JUNTA DE RELACIONES LABORALES
DE LA AUTORIDAD DEL CANAL DE PANAMÁ
Tel (507) 321-0375 Fax (507) 321-0377

COTIZACIÓN - COMPRA POR URGENCIA

Para:	**De: GRETA HO**
Email:	**Página (s): 3**
Teléfono:	**Fecha: 10 de septiembre de 2021**

Agradecemos nos coticen lo siguiente:

RENGLÓN No.1

Implementación (suministro - instalación y configuración) de consola de antivirus para 30 agentes (28 dispositvos y 2 servidores).

Características	Descripción
Consola Centralizada de Administración	La solución debe contar con una consola de administración centralizada para administración de activos tecnológicos, políticas y reportaje.
Posicionamiento	La opción a evaluar debe estar posicionada como una solución de tipo “Next-Generation”
Agente Único	Todos los requerimientos de protección presentes en esta ficha técnica deben estar incorporados en un único módulo de despliegue que cuente con todas las funcionalidades requeridas y que no requiera diferentes ciclos de despliegue para la activación de cualesquiera de las funcionalidades necesarias.
Granularidad de Perfiles	La consola de administración debe proporcionar la capacidad de crear usuarios basados en nivel administrativo, administración por grupos y diferentes tipos de acceso basados en Roles.
Ciclos de Actualización	Es de vital importancia que la solución presentada no dependa de actualizaciones diarias de firmas y que reduzca en gran medida la dependencia de actualizaciones de cualquier índole para proporcionar un nivel de seguridad efectivo en las estaciones, de preferencia 1 o 2 actualizaciones por año.
Utilización de Recursos	La solución a evaluar debe garantizar un impacto bajo en el rendimiento de los sistemas, menos de un 10% de utilización de CPU preferiblemente.
Reportaje Avanzado	La consola de administración debe proveer información detallada sobre los incidentes de ataque, así como también del tipo de malware que intenta afectar la infraestructura tecnológica presentando características tales como: capacidad anti-sandboxing, detección de ambientes virtuales y de auto-ejecución del malware y capacidades de elevación de privilegios.
Sistemas Operativos Soportados	Debe soportar estaciones de trabajo de Windows XP SP3 hasta sus más recientes versiones, así como también servidores Windows Server 2003 en adelante. En adición, debe cubrir de igual forma plataformas Mac recientes y Linux (Redhat y Centos).
Motor de convicción No-Basado en Firmas (Signatures)	La solución debe poseer un motor de análisis y prevención que no dependa de actualizaciones diarias de firmas en las estaciones y servidores y que no depender del análisis tradicional de motores de antivirus (heurística y análisis de comportamiento).
Protección de Memoria Avanzada	Monitorear y controlar los incidentes en memoria a fin de proporcionar protección frente a violaciones de memoria tales como: Stack Pivot, Stack Protect, RAM Scraping, Malicious Payload, Process Injection (Incluyendo cualquier tipo de modificación o escritura en memoria) así como también intentos de elevacion de tipo LSASS Read ó Zero allocate.
Control de Scripts	Monitoreo, control y bloqueo de scripts en sus diferentes variedades, teniendo la posibilidad inclusive de controlar el uso de Powershell en las estaciones basado en políticas cubriendo Active Scripts / PowerShell / Macros entre otros.
Control de Aplicaciones	De forma integrada en la solución de endpoint, no como módulo separado o adicional, la solución debe proporcionar la capacidad de implementar esquemas de control de aplicaciones de tipo “Listas blancas” con la intención de proteger equipos de trabajo de diversa índole y también permitiendo crear ventanas de cambios conforme se requiera por la administración.
Capacidades de Sandboxing	Capacidad de someter archivos detectados como sospechosos o potencialmente maliciosos para análisis adicional, detalles, acciones y especificaciones sobre como el malware intenta afectar el sistema. Esta capacidad no debe estar limitada a cantidad de envíos y debe ser configurable acorde a las políticas de la institución.
Capacidad de Prevención	La solución debe poseer un alto nivel de prevención de ejecución de malware y fundamentar su modelo de protección en detener las amenazas antes de que se ejecuten en el sistema y no depender de análisis de comportamiento post-ejecución.

Monitoreo de Nuevos Archivos en el sistema	Debe tener la capacidad de monitorear y analizar de forma silenciosa, todos los archivos nuevos que se crean en una estación o servidor a fin de identificar si son maliciosos o no.
Auto-Protección de Servicios del Producto	Debe incorporar protección frente a los intentos de detención de servicios o procesos del AV por parte de usuarios.
Capacidad de Observar Inicio y Fin de los procesos ejecutados	La solución debe tener la característica de identificar la primera vez que identifica un nuevo proceso ejecutándose dentro de la estación y debe también informar la última vez que ha visto un proceso en ejecución.
Obtención de Muestras	La solución debe permitir a los administradores, configurar la misma para que sea capaz de recolectar muestras de malware o de archivos sospechosos identificados en las estaciones a fin de poder someter los mismos a servicios de inteligencia de amenazas de terceros o realizar análisis forense exhaustivo mediante otros canales de investigación. Dichas muestras deben poder ser recogidas del sistema en cuestión o ser centralizadas en la consola de administración.
Control de Dispositivos	La solución debe contar con la funcionalidad integrada en un mismo agente, de control de dispositivos de almacenamiento removible, pudiendo identificar eventos de conexión de los mismos, su comportamiento y la capacidad de crear directivas basadas en ID del Fabricante, ID del producto, Serial del dispositivo, entre otros
Integración con Plataformas SIEM	Debe proporcionar integración transparente con los más importantes fabricantes de soluciones de Administración y Correlación de eventos de seguridad, para proporcionar eventos e información acerca de todos los componentes de la solución.
Capacidad de Análisis Forense	La consola de administración, así como el agente, deben estar en la capacidad de recolectar, analizar y presentar información relevante para los equipos de seguridad de la información, a fin de que puedan fácilmente recuperar información para análisis forense identificando detalles, vectores de ataque de forma intuitiva y fácil.
Soporte Técnico	La solución a escoger debe contar con su respectivo plan de soporte 24/7 vía, Email, teléfono o Conexión Remota de soporte de parte del proveedor local.

RENGLÓN No.2

Actualización de Tecnologías de Backup para Junta Relaciones Laboral de la ACP

Términos de referencia para soluciones de software de respaldo

1. 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
2. La solución puede tener instalación de agentes como sin agentes para poder realizar sus tareas de respaldo, recuperación, replicación de máquinas virtuales y físicas
3. Deberá poder realizar respaldos sin detener las máquinas virtuales o físicas, y sin generar una merma en su rendimiento
4. La solución debe brindar respaldo, recuperación y replicación para sus cargas de trabajo críticas, lo que incluye: VMware, Nutanix, Google Cloud, Hyper-v, AWS, Microsoft Azure, Windows, Linux, Oracle Solaris, MAC, IBM AIX NAS, aplicaciones empresariales como SAP, Microsoft, Oracle
5. La solución debe ser sencilla, flexible y confiable para proteger sus cargas de trabajo físicas, virtuales, SaaS y en la nube.
6. Que el licenciamiento de la solución pueda ser portable a cualquier carga de trabajo en la premisa del cliente, nube privada o nube pública.
7. Que la solución sea compatible con almacenamiento S3 compatible y Archivado de datos frios.
8. Que la solución de respaldo tenga protección contra ransomware en repositorios Linux
9. Que la solución sea capaz de recuperar instantáneas para NAS, Microsoft SQL y Oracle
10. Que la solución sea compatible con servicios Baas y DRaaS
11. Que la solución pueda combinar todas las opciones de respaldo y replicación con monitoreo más análisis proactivo.
12. Que la solución tenga API para integraciones con diferentes marcas de almacenamiento avanzado.
13. La solución debe asegurar de que sus datos estén respaldados y sean recuperables de acuerdo a sus condiciones con diversas opciones de backup y recuperación granular.
14. Que la solución Consolide y amplíe sus repositorios de backup de forma inteligente
15. Que la solución Elija dónde guardar sus backups al seleccionar entre objetivos locales de más alto rendimiento (nivel de rendimiento), almacenamiento de objetos a largo plazo en la nube (nivel de capacidad) o necesidades de almacenamiento en frío al plazo más largo (nivel de archivo) con el fin de cubrir y automatizar sus necesidades de retención de datos y los objetivos de costos.
16. La solución debe estar listo para la recuperación de una manera segura y que cumpla las normas con un conjunto de herramientas integradas que le brinde recuperabilidad verificada, protección y restauraciones de seguridad, restauraciones planificadas compatibles con RPDG, sandbox virtual para hacer pruebas y más con el fin de verificar que sus backups estén listos.

17. La solución puede contar con La protección de datos continua que reduce los tiempos de inactividad y minimiza la pérdida de datos para sus cargas de trabajo críticas.
18. La solución debe brindar La protección de datos continua y brindar opciones de RTO y RPO ajustables con el fin de mantener sus capacidades de recuperación ante desastres.
19. La solución debe reducir el impacto en la red, el sistema y la carga de trabajo con backups directamente desde una snapshot basada en almacenamiento.
20. La solución debe crear backups con reconocimiento de aplicaciones con la tecnología para snapshots de almacenamiento.
21. La solución debe contar con Acciones de reparación y diagnóstico inteligente
22. La solución debe contar con Monitorización, informes y análisis
23. Que la solución pueda restaurar una unidad con errores o una partición
24. Que la solución Restaure archivos individuales en minutos.
25. Que la solución pueda hacer múltiples tareas de respaldo
26. Que la solución Respalde archivos y directorios específicos, incluyendo el soporte a atributos ampliados (xattr): no solo haga backup de datos desde sistemas de archivos que no están admitidos por el módulo de snapshot (como NSS, ZFS y otros) sino que además asegúrese de que todos los metadatos adicionales importantes estén seguros.
27. Que la solución restaure su sistema completo al mismo hardware o a uno diferente.

Requisitos

**Paz y Salvos Nacional (DGI) y de la Caja de Seguro Social vigentes

**Experiencia en clientes con más de 10 usuarios en desastres en data center o similitudes, en Panamá. (presentar mínimo 1 carta de referencia).

**La empresa ofertante debe tener más de 5 años activos en el Territorio Nacional y dedicados a las soluciones y servicios tecnología de la información (TI). (Presentar mínimo 1 carta de referencia).

**Experiencia mínima de 3 años en manejo y soporte de la marca en el territorio panameño. (presentar mínimo 1 carta de referencia).

**Certificación de mínimo 2 ingenieros en la solución ofertada en temas de instalación, configuración y soporte basados en Panamá.

**Carta del fabricante donde certifique que el proveedor es partner autorizado de la marca en desastres en data center o similitudes.

**Idoneidad de la junta técnica de ingeniería y arquitectura

**Entrega inmediata

Nota:

Para consultas y aclaraciones contactar al ingeniero Rolando Rodríguez al correo rrodriguez@juntalaboral-acp.com

Atentamente,

ESTA COMPRA SE ADJUDICARÁ POR RENGLÓN Y SEGÚN EL PRECIO MÁS BAJO SIEMPRE Y CUANDO CUMPLA CON LAS CARACTERISTICAS MÍNIMAS ESTABLECIDAS Y LOS REQUISITOS EXIGIDOS. La empresa que no entregue la documentación sobre las características del equipo propuesto no será considerada.

Las propuestas deberán ser enviadas por correo electrónico a compras@juntalaboral-acp.com, hasta la 1:00 p.m. del día lunes 13 de septiembre de 2021.

La cancelación al proveedor se hará a los treinta (30) días posteriores a la presentación del original de la factura y original de la orden de compra y los certificados de **Paz y Salvo Nacional y de la Caja de Seguro Social.**

En virtud del artículo 43 de la Ley Orgánica de la Autoridad del Canal de Panamá, la Junta de Relaciones Laborales de la Autoridad del Canal de Panamá está exenta del pago de todo tributo, impuesto, derecho, tasa, cargo o contribución, de carácter nacional o municipal.

LA PRESENTACIÓN DE PROPUESTA EQUIVALDRÁ A LA ACEPTACIÓN, SIN RESERVA NI CONDICIONES, DE LOS DOCUMENTOS, TÉRMINOS Y CONDICIONES ESTABLECIDAS.