JUNTA DE RELACIONES LABORALES
DE LA AUTORIDAD DEL CANAL DE PANAMÁ
Tel (507) 321-0375 Fax (507) 321-0377
compras@juntalaboral-acp.com

COTIZACIÓN

Para:	**De: COMPRAS**
Email:	**Página (s): 3**
Teléfono:	**Fecha: 26 de enero de 2022**

Agradecemos nos coticen lo siguiente:

RENGLÓN No.1

Implementación (suministro - instalación y configuración) de consola Antimalware basado en la nube para 42 agentes (40 dispositvos y 2 servidores). Por un termino de 2 años

Características	Descripción
Gestión de Seguridad en Todas las plataformas mediante	La solución debe contar con el uso de sistemas operativo, Windows, Mac y dispositivos móviles Andoid y IOS
Procesamiento	La opción para evaluar debe estar posicionada como una solución de tipo Nueva Generación (Next Generation)
Protección del dispositivo.	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.
Tipo de procesadores	Pentiun, AMD, INTEL en windowa
	Power Pc o Intel en Mac
Tipo de Memoria Ram	Memoria Ram mínima de 512 MB o superior y en servidores de 2gb o superior.
Utilización de Recursos.	La solución para evaluar debe garantizar un impacto bajo el rendimiento de los sistemas menos un 10% de Utilización de CPU
Zero Trust Agent	La solución debe contar con una autenticación con los permisos dentro o fuera de la red para la seguridad de la organización. Para los accesos a la información
Real time Endpoint Estatus	La solución brindara tiempo real de los equipos de conexión y desconexión a través de la consola de administración.
Capacitates 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.
Tipo de protección de antivirus y protección web.	La solución debe contar con sitios bloqueos de sitios web no deseados por medio de políticas en la consola
Protección Contra amenazas y seguridad web.	La solución debe contar con un cortafuegos que no permita ciertos tipos de tráfico en la red.
Protección a usuarios	La solución debe contar con un monitoreo del comportamiento que protege al usuario de modificaciones inusuales al sistema operativo o al software que este instalado
Control de Vulnerabilidades	La solución debe contar con un control de vulnerabilidad de los equipos de la organización para que se puedan validar los parches requeridos por red.
Panel de Vulnerabilidades	La Solución debe llevar un panel de vulnerabilidades con el fin de sacar informes mensuales de los equipos de la organización.
Control Escaneo Programados	La solución debe llevar un escaneo programado de toda la red de la organización para poder conllevar, los análisis preventivos y correctivos.
Control de Aplicaciones	La solución debe contar con un control de reputación web que ayude a evitar accesos a paginas maliciosas que presenten riesgos potenciales para la seguridad al comparar cualquier sitio malicioso mediante su base de datos de seguridad. Si el sitio web es seguro se agrega a una lista blanca para su aprobación.
Protección de Datos	La solución debe contar con una protección de datos
Prevención de Perdida de Datos	La solución debe contar con un control de dispositivos que limite el acceso a unidades de Usb u otros dispositivos conectados para evitar la pérdida de datos y bloquear amenazas.
Capacidad de Análisis Forense	La consola de administración como el agente deben estar en capacidad de recolectarr, analizar y presentar información relevante para los equipos de seguridad de la información para análisis forense identificando detalles, vectores de ataque de forma fácil.
Protección Dispositivos Moviles	La solución debe contar con una gestión y seguridad para dispositivos móviles.
Seguridad Dispositivos Moviles	La solución debe contar con la gestión de dispositivos móviles para Android y dispositivos IOS
Antivirus y Seguridad Web	La solución debe contar con protección avanzada contra ataques dirigidos y contra phishing selectivo.
Integración de Plataforma Siem	Debe proporcionar una integración transparente con lo más importante fabricantes de soluciones de Administración y correlación de eventos de seguridad para proporcionar eventos e información acerca de todos los componentes de la solución.

Se fija el 26/1/2022 a las 9: a.m.

Uso de Plataforma	La solución debe contar con una consola de administración en la nube.
	La solución debe contar con actualizaciones y parches automáticos mediante la nube.
	Su rango de falsos positivos debe estar dentro de los niveles aceptados por la industria y causar un nivel bajo de impacto en endpoint sin imortar su Sistema Operativo: Windows (Estaciones y servidores) OS, X, Linux etc.
	Debe ser de fácil manejo en los agentes de usuario final.
	La solución no debe depender de una amplia infraestructura on-premise para su administración y despliegue y debe ser de preferencia en la nube.
	La solución debe proporcionar todas las facilidades y beneficios de la nube como una alta disponibilidad y capas de seguridad.
Soporte	La solución debe contar con soporte 8x5 de fabrica en la nube.

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

El proponente favorecido entregará un Certificado con la informacion de las licencias de antivirus válido por 2 años

La empresa ofertante debe tener más de 5 años activos en el Territorio Nacional y dedicados a las soluciones y servicios de 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. En su defecto puede presentar certificación emitida por el representante legal de la empresa que indica que son partner de la marca propuesta.

El proponente favorecido debe entregar la certificación en ISO 9001-2015 del fabricante del software propuesto

Entrega inmediata

El proponente favorecido debe entregar tres (3) Certificaciones de usuario final de la marca

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

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 no será considerada.

Las propuestas deberán ser enviadas por correo electrónico a compras@juntalaboral-acp.com, hasta la 3:15 p.m. del día martes 1 de febrero de 2022.

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.

Se fija el 26/1/2022 a las 9: a.m.