, provisto directamente por el fabricante.		
		<p>Se deben considerar:</p> <ul style="list-style-type: none"> o Administración de acceso de los escritorios virtuales. o Sistema Operativo Windows para escritorios virtuales o Licenciamiento de módulo de virtualización. o Licenciamiento de administración de acceso a los escritorios virtuales. o Licenciamiento de sistema operativo Windows para escritorios virtuales. <p>Si producto de la arquitectura de su solución requiere licenciamiento adicional, este lo debe considerar con la finalidad que los 70 usuarios estén correctamente licenciados en la solución VDI y en el sistema operativo Windows cliente.¹²</p>		

¹² Consulta N° 03 de la empresa CLIC IT S.A.C

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año de la unidad, la paz y el desarrollo”

		Licenciamiento bajo modelo de suscripción, donde el enlace de comunicación a la Consola de Administración, VDIs y/o Aplicaciones sea ON-PREmise.		
		MIDAGRI cuenta con una plataforma de virtualización compuesta por 8 nodos con un total de 16 procesadores, cada procesador cuenta con 24 cores desplegada con el siguiente software:		
		· vRealize Log Insight 16 CPU		
		· vRealize Operations 8 Enterprise - 16 CPU		
		· vSphere 7 Enterprise Plus - 16 CPU		
		· vCenter Server 7 Standard		
		Se debe proporcionar el licenciamiento de todo el software necesario, para el funcionamiento del módulo de virtualización solicitado.		
		Debe estar vigente tecnológicamente y pertenecer a la última versión o generación liberada por el fabricante. Se debe acreditar para la presentación de la propuesta con una carta oficial del fabricante con referencia al presente proceso. ¹³		
	Administración de la solución	Debe permitir configurar, administrar y gestionar grupos de escritorios y aplicaciones virtuales a entregar, uso de licencias de escritorio, aprovisionamiento de imágenes de escritorio virtual, autenticación y control de autorizaciones.		
		Debe contar con una herramienta o funcionalidad nativa de mesa de ayuda, en la que sea posible que un técnico intervenga en la sesión virtualizada.		
		Debe permitir la interacción entre el administrador y el usuario mediante el envío de mensajes directamente desde la consola de monitoreo y soporte.		
		Debe permitir la visualización de la imagen del escritorio virtual en varios monitores.		
		Debe soportar políticas de impresión de tal manera que pueda configurarse, sin necesidad de cambios en los scripts de inicio de sesión, mediante la aplicación de GPO's y de forma nativa de la solución.		
		Debe presentar un tablero con un resumen de la información de alerta para ver y remediar incidentes.		

¹³ Observación N° 01 de la empresa CLIC IT S.A.C

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

		Debe contar con una herramienta para monitorear el uso, salud y desempeño de la infraestructura, escritorios y protocolos.		
		La herramienta de monitoreo debe tener registros para auditar el acceso a las máquinas virtuales.		
	Gestión de recursos virtualizados	Debe ser capaz de provisionar y controlar el acceso a los recursos virtualizados (aplicaciones y escritorios) ya sea en el modelo de sesión única o multisesión cuando se encuentre disponible.		
		Debe tener recursos para aprovisionar y desaproveionar máquinas virtuales bajo demanda, independientemente de donde se asigne este recurso.		
		Debe implementar el aprovisionamiento y administración de recursos virtualizados en máquinas virtuales con los sistemas operativos Microsoft Windows 10 o superior, RHEL 8 o superiores y Windows Server 2019 o superiores.		
		Debe contar con una herramienta integrada a la solución que permita el aprovisionamiento de máquinas virtuales desde una sola imagen central, de manera que los administradores tengan autonomía para entregar los recursos con las actualizaciones más recientes, cada vez que se realice el inicio de sesión.		
		El aprovisionamiento y desaproveionamiento de recursos (máquinas virtuales) debe ser opcional según demanda, y compatible con cualquier Hipervisor.		
		Debe permitir la creación de varias máquinas virtuales automáticamente, basadas en la misma imagen del sistema operativo.		
		Debe permitir la configuración de un grupo de escritorios virtuales en standby (o aprovisionado) que pueda atender la demanda de conexión de los usuarios de forma paulatina, evitando el desperdicio de recursos físicos con escritorios virtuales encendidos y sin uso, estos escritorios en modo standby deben ser activados en cada grupo de escritorios virtuales a través de la consola de administración.		
		Debe permitir la creación de varios escritorios virtuales automáticamente, basados en una imagen de sistema operativo preconfigurada, acelerando la entrega de escritorios virtuales a usuarios no persistentes.		

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año de la unidad, la paz y el desarrollo”

		Debe poder crear grupos persistentes de escritorios virtuales, es decir, grupos de escritorios virtuales que se pueden aprovisionar para el usuario y que, después del primer aprovisionamiento, solo puede acceder el mismo usuario.		
		Debe ofrecer una herramienta de virtualización de aplicaciones que permita a los administradores de escritorio transformar aplicaciones compatibles con Microsoft Windows en aplicaciones portátiles que puedan ejecutarse sin necesidad de un Escritorio completo.		
		Deber permitir la creación y uso compartido o dedicado de escritorios virtuales sobre plataformas Windows y distribuciones Linux, sin limitar el número de Escritorios de cada tipo hasta el total de licencias adquiridas en el presente procedimiento de selección.		
	Equilibrio de sesiones	A los efectos del balanceo de carga inteligente entre servidores de servicios de acceso a aplicaciones remotas, el software debe identificar y establecer la conexión del usuario con el servidor menos cargado; teniendo en cuenta factores como el uso de la CPU, el uso de la memoria y la cantidad de sesiones en ejecución. ¹⁴		
	Gestión de perfiles	La funcionalidad de gestión inteligente de perfiles debe ser una parte integrada de la solución, sin costo adicional.		
		Debe proporcionar la funcionalidad de perfil móvil, es decir, conservar las personalizaciones del perfil de usuario y almacenarlas en un servicio de gestión de perfiles dinámicos, aplicando las características conservadas por el usuario a los recursos virtualizados (aplicaciones o escritorios) siempre que los usuarios inicien sesión.		
		Debe permitir que el administrador use perfiles de solo lectura, que se descartan al cerrar la sesión, sin depender de los servidores de archivos.		
		Debe permitir que el dispositivo redirija las carpetas a los servidores de archivos especificados. Se deben redirigir las carpetas de archivos de usuario predeterminadas, como las que se enumeran a continuación: Escritorio, Documentos, Videos, Imágenes, Música, Descargas, Favoritos, Contactos, Enlaces, Búsquedas, Menú Inicio y AppData.		
		Debe permitir que la sincronización de los datos del perfil de usuario sea parcial, es decir, dando la posibilidad al administrador de seleccionar lo que		

¹⁴ Observación N° 04 de la empresa CLIC IT S.A.C

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año de la unidad, la paz y el desarrollo”

		debe o no sincronizar en el perfil de usuario, pudiendo realizar esta configuración de forma global o específica por usuario.		
		Debe poseer una solución de transmisión de perfiles para que se pueda entregar de manera escalonada siguiendo la demanda del usuario, sin que el usuario tenga que esperar a que su perfil completo comience a usarlo.		
		Debe permitir la sincronización de perfiles mientras el usuario está conectado, reduciendo así la carga excesiva de datos durante el cierre de sesión, realizando solo el delta al final del uso.		
	Experiencia del usuario	Debe proporcionar al usuario acceso a los recursos virtualizados desde un único portal, este portal de acceso debe estar disponible para acceso externo con alta disponibilidad en todos los Centros de Datos, sin embargo, la solución debe permitir que la sesión del usuario con el recurso virtualizado se establezca con el Centro de Datos más cercano al backend del servidor accedido por el recurso virtualizado.		
		Debe proporcionar una aplicación cliente que permita al usuario a través de un dispositivo físico acceder a un escritorio virtual o aplicación publicada, compatible con los siguientes sistemas operativos Windows, MacOS, Linux, Android, iOS y Chromebook.		
		Debe permitir que los usuarios marquen sus aplicaciones y escritorios favoritos, que se agregarán a una página separada en su perfil.		
		Debe contar con un cliente soportado para instalación y acceso a la plataforma para los siguientes Sistemas Operativos: Windows, Linux, MacOS, Android e IOS.		
		Debe soportar el uso de estaciones tipo thin client que utilicen sistemas operativos basados en Linux y/o Microsoft Windows Embedded.		
		Debe permitir; independientemente del método de acceso (cliente instalado o navegador web), la redirección multimedia, permitiendo así reproducir las aplicaciones de sonido en el sistema de sonido del dispositivo local.		
		Debe permitir al usuario utilizar un navegador web para acceder, a través del protocolo HTTPS, a un escritorio virtual o aplicación publicada, si el dispositivo físico utilizado no permite la instalación de la aplicación cliente de la solución ofrecida.		

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año de la unidad, la paz y el desarrollo”

		Debe permitir a los usuarios controlar los recursos de sonido, el tamaño de la ventana y reiniciar su escritorio virtual sin necesidad de la intervención del administrador, excepto para reiniciar los escritorios virtuales que funcionan con multisesión.		
		Debe permitir al usuario continuar con su trabajo, exactamente donde lo dejó, en caso de que necesite cambiar de estación de trabajo o abrir una sesión en otro tipo de equipo. Esta funcionalidad debe cerrar la sesión de usuario abierta en el dispositivo inicial y abrirla en el nuevo dispositivo, lo que permitirá que el escritorio "siga" al usuario.		
		Debe admitir de forma nativa y realizar la optimización del tráfico con respecto a las herramientas de colaboración más utilizadas, como Microsoft Teams, Zoom y Cisco Webex.		
		Debe permitir el uso de tokens criptográficos y tarjetas inteligentes para firmar documentos en escritorios virtuales.		
		La herramienta debe ser capaz de facilitar la interacción del usuario al acceder a aplicaciones y/o escritorios a través de dispositivos táctiles, optimizando las funciones emergentes del teclado, el desplazamiento de la pantalla y el zoom automático		
	Seguridad	Debe ofrecer un portal de autoservicio capaz de integrarse con la solución de virtualización de escritorio y otras aplicaciones Web, con el fin de unificar la experiencia del usuario y aumentar la seguridad en el acceso a los datos, aplicando configuraciones de autenticación de acceso condicional y de doble factor.		
		Debe permitir el acceso a escritorios y aplicaciones virtualizadas a través de un portal disponible vía Web, con autenticación segura y acceso vía SSL o TLS.		
		Debe controlar las acciones de “copiar y pegar” entre la máquina del usuario y el contenido accedido.		
		Debe tener recursos para controlar la captura de pantalla de los recursos virtualizados (anticaptura de pantalla).		
		Debe disponer de recursos para evitar la captura/ copia de información tecleada durante el acceso a los recursos virtualizados (Anti-keylogger o similar).		
		Debe restringir o permitir que el contenido disponible se imprima en impresoras conectadas al dispositivo del usuario.		

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año de la unidad, la paz y el desarrollo”

		Debe permitir o bloquear la conexión de los periféricos de los usuarios con los escritorios y aplicaciones virtualizadas, tales como: discos locales, unidades de red, CD-ROM, DVD-ROM y dispositivos extraíbles (pendrive, HD externo, etc.).		
		Debe poner a disposición, en la interfaz de acceso, únicamente los escritorios virtuales o aplicaciones publicadas a los que el usuario tenga acceso, observando los permisos y privilegios definidos luego del proceso de autenticación y análisis del dispositivo.		
		Debe contar con recursos para controlar los cambios realizados en el entorno de virtualización de aplicaciones y escritorios, de manera que, cuando sea necesario, los administradores tengan acceso a logs con los cambios realizados en la configuración o permisos del entorno, con fecha y autor de los cambios		
A.2	MODULO DE SEGURIDAD DE ACCESO			
	DESCRIPCIÓN	CARACTERÍSTICAS TÉCNICAS		
	Características generales	Certificado Digital SSL por el período de 02 años.		
		Debe soportar acceso a los usuarios a través de un portal, que deberá contener asociado de un certificado digital de una entidad de certificados públicos de confianza, como mínimo contener algoritmo RSA Public Key SHA-2 (Funciones hash admitidas: 256, 384, 512), Compatibilidad con el cifrado de claves públicas de 2.048 bits (3.072 bits y 4.096 bits disponibles).		
	Seguridad de segundo factor de autenticación	La solución debe implementar una autenticación multifactor, el cual puede ser solicitado al ingresar a contenido corporativo desde redes internas y/o externas. Este sistema deberá soportar el algoritmo HMAC-Based One-time Password (HOTP) especificado en la RFC 4226 y/o el algoritmo Time-based One-time Password (TOTP) especificado en la RFC 6238.		
A.3	MODULO DE SEGURIDAD DE VIRTUALIZACIÓN			
	DESCRIPCIÓN	CARACTERÍSTICAS TÉCNICAS		
	Características generales	Licenciamiento de software antimalware de la última versión estable y liberada por el fabricante a la fecha de la presentación de la propuesta, para 70 escritorios virtuales.		

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

		Licenciamiento por el periodo de 02 años, el cual debe incluir derecho a actualizaciones y soporte 24x7.		
		El licenciamiento de software antimalware debe ser gestionado a través de una consola implementada en los servidores de la Entidad.		
		El software debe incluir un sistema de análisis de vulnerabilidades derivadas de plataformas Windows y programas de terceros que permita la descarga centralizada de parches, la aplicabilidad, la distribución y la instalación remota de estos. Este sistema debe estar integrado al software antimalware por lo que no deberá requerir la instalación de ningún componente adicional para su normal desempeño.		
		El software antimalware debe estar en idioma español.		
		Deberá contar con un sistema de distribución y despliegue centralizado permitiendo en determinados casos generar instaladores independientes y personalizados.		
		La consola de administración debe poder instalarse en sistemas operativos tales como Windows Server 2019 o posterior, o se podrá desplegar en la nube.		
		La consola de administración deberá poder lanzar tareas de despliegue de clientes de forma remota.		
		La consola de administración deberá poder mostrar un resumen de la instalación indicando el estado y sugiriendo una acción de refuerzo si fuese necesario.		
		La consola deberá ser 100% web permitiendo implementar una nube privada a través de un componente web seguro (https), a fin de poder gestionar los escritorios virtuales de la red corporativa de forma transparente . ¹⁵		
		La consola de administración deberá poder registrar eventos creando logs por cada uno de los eventos que realice dependiendo del ítem (exploración, actualización, bloqueos, etc.)		
		La consola de administración deberá permitir implementar exclusiones en la exploración, con capacidad para excluir de la exploración archivos, directorios y/o procesos, etc.; de forma centralizada.		

¹⁵ Consulta N° 14 de la empresa GRUPO ELECTRODATA S.A.C

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

		La consola de administración deberá permitir la programación de tareas, capacidad para programar tareas de exploración, actualización, etc.		
		La consola de administración deberá permitir la configuración de repositorios para actualización, capacidad para agregar/eliminar repositorios hacia donde se descarga la actualización de las definiciones de virus.		
		La consola de administración deberá permitir la instalación remota, pudiendo lanzar tareas de instalación en clientes de forma remota desde un servidor de administración antivirus.		
		La consola de administración deberá mostrar un inventario general de todos los escritorios virtuales, logrando especificar los recursos de cómputo y almacenamiento que tienen instalado todos y cada uno de los escritorios virtuales protegidos.		
		La consola de administración deberá poder programar análisis de malware en todos los escritorios virtuales sin que esto implique una saturación del procesador o memoria para realizar esta actividad, para esto se deberá poder especificar que el escaneo se realice utilizando los tiempos muertos del usuario, el objetivo es evitar saturar los recursos cuando el usuario los necesite.		
		La consola de administración deberá contar con una cuarentena local capaz de aislar posibles amenazas de malware no firmadas, pudiendo liberar y limpiar programas o archivos.		
		La consola de administración deberá poder reportar y enviar directamente al fabricante, software y/o amenazas no firmadas para su evaluación.		
	Gestión y gobierno centralizado	La consola de administración deberá poder integrarse con el directorio activo a fin de llevar una sola gestión (grupos organizativos)		
		La consola de administración deberá tener la capacidad de definir políticas de bloqueo de configuraciones por medio de una contraseña. Este bloqueo debe ser selectivo para configuraciones de objetos específicos (Módulos de protección). Se aceptará que el bloqueo de configuraciones se realice por medio de la aprobación de un usuario administrador.		
		Este sistema deberá tener la capacidad de generar reportes locales en cada escritorio virtual, referentes a todas las transacciones o eventos de seguridad realizadas por cada producto.		
		Deberá permitir la actualización independiente de productos para aquellos equipos que no puedan sincronizar con la consola.		

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

		Deberá proteger sistemas operativos como Windows Server 2019 o superior y Windows 10 o superior.		
		Deberá incluir un sistema de análisis basado en algoritmos heurísticos capaces de detectar malware por similitud.		
		Deberá incluir un sistema que optimice la detección y eliminación de malware empaquetado usado para saturar el performance de los residentes antivirus lanzando miles de variables a partir de un malware ya conocido.		
		Deberá incluir tecnología basada en el análisis del comportamiento de amenazas logrando detenerlas incluso sin estar firmadas.		
	Tecnología antimalware	Deberá contar un módulo de protección especialmente diseñado para hacerle frente a todo tipo de amenazas de tipo RANSOMWARE cual deberá permitir poner en cuarentena la amenaza y si fuese necesario incluir una lista blanca de aplicaciones específicamente para este módulo.		
		Deberá poder reconocer y bloquear amenazas de día cero basadas en vulnerabilidades del sistema operativo y programas instalados.		
		Deberá incluir tecnologías de Machine Learning que le permitan automatizar el aprendizaje de nuevas amenazas de malware a través de sus diferentes sensores o tecnologías propuestas.		
		Deberá contar con tecnologías de inteligencia artificial y aprendizaje automático capaz de reconocer y actuar sobre ataques de tipo malware ofuscado.		
		Deberá tener un módulo que permita la implementación de políticas de seguridad para el control de aplicaciones, el mismo que deberá poder definir aplicaciones en lista negra para evitar que estas se ejecuten en los escritorios virtuales.		
		El módulo de control de aplicaciones deberá poder implementar sus políticas de aplicaciones en lista negras reconociendo el hash, versiones y fabricantes específicos de las aplicaciones a bloquear.		
		El módulo de control de aplicaciones deberá tener un modo que permita la implementación de políticas de seguridad para el control de aplicaciones el mismo que deberá poder definir aplicaciones en lista blanca que permitan que solo estas puedan ejecutarse en determinados escritorios virtuales.		
	Atributos de prevención	El módulo de control de aplicaciones deberá poder aplicar políticas de seguridad a directorios y archivos específicos.		

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”
“Año de la unidad, la paz y el desarrollo”

		El módulo de control de aplicaciones deberá permitir que el usuario pueda solicitar permiso de acceso a determinada aplicación bloqueada desde su escritorio virtual, a fin de mejorar los tiempos de respuesta con el usuario.		
		Deberá incluir una protección contra dispositivos USB físicos manipulados.		
		Deberá tener un módulo que permita la implementación de políticas de seguridad para el control de dispositivos extraíbles, el mismo que deberá poder ser desplegado, habilitado o deshabilitado desde la consola de administración.		
		El módulo de control de dispositivos deberá tener la capacidad de asignar privilegios de solo lectura a cualquier USB de almacenamiento externo que se conecte al escritorio virtual a fin de evitar que cualquier aplicación de peligro se escriba o ejecute desde este medio.		
		El módulo de control de dispositivos deberá permitir la creación de listas blancas específicas construidas a partir del reconocimiento del ID del hardware de cada USB de almacenamiento.		
		Deberá tener un módulo que permita la implementación de políticas de seguridad para la navegación web.		
		Deberá incluir un módulo que proteja las transacciones bancarias.		
		Deberá incluir un módulo de monitoreo de redes que permita monitorear la red permitiendo la creación y análisis de métricas de evaluación para discos duros, servicios críticos, CPUs, impresoras, enrutadores, switches, servidores web, servidores de correo y servidores de base de datos a fin de establecer semáforos que faciliten la lectura de informes y alertas de anomalías presentadas en la red, a fin de detectar oportunamente tendencias de rendimiento. Se aceptará sean capaces de exportar logs mediante syslog		
		Deberá permitir implementar tareas de escaneo de malware en modo de reposo para de esta forma evitar saturar los recursos de los escritorios virtuales.		
		Deberá contar con módulo de protección que permita auditar la seguridad a nivel físico de cualquier dispositivo USB que se conecte al escritorio virtual asegurándose de que de este no esté corrupto con algún tipo de keylogger físico, el sistema deberá solicitar un código de seguridad cada que se conecte un nuevo dispositivo.		

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año de la unidad, la paz y el desarrollo”

		Deberá mitigar el daño provocado por contagios; cierra los puertos, monitorea aplicaciones y motores de correo electrónico, analice archivos y carpetas, que efectúe seguimientos y bloquee las comunicaciones que generen una infección.		
		Deberá incluir protección que amenace específicamente las vulnerabilidades del sistema operativo, deberá incluir protección anti-exploit capaz de proteger de esas amenazas que aprovechan las brechas de seguridad en los programas instalados, desde editores de texto hasta plugins de los navegadores.		
		Deberá contar con un módulo de gestión de parches centralizado capaz de reconocer vulnerabilidades que derivan de la ausencia de parches en el sistema operativo y programas instalados en los escritorios virtuales.		
	Atributos de mitigación	El módulo de gestión de parches deberá ser capaz de clasificar los parches que necesitan aplicarse en los escritorios virtuales a fin de cerrar los huecos de seguridad encontrados, así como lanzar pruebas de aplicabilidad de los mismos a fin de asegurarse de que estos no ocasionen problemas de compatibilidad.		
		Deberá contar con un cortafuego administrable capaz de monitorear todo el tráfico entrante y saliente en todos y cada uno de los escritorios virtuales.		
		El cortafuego deberá poder ser implementado en modo de piloto automático reconociendo todo el tráfico para luego implementar reglas específicas.		
		El cortafuego deberá poder notificar cuando una aplicación sea bloqueada.		
		El cortafuego deberá tener un asistente de configuración que permita implementar reglas de restricción y permiso a determinadas aplicaciones y puertos.		
		Si el administrador así lo prefiere se podrá habilitar opción de desactivar cortafuego desde el cliente.		
	Atributos de detección	Deberá incluir tecnología innovadora para escritorio virtual que detenga y elimine proactivamente el software malicioso, extienda la cobertura contra nuevos riesgos de seguridad y reduzca el costo de respuesta frente a epidemias.		
		Deberá permitir defender los sistemas contra virus, gusanos, troyanos, phishing, adware y spyware.		

“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año de la unidad, la paz y el desarrollo”

		Deberá bloquear las amenazas que no escriben en el disco duro con el escaneo en memoria.		
		Deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexión con servidores maliciosos de comando y detectar patrones típicos de equipos que forman parte de una Botnet.		
		Deberá contar con protección contra ransomware que supervise el comportamiento de las aplicaciones y los procesos que intentan modificar los datos.		
		Deberá bloquear una amplia gama de virus y amenazas de código malicioso, incluso los que están ocultos en archivos comprimidos; que descubra virus desconocidos con detección heurística y genérica.		
		Deberá proteger contra exploits dirigidos a aplicaciones y servicios Microsoft, especialmente a servicios del sistema operativo Microsoft Windows, Microsoft Word, Microsoft Excel, Microsoft Outlook.		
		Deberá incluir un antivirus residente capaz de analizar diferentes protocolos de comunicación como HTTP, HTTPS, SMPT, POP, IMAP y otros.		
		El residente antivirus deberá poder tomar diversas acciones en caso de una infección, bloquear el acceso al archivo, desinfectar y copiar en cuarentena para su análisis, mandar a cuarentena o eliminar el archivo.		
		El residente antivirus deberá poder tomar diversas acciones en caso de analizar archivos comprimidos, bloquear el acceso al archivo, desinfectar y copiar en cuarentena para su análisis, mandar a cuarentena o eliminar el archivo.		
		El residente de antivirus deberá poder comprobar la existencia de virus informáticos en correos recibidos / enviados en el cliente de correo. Adicionalmente se podrá realizar la comprobación solo en los correos no leídos. El postor puede considerar otra consola para gestionar la protección de correo electrónico.		
		El residente de antivirus deberá poder adjuntar un informe de ante un correo electrónico infectado.		
		El residente deberá detectar y neutralizar amenazas de los programas maliciosos en los correos masivos antes incluso de que estén disponibles las actualizaciones de las firmas de virus correspondientes.		



“Decenio de la Igualdad de Oportunidades para Mujeres y Hombres”

“Año de la unidad, la paz y el desarrollo”

		Deberá contar con un módulo de copias de seguridad de información sensible que permita programar y ejecutar copias de seguridad de los archivos y carpetas más críticas en los clientes de forma diferencial y automática.		
		El módulo de copias de seguridad debe escanear la data respaldada garantizando de esta manera de que se resguarden copias sin virus.		
		El módulo de copias de seguridad debe permitir definir el destino de la información a respaldar.		