Asunción, 25 de agosto de 2017.

Ref.: Contratación Directa N° 14/2017
"ADQUISICIÓN DE ACTIVOS INTANGIBLES"
ID N°: 334.735.-

Señores
OFERENTES
Presente

ADENDA Nº 01

La **Auditoría General del Poder Ejecutivo,** procede a realizar Adenda a la Carta de Invitación en atención a la NOTA DNCP/DNC/ N° 21282/2017 de fecha 24 de agosto del corriente, así mismo, les recordamos que las modificaciones realizadas formarán parte de la Carta de Invitación; y por consiguiente, serán de observación y aplicación obligatoria por parte de los oferentes.

ENMIENDA 1:

La Convocante establece modificar la Carta de Invitación, en los ***puntos 6, 7, 14, 17, 18, 20 y 31 del Anexo B***, quedando como se detalla a continuación:

6. Para aclaraciones sobre los documentos que forman parte de la Carta de Invitación, la dirección y contacto de la Convocante es la siguiente: *Lic. Marcos Sosa, Jefe de la UOC, dirección Juan Bautista Alberdi Nª 972 c/ Manduvirá, en la oficina de la Unidad Operativa de Contrataciones (UOC). Teléfono 493 171/5.- uoc@agpe.gov.py.-*

7. Fecha y hora límites para realizar consultas: 01/09/2017 hasta las 10:00 horas

***14.* El porcentaje de garantía de mantenimiento de ofertas deberá ser del:** *5% sobre el monto total de la oferta.*

17. Para propósitos de la presentación de las ofertas: *La dirección de la Convocante es, Juan Bautista Alberdi Nª 972 c/ Manduvirá", Unidad Operativa de Contrataciones (UOC).*

De no contar con un mínimo de 3 (tres) ofertas al vencimiento del plazo de entrega, la Autoridad competente de la Entidad, bajo su exclusiva responsabilidad, podrá disponer la evaluación de las que se hubieren presentado, sin necesidad de realizar una prórroga, debiendo en todo los casos asegurar al Estado Paraguayo las mejores condiciones de contratación, o prorrogar la fecha de entrega y apertura de ofertas, según lo estipulado en las Resoluciones DNCP N° 522/2015, 805/2009 y el Art. 34 de la Ley 2.051/03 "De Contrataciones Públicas"

Atención: *Lic. Marcos Daniel Sosa.-*

Dirección: *Juan Bautista Alberdi Nº 972 c/ Manduvira.-*
Número del Piso/Oficina: *Unidad Operativa de Contrataciones*
Ciudad: *Asunción, Paraguay*
Código postal: *N/A*
La fecha límite para presentar las ofertas es:
Fecha: *04/09/2017*
Hora: *09:00 horas.*

PRESIDENCIA DE LA REPÚBLICA · AUDITORÍA GENERAL DEL PODER EJECUTIVO · Unidad Operativa de Contrataciones

18. La apertura de las ofertas tendrá lugar en:
Dirección: *Juan Bautista Alberdi Nº 972 c/ Manduvira.-*
Número del Piso/Oficina: *Unidad Operativa de Contrataciones*
Ciudad: *Asunción, Paraguay*
Fecha: *04/09/2017*
Hora: *09:15 horas.*

20._Para la evaluación y comparación de las ofertas, la Convocante utilizará los siguientes criterios: .....

c) Capacidad financiera:
Con el objetivo de calificar la situación financiera del oferente, se considerarán los siguientes índices:
- **Ratio de Liquidez:** activo corriente / pasivo corriente
  Deberá ser igual o mayor que 1, en promedio, en los 2 (dos) años 2015 y 2016.
- **Endeudamiento:** pasivo total / activo total
  No deberá ser mayor a 0,80 en promedio, en los 2 (dos) años 2015 y 2016.
- **Rentabilidad:** Porcentaje de utilidad después de impuestos o pérdida con respecto al Capital

El promedio en los 2 (dos) años 2015 y 2016, no deberá ser negativo.

d) Capacidad técnica:
- Catálogos, documentos técnicos o folletos que demuestre que el bien ofertado cumple con las especificaciones técnicas establecidas.
- El oferente deberá contar como mínimo con 2 (dos) técnicos certificados en la herramienta. Para demostrar deberá adjuntar a su oferta copias autenticadas de los certificados correspondientes **(para el ítem Nº 1).**

31. La convocante podrá aceptar la garantía de cumplimiento de contrato en forma de declaración jurada. SI. Conforme al Formulario N° 3. La garantía deberá extenderse por todo el periodo de ejecución del contrato más 30 días posteriores a la vigencia del mismo.-

ENMIENDA 2:

La Convocante establece modificar la Carta de Invitación, en el Anexo C – Especificaciones Técnicas, quedando como se detalla a continuación:

1- **Especificaciones Técnicas**

ÍTEM Nº 1:
Descripción: Licencias de software antivirus.-
Duración de la licencia: 2 años
Cantidad: 65 (sesenta y cinco) unidades
Especificaciones Técnicas Requeridas del Producto
- Acceso a la consola vía WEB (HTTPS) o MMC;
- Capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la contraseña de remoción del actual antivirus;
- Capacidad de instalar remotamente la solución de antivirus en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory;
- Capacidad de gestionar estaciones de trabajo y servidores de archivos (tanto Windows como Linux y Mac) protegidos por la solución antivirus;

- Métodos de detección basados en: Firmas, Heurística, asistido por Nube de seguridad del proveedor;
- La solución deberá contar con tecnologías de detección proactiva de amenazas basadas en la nube del mismo fabricante;
- Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto;
- Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas;
- Capacidad de hacer distribución remota de cualquier software por la estructura de gerenciamiento de antivirus para que sea instalado en las máquinas clientes;
- Capacidad de desinstalar remotamente cualquier software instalado en las máquinas clientes;
- Capacidad de importar la estructura de Active Directory para encontrar máquinas;
- Debe tener soporte total al protocolo IPv6;
- Capacidad de monitorear diferentes subredes con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección;
- Capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente;
- Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado;
- Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos;
- Proporciona las siguientes informaciones de las computadoras:
  - Si el antivirus está instalado;
  - Si el antivirus ha iniciado;
  - Si el antivirus está actualizado;
  - Minutos/horas desde la última conexión de la máquina con el servidor administrativo;
  - Minutos/horas desde la última actualización de vacunas
  - Fecha y horario de la última verificación ejecutada en la máquina;
  - Versión del antivirus instalado en la máquina;
  - Si es necesario reiniciar la computadora para aplicar cambios;
  - Cantidad de virus encontrados (contador) en la máquina;
  - Nombre de la computadora;
  - Fecha y horario de la última actualización de vacunas;
  - Sistema operativo con Service Pack;
  - Dirección IP;
  - Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido.
  - Actualizaciones de Windows Update instaladas
  - Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD
  - Vulnerabilidades de aplicativos instalados en la máquina
- Permite bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no consiga modificarlas;
- Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet;

PRESIDENCIA DE LA REPÚBLICA · AUDITORÍA GENERAL DEL PODER EJECUTIVO · Unidad Operativa de Contrataciones

- Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes;
- Capacidad de interrelacionar servidores de administración en estructura de jerarquía para obtener informes sobre toda la estructura de antivirus;
- Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos;
- Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML.
- Capacidad de generar traps SNMP para monitoreo de eventos;
- Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento;
- Debe tener compatibilidad con Microsoft NAP, cuando se instale en Windows 2008 Server;
- **Capacidad de conectar máquinas vía Wake on Lan para realización de tareas (barrido, actualización, instalación).**
- Capacidad de habilitar automáticamente una política en caso de que ocurra una epidemia en la red (basado en cantidad de virus encontrados en determinado intervalo de tiempo);
- Capacidad de realizar actualización incremental de vacunas en las computadoras clientes;
- Capacidad de reportar vulnerabilidades de software presentes en las computadoras.
- Capacidad de realizar inventario de hardware de todas las máquinas clientes;
- Capacidad de realizar inventario de aplicativos de todas las máquinas clientes;
- Capacidad de diferenciar máquinas virtuales de máquinas físicas;
- **Estaciones Windows**:
  - **Antivirus de archivos residente (antispyware, antitroyano, antimalware) que verifique cualquier archivo creado, accedido o modificado;**
  - Antivirus de web (módulo para verificación de sitios y downloads contra virus)
  - Antivirus de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos)
  - Firewall con IDS
  - Autoprotección (contra ataques a los servicios/procesos del antivirus)
  - Control de dispositivos externos
  - Control de ejecución de aplicativos
  - Control de vulnerabilidades de Windows y de los aplicativos instalados
  - Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;
  - Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, para que cualquier objeto detectado con el resultado elegido sea ignorado;
  - Capacidad de agregar aplicativos a una lista de "aplicativos confiables", donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas;
  - Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks);
  - Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
  - Capacidad de verificar solamente archivos nuevos y modificados;
  - Capacidad de verificar objetos usando heurística;
  - Capacidad de agendar una pausa en la verificación;

PRESIDENCIA DE LA REPÚBLICA · AUDITORÍA GENERAL DEL PODER EJECUTIVO · Unidad Operativa de Contrataciones

- Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo;
- Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.
- Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL);
- Capacidad de verificar enlaces introducidos en correos electrónicos contra phishing;
- Capacidad de verificar tráfico SSL en los browsers: Internet Explorer, Edge, Chrome, Firefox y Opera;
- Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística;
- Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador.
- **Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script), usando heurísticas;**
- Capacidad de modificar las puertas monitoreadas por los módulos de web y correo electrónico;
- Posibilidad de agregar sitios de la web en una lista de exclusión, donde no serán verificados por el antivirus de web.
- Debe contar con módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas. Tales registros de secuencias deben ser actualizados conjuntamente con las vacunas.
- Debe contar con módulo que analice cada macro de VBA ejecutado, buscando señales de actividad maliciosa.
- Debe contar con módulo que analice cualquier intento de edición, exclusión o grabación del registro, de forma que sea posible elegir claves específicas para ser monitoreadas y/o bloqueadas.
- Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas.
- Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica;
- Debe tener módulo IDS (Intrusion Detection System) para protección contra portscans y exploración de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas.
- El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
  - Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;
  - Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.
- Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:
  - Discos de almacenamiento locales
  - Almacenamiento extraíble
  - CD/DVD
  - Modems
  - Lectores de smart card
  - Wi-Fi
  - Adaptadores de red externos

PRESIDENCIA DE LA REPÚBLICA • AUDITORÍA GENERAL DEL PODER EJECUTIVO • Unidad Operativa de Contrataciones

- Dispositivos MP3 o smartphones
- Dispositivos Bluetooth

- Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario.
- Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario.
- Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento.
- Capacidad de configurar nuevos dispositivos por Class ID/Hardware ID
- **Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gerenciador de download, juegos, aplicación de acceso remoto).**
- Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo.
- Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.
- Capacidad de, en caso de que la computadora cliente salga de la red corporativa, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.

- **Servidores Windows**:
  - **Antivirus de archivos residente (antispyware, antitroyano, antimalware) que verifique cualquier archivo creado, accedido o modificado;**
  - Autoprotección contra ataques a los servicios/procesos del antivirus;
  - La solución deberá contar con protección Anti-Ransonware que actué de forma proactiva ante un proceso de cifrado en las carpetas de red compartidas producido por un equipo remoto;
  - El modulo Anti-Ransonware debe permitir la definición granular de las carpetas a proteger;
  - Firewall con IDS;
  - Control de vulnerabilidades de Windows y de los aplicativos instalados;
  - Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones:
    - Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
    - Gerenciamiento de tarea (crear o excluir tareas de verificación)
    - Lectura de configuraciones
    - Modificación de configuraciones
    - Gerenciamiento de respaldo y cuarentena
    - Visualización de informes
    - Gerenciamiento de informes
    - Gerenciamiento de claves de licencia
    - Gerenciamiento de permisos (agregar/excluir permisos superiores)

    El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
    - Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;
    - Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados.

- **Capacidad de reanudar automáticamente tareas de verificación que hayan sido interrumpidas por anormalidades (corte de energía, errores)**
- Capacidad de automáticamente pausar y no iniciar tareas agendadas en caso de que el servidor esté funcionando con fuente ininterrumpida de energía (uninterruptible power supply – UPS)
- En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software;
- Capacidad de configurar niveles de verificación diferentes para cada carpeta, grupo de carpetas o archivos del servidor.
- Capacidad de bloquear acceso al servidor de máquinas infectadas y cuando una máquina intenta grabar un archivo infectado en el servidor.
- Capacidad de crear una lista de máquinas que nunca serán bloqueadas aunque sean infectadas.
- Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;
- Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: "Win32.Trojan.banker") para que cualquier objeto detectado con el resultado elegido sea ignorado;
- Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
- Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
- Capacidad de verificar solamente archivos nuevos y modificados;
- **Capacidad de elegir qué tipo de objeto compuesto será verificado (ej.: archivos comprimidos, archivos auto descompresores, .PST, archivos compactados por compactadores binarios)**
- Capacidad de verificar objetos usando heurística;
- Capacidad de configurar diferentes acciones para diferentes tipos de amenazas;
- Capacidad de agendar una pausa en la verificación;
- Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo;
- Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.
- Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán
- Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena
- Debe contar con módulo que analice cada script ejecutado, buscando señales de actividad maliciosa.

- **Servidores Linux:**
  - **Antivirus de archivos residente (antispyware, antitroyano, antimalware) que verifique cualquier archivo creado, accedido o modificado;**

    Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones:
    - Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
    - Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes;

- Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;
- Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.
- En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros software;
- Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
- Capacidad de verificar objetos usando heurística;
- Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán
- Posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena

Requerimientos al Oferente

- La Empresa adjudicada deberá implementar el software y migrar a las últimas versiones e implementar todos los módulos de la herramienta en todo el parque de la institución.
- Capacitación oficial de la herramienta a las personas de la Dirección General de Tecnologías de la Información y Comunicación, dictada por técnicos certificados por la marca, la cual debe incluir derecho a examen de certificación. En dicha capacitación se expedirá certificados a los participantes.
- Soporte técnico incluido durante todo el periodo de licenciamiento.
- Cantidad de ticket ilimitado, asistencia en sitio sin costo durante todo el periodo de licenciamiento.
- Presentar autorización del fabricante.
- La convocante podrá solicitar si cree necesario a los oferentes una demostración del manejo y despliegue de la herramienta.

ÍTEMS Nº 2:
Descripción: Licencias de software Microsoft Office 2016 Standard OLP GOV.-
Duración de la licencia: Permanente
Cantidad: 25(veinticinco) unidades.-

ÍTEMS Nº 3:
Descripción: Software para Backup y replicación para ambientes virtualizados con VMWARE.
Duración de la licencia: Permanente
Cantidad: 1 (una) unidad.-

Especificaciones Técnicas	Características
Marca/Fabricante	Indicar exactamente de manera a comprobar en el catálogo on-line del fabricante
Modelo/Producto	Indicar exactamente de manera a comprobar en el catálogo on-line del fabricante
Origen/Procedencia	Indicar
Cantidad	1 (una) Unidad (capacidad de 2 sockets)
Licencia	Licenciamiento de uso perpetuo, con servicio de mantenimiento y actualización del producto ofrecidos por el término mínimo de 1 año.
Requisitos del Oferente	El oferente deberá presentar la carta de autorización del fabricante y/o distribuidor autorizado de la marca. La oferta deberá incluir Instalación, configuración y capacitación de la solución.
	El oferente deberá contar con un mínimo de 2 técnicos certificados en la marca. Presentar copias de certificados actualizados.

Especificaciones Técnicas	Características
Funcionalidades	La solución deberá incluir funcionalidades de respaldo (backup) y replicación integradas en una única solución; incluyendo vuelta atrás (rollback) de réplicas y replicación desde y hacia la infraestructura virtualizada.
	La solución no deberá necesitar de la instalación de agentes para poder realizar sus tareas de respaldo, recuperación y replicación de máquinas virtuales.
	Deberá poder realizar respaldos sin detener las máquinas virtuales, y sin generar una merma en su performance, facilitando las tareas de respaldo (backup) y migraciones en conjunto.
	Deberá ser capaz de comprender las máquinas virtuales como objetos del entorno virtual y respaldar las configuraciones de las mismas, al margen de los datos propios de las maquinas.
	Deberá ser capaz de respaldar de forma indistinta una máquina virtual completa o discos virtuales específicos de una máquina virtual.
	Deberá proveer una herramienta de gestión de archivos para los administradores de máquinas virtuales en la consola del operador
	Deberá integrarse en forma extensiva, con las APIs de los fabricantes de infraestructura virtualizada, para la protección de datos.
	Deberá poder realizar respaldos (backup) incrementales ultra rápidos aprovechando la tecnología de seguimiento de bloques de disco modificados (changed block tracking) reduciendo al mínimo el tiempo de respaldo (backup) y posibilitando un respaldo (backup) y una replicación más frecuente. De este modo logrando lo establecido respecto de la merma de performance.
	La solución deberá ofrecer múltiples estrategias y opciones de transporte de datos para las tareas de respaldo (backup) a saber:
	- Directamente a través de Storage Area Network (SAN).
	- Directamente desde el storage a través del Hypervisor I/O (Virtual Appliance).
	- Mediante el uso de la red local (LAN).
	- Directamente de instantánea, con al menos un fabricante de sistemas de almacenamiento
	Deberá poder mantener un respaldo (backup) completo sintético eliminando así la necesidad de realizar respaldo (backup) completos (full) periódicos ya que proporcionará un respaldo (backup) incremental permanente con lo que se permita ahorrar tiempo y espacio.
	Deberá contar con la tecnología de deduplicación para lograr un ahorro de espacio de almacenamiento para los respaldo (backup).
	Deberá proveer una estrategia de recuperación rápida que permita proveer/devolver el servicio a los usuarios casi inmediatamente y en forma sencilla. Dicha estrategia debe consistir en el inicio y encendido de la máquina virtual, que haya fallado, directamente desde el archivo de respaldo (backup) en el almacenamiento habitual del respaldo (backup).
	La recuperación instantánea de las máquinas virtuales, deberá permitir más de una máquina virtual y/o punto de restauración en simultáneo para la disponibilidad del punto de recuperación funcional, permitiendo así, tener múltiples puntos en el tiempo de una o más máquinas virtuales funcionando.

Especificaciones Técnicas	Características
Funcionalidades	Posterior a una recuperación rápida, se deberá poder realizar una restauración total sin interrupciones del servicio. La herramienta debe asegurar que el trabajo realizado por los usuarios no estará afectado al migrar sus máquinas virtuales desde el respaldo (backup) hasta el almacenamiento de producción.
	Deberá poseer una opción de recuperación instantánea de archivos que se encuentren dentro de los respaldos (backup) y replicaciones de las máquinas virtuales. Lo que debe permitir acceder a los contenidos de los discos virtuales de dichas máquinas sin necesidad de recuperar el respaldo (backup) completo y reiniciar desde el mismo la máquina virtual.
	Deberá incluir un asistente para la recuperación instantánea a nivel de archivos en los sistemas de archivos más utilizados de Windows y Linux.
	Deberá asegurar la consistencia de aplicaciones transaccionales en forma automática por medio de la Integración con Microsoft VSS, dentro de sistemas operativos Windows.
	Deberá poder realizar notificaciones por correo, SNMP o a través de los atributos de la máquina virtual del resultado de la ejecución de sus trabajos.
	Se deberá poder recuperar a nivel de objetos de cualquier aplicación virtualizada, en cualquier sistema operativo, utilizando las herramientas de gestión de aplicaciones existentes.
	Deberá incluir herramientas de fácil recuperación guiada, mediante la cual los administradores de servidores de correo, puedan recuperar objetos individuales, tales como correos electrónicos y contactos, sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.
	Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de servicio de directorio, tales como, Microsoft Active Directory, pueden utilizar para recuperar objetos individuales, tales como usuarios, grupos, directivas de grupos (GPO), registros de DNS, particiones de configuración. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma.
	Deberá incluir herramientas de fácil recuperación guiada mediante el cual los administradores de servidores de bases de datos, puedan recuperar objetos individuales, tales como tablas y registros. Sin necesidad de recuperar los archivos de la máquina virtual como un todo y reiniciar la misma
	Deberá poder ofrecer confiabilidad en un 100% en el inicio correcto de todas sus máquinas virtuales respaldadas y en el funcionamiento del rol que cumple dichas máquinas virtuales (DNS Server, DomainController, Mail Server, Database Server, Web Server,) al momento de la recuperación.
	Deberá poder crear una copia de trabajo del entorno de producción de cualquier estado anterior para la resolución de problemas, pruebas de procedimientos, capacitación, etc. ejecutando una o varias máquinas virtuales desde el archivo de respaldo (backup) en un entorno aislado, sin necesidad de más espacio de almacenamiento y sin modificar el respaldo (backup).
	Deberá ofrecer el archivado en cinta, soportando VTL (Virtual Tape Libraries), biblioteca de cintas y drives independientes.
	Deberá ofrecer Trabajos de Copia de Backup con implementación de políticas de retención.

PRESIDENCIA DE LA REPÚBLICA
AUDITORÍA GENERAL DEL PODER EJECUTIVO
Unidad Operativa de Contrataciones

Especificaciones Técnicas	Características
Funcionalidades	No deberá requerir hardware específico para alcanzar la de-duplicación y compresión de la información fuera de los requerimientos estándar de cualquier software, y específicos para el caso.
	No deberá requerir licencias independientes para las actividades de respaldo, recuperación y replicación.
	Deberá ser capaz de realizar replicas en otros sitios o infraestructuras desde los respaldos realizados.
	Es necesario que ofrezca la posibilidad de regular de forma dinámica e parametrizable la exigencia sobre los sistemas respaldados, de forma tal, que se puedan definir umbrales de performance en discos para regular el impacto sobre la plataforma productiva.
	Deberá ofrecer la posibilidad de almacenar los respaldos de forma encriptada, así como asegurar el tránsito de la información bajo este esquema.
	Deberá disponer de funcionalidades integradas que permitan la selección de un destino de almacenamiento de respaldos que pueda estar alojado en un proveedor de servicios en la nube (BaaS).
	Deberá disponer de funcionalidades integradas que permitan la selección de un destino de replica que pueda estar alojado en un proveedor de servicios en la nube (DRaaS).
	Deberá disponer la funcionalidad de generar un almacenamiento de backup global, el cual puede incluir varios y distintos tipos de Storage, y apuntar los trabajos de backup al mismo como si fuese uno, permitiendo también el crecimiento a gran escala del mismo sin impacto sobre el ambiente de backup ya configurado.
	Deberá integrar una solución unificada de monitoreo de ambientes virtuales y respaldos de forma de poder co-relacionar ambas infraestructuras, las alarmas y reportes.
	Deberá ofrecer un conjunto de reportes capaces de presentar información de tipo:
	a. Reportes que permitan la planificación de la capacidad.
	b. Reportes que permitan la determinación de inefectividad en el uso de recursos.
	c. Reportes que faciliten la visibilidad de tendencias negativas y anomalías.
	d. Tableros de control claros, presentables e integrables en sitios web.
	Deberá poseer la capacidad de generar segregación de acceso según el perfil del usuario, al monitoreo de la infraestructura conectada a la plataforma.
	Capacidad de definir grupos de cintas magnéticas para ser utilizadas en una misma sesión de almacenamiento a cinta (Media Pool) para maximizar el rendimiento y velocidad de transferencia.
	Capacidad de procesar el envío de datos en múltiples unidades de cinta en paralelo para maximizar el ancho de banda y minimizar el tiempo de transferencia.
	Capacidad de procesar múltiples trabajos de envío a cinta en paralelo hacia múltiples unidades de cinta.
	Capacidad de lectura directa desde el sistema central de almacenamiento, cuando en un entorno de infraestructura VMWare, este se encuentre presentado a través de protocolo NFS, evitando así, el paso de la información a través de las interfaces de control del hipervisor.

ENMIENDA 3:

La Convocante establece modificar el punto 5 del Modelo de Contrato, quedando como se detalla a continuación

Nº de Orden	Nº de Ítem	Descripción del Bien	Marca	Procedencia	Unidad de Medida	Cantidad	Precio Unitario	Monto total
1	1	Licencias de software antivirus por 2 años. ***Conforme al detalle del Anexo C - Especificaciones Técnicas de los Bienes o Servicios a ser Adquiridos.***			Unidad	65		
2	2	Licencias de software Microsoft Office 2016 Standard OLP GOV. Con una duración de licencia permanente.-			Unidad	25		
3	3	Software para Backup y replicación para ambientes virtualizados con VMWARE. ***Conforme al detalle del Anexo C - Especificaciones Técnicas de los Bienes o Servicios a ser Adquiridos.***			Unidad	1		

Total: _____

El Proveedor se compromete a proveer los bienes a la Contratante y a subsanar los defectos de éstos de conformidad a las disposiciones del Contrato.

La Contratante se compromete a pagar al Proveedor como contrapartida del suministro de los bienes y servicios y la subsanación de sus defectos, el Precio del Contrato o las sumas que resulten pagaderas de conformidad con lo dispuesto en las Condiciones Especiales del Contrato (CEC).

Sin otro motivo en particular, me despido atentamente.

PRESIDENCIA DE LA REPÚBLICA · AUDITORÍA GENERAL DEL PODER EJECUTIVO · Unidad Operativa de Contrataciones

Lic. Marcos Daniel Sosa
Jefe de UOC
Auditoría General del Poder Ejecutivo