ANEXO 1— ANEXO TÉCNICO

ADQUISICIÓN DE LICENCIAS DE ANTIVIRUS GRAVITYZONE BITDEFENDER PARA EL CUMPLIMIENTO DE LAS FUNCIONES MISIONALES DE LAS DISTINTAS DEPENDENCIAS DE LA GOBERNACIÓN DE BOLIVAR.

DESCRIPCIÓN DEL PROYECTO:
Se requiere la contratación conforme con las especificaciones establecidas a continuación:

ITEM	DESCRIPCION	UNIDAD DE MEDIDA	CANTIDAD
1	LICENCIA DE SOFTWARE DE ANTIVIRUS BITDEFENDER GRAVITYZONE (Cloud Bitdefender GravityZone Enterprise Security 250 - 499, 1 Año)	UNIDAD	400

CARACTERISTICAS TÉCNICAS MÍNIMAS EXIGIDAS

Son un conjunto de programas cuyo objetivo es detectar y eliminar los virus informáticos que se puedan presentar en la entidad.

A. Consola de administración que proporciona las funcionalidades básicas y avanzadas de gestión de productos.
B. Servicios de seguridad para equipos de escritorio físicos, portátiles y servidores.
C. Servicios de seguridad para entornos virtualizados que proporcionan un servicio antimalware creado especialmente para un entorno virtualizado.
D. Escalabilidad servicios de seguridad para dispositivos móviles que brindan seguridad y control de cumplimiento para teléfonos inteligentes y tabletas basados en sistemas operativos iOS y Android.
E. Servicios de seguridad para la introspección del hipervisor que proporciona la introspección en tiempo real de la memoria de la máquina virtual para prevenir e identificar ataques avanzados.
F. Servicios de seguridad para servidores que ofrecen opciones de antimalware, antispam, control de contenido y filtrado de archivos adjuntos

1. El paquete de instalación debe entregarse como un solo dispositivo virtual (imagenvirtual).
Las plataformas de virtualización soportadas deben ser:
a. VMware vSphere, VMware View, VMware Horizon suites
b. Citrix XenServer, Citrix XenApp, Citrix XenDesktop
c. Microsoft Hyper-V
d. Red Hat Enterprise Virtualization
e. Kernel-based Virtual Machine or KVM
f. Oracle VM
g. Nutanix

Se deben admitir otras plataformas de virtualización si se realiza una solicitud al desarrollador de productos antimalware.

2. El producto debe permitir la implementación centralizada de máquinas de escaneo dedicadas.
3. Para fines de escalabilidad, el producto debe permitir que cualquier componente o servicio se instale de forma independiente o en un método agrupado.
4. Para propósitos de escalabilidad, el producto debe tener componentes dedicados para servicios de base de datos, servicios de comunicación, actualización y servicios web.
5. Para alta disponibilidad y balanceo de carga, el producto debe incluir un módulo dedicado de balanceador de carga disponible.
6. Licencia flexible (clave separada para cada servicio de seguridad que permite un número diferente de objetos con licencia y fechas de vencimiento diferentes, historial de todas las claves ingresadas) o licencia única que puede administrar todos los servicios de seguridad.
7. Actualización con un clic: un clic para actualizar todos los componentes de la consola de administración, sin depender de su orden de instalación ni de ningún otro requisito.
8. Actualizaciones a pedido que permitirán a los administradores elegir qué paquetes de servicios de seguridad se actualizarán para ahorrar ancho de banda.
9. Debería usar una base de datos no relacional / no SQL, sin requerir ninguna clave de licencia de terceros para implementaciones mayores que un cierto número de puntos finales.

10. Las notificaciones deben mostrarse en el menú principal, con aspectos destacados de los elementos no leídos, con la capacidad de enviarlo por correo electrónico, alertando al administrador sobre problemas importantes: problemas de licencias, alertas de brotes de malware y / o máquinas desactualizadas.

11. Capacidad para agregar, eliminar, organizar, configurar y personalizar múltiples portlets de seguridad

12. Capacidad de soportar múltiples páginas con múltiples portlets de seguridad.

13. Capacidad para ofrecer información de seguridad en tiempo real con gráficos fáciles de leer.

14. Capacidad para configurar el destino de los informes, el fondo del tipo de informe de seguridad, el intervalo de tiempo para la información presentada y mostrada y el nombre del portlet.

15. Integración con Microsoft Active Directory, VMware vCenter, Citrix Xen para importar el inventario e información de estas plataformas.

16. Tiempo de sincronización configurable (en horas) con Microsoft Active Directory.

17. Integración con Microsoft Hyper-V, RedHat Linux Virtual Machine, Oracle VM, KVM y cualquier otra máquina virtual que se descubra a través del descubrimiento de la red.

18. Descubrimiento de redes para máquinas no integradas en Microsoft Active Directory, VMware v Center, Citrix XenServer, tanto para estaciones de trabajo físicas como virtuales y servidores.

19. Búsqueda en tiempo real, clasificación y filtrado por nombre, sistema operativo, dirección IP, FQDN o etiqueta.

20. Capacidades de implementación remota y desinstalación del producto antimalware existente.

21. Paquetes de instalación manual y configurable para el producto antimalware.

22. Capacidad para configurar y ejecutar tareas de escaneo remoto.

23. Capacidad para reiniciar remotamente un punto final.

24. Capacidad para ver la sección de resultados de tareas centralizada con información detallada de cada subtarea.

25. Capacidad para asignar pólizas en todos los niveles de gestión.

26. Capacidad para configurar la herencia de políticas y forzar la configuración de políticas.

27. Capacidad para ver las propiedades detalladas de los puntos finales administrados, como el nombre, IP, sistema operativo, grupo, política asignada, estado de las capas de protección, realzar investigación forense de los registros recopilados, resolución de problemas y el estado más reciente del malware, auditoria de seguridad, los últimos registros de análisis y los usuarios conectados al punto final.

28. Capacidad para aplicar políticas basadas en la ubicación y basadas en el usuario registrado.
29. Capacidad para aplicar varias políticas a un único punto final, pero solo una activa a la vez.
30. Capacidad para aplicar una política a un grupo de puntos finales.
31. Capacidad de permitir Perfiles para reglas de políticas.
32. Una plantilla única para cada servicio de seguridad. Cada servicio de seguridad tiene su plantilla de política configurable con opciones específicas para activar / desactivar y configurar funcionalidades como el análisis antimalware, las capacidades de la zona de pruebas en la nube, las opciones de aprendizaje automático, la introspección del hipervisor, el cortafuegos, el control de acceso a la red, la inclusión en la lista blanca de aplicaciones, la lista negra de aplicaciones y el acceso a la web. control, control de dispositivos, ubicación de dispositivos, aplicación de autenticación y acciones a tomar en caso de malware y dispositivos no compatibles detectados, como bloqueo remoto, desbloqueo, borrado, cifrado SD.
33. Gran cantidad de informes.
34. Fácil de usar desde una vista: resumen y detalles en la misma página, sección de resumen activo (filtra los detalles haciendo clic en la sección de resumen).
35. Programado, se puede enviar por correo a cualquier número de destinatarios (no es necesario tener también una cuenta en la consola).
36. Filtros para informes programados para recibir por correo únicamente información relevante para cada usuario.
37. Archivar con todas las instancias generadas de un informe programado.
38. Exportar resumen a archivo .pdf, detalles a archivo .csv.
39. Restauraciones remotas, con ubicación configurable y borrar.
40. Capacidad de centralizar la cuarentena para archivos infectados.
41. Capacidad de aplicar filtro para equipos y máquinas virtuales
42. Capacidad de aplicar filtro para servidores Exchange on-premise
43. Descargue archivos, disponibles solo para máquinas virtuales integradas con vShield o NSX.
44. Personalice la hora en que los archivos se almacenan en cuarentena hasta 90 días.
45. Administración basada en roles.
46. Múltiples tipos predefinidos: a. Administrador de Compañía: Configure los ajustes del Centro de control, gestionar las claves de licencia de los servicios de seguridad, administrar usuarios, administrar redes, ver y analizar datos, investigación avanzada. b. Administrador de red: Administrar usuarios, Administrar redes, Ver y analizar datos c. Analista de Seguridad: ver y analizar datos. 1. Lista de usuarios que se puede importar desde Microsoft Active Directory (la autenticación AD se usará para iniciar

sesión). 2. Configuración detallada de los derechos de destino administrativos, para seleccionar qué servicios y objetos puede administrar un usuario. Cierre de sesión automático para cualquier tipo de usuario para mayor seguridad con respecto a la información que se muestra en la consola de administración.
47. Registrar las acciones del usuario para su cumplimiento.
48. Registros detallados para cada acción del usuario.
49. Búsqueda compleja
50. El acceso a la consola de administración debe estar protegido (https).
51. La solución permite habilitar el acceso con MFA (Múltiple Factor de Autenticación)
52. El servidor web, desde la consola de administración central, debe permitir la importación de certificados digitales emitidos por una autoridad de certificación con licencia o por su propia organización. Importar certificados para que sea intuitivo y hecho desde la consola de administración central.
53. La gestión y la comunicación con dispositivos móviles (iOS) deben realizarse de forma segura, a través de certificados digitales. Estos certificados serán firmados por una Autoridad de Certificación autorizada o por su propia organización.
54. Le permite importar la cadena de certificados de PKI (infraestructura de clave pública).
55. Debe admitir claves de cifrado de certificado digital con una longitud mínima de 1024 bits.
56. Los certificados digitales, una vez importados, deben ser reemplazables en caso de que caduquen o sean revocados.
57. Los certificados aceptados en el proceso de importación deben estar en formato pfx o p12 y protegidos por una contraseña.
58. La solución debe ser capaz de generar certificados digitales por sí misma.
59. La solución debe poder mostrar en la consola central información sobre los certificados: nombre, autoridad de emisión, fecha de emisión y fecha de vencimiento de los certificados emitidos.
60. La solución debe permitir la prueba de nuevos kits o actualizaciones de productos en un entorno cerrado.
61. La solución permite recibir actualizaciones de manera prioritaria.
62. La solución debe tener la capacidad de decidir qué kitsse publicarán en la red.
63. La solución debe poder definir y aplicar diferentes políticas para los puntos finales críticos de producción y actualizarlos después de que se haya probado el nuevo paquete.
64. La solución debe poder desactivar la opción de clasificación.
65. La plataforma de ensayo debe entregarse como un dispositivo virtual.

66. El servidor de actualización puede actuar como una puerta de enlace para los datos.
67. La consola y la plataforma de pruebas deben poder descargar automáticamente nuevos kits.
68. La consola debe poder configurar el número máximo de kits que puede almacenar.
69. La opción de organización puede definir varios anillos de actualización para aplicar actualizaciones de productos.
70. La solución permite asignar un role de Relay a sus agentes con el fin de proveer actualizaciones de seguridad y productos a los demás agentes instalados en los puntos finales de la red.
71. La solución puede usar actualizaciones fuera de línea en una infraestructura aislada.
72. Las actualizaciones se pueden recuperar y transferir a través de USB HDD / USB Stick, File Server, FTP e instalarse en la infraestructura aislada.
73. La solución debe permitir a los administradores utilizar la llamada a la API.
74. La solución debe incluir métodos para administrar cuentas de usuario, configurar notificaciones, administrar grupos, carpetas y puntos finales, administrar políticas, generar informes a través de APIs.
75. La existencia de un único motor antimalware.
76. La solución debe proveer capacidades de protección para Windows, MacOS y Linux.
77. La solución debe proveer un único instalador para cada plataforma (por ejemplo un único instalador para sistemas operativos Windows, único instalador para Sistemas operativos MacOS, igual para Linux)
78. Para minimizar el consumo de recursos, los productos antimalware deben permitir la instalación de módulos personalizados (por ejemplo, la instalación del producto antimalware sin el módulo de control de acceso web o sin el módulo Firewall).

NOTA: la adquisición de los antivirus, deben ser cargados o vinculados a la consola (GravityZone Control Center) de administración existente de la entidad.

1. PRINCIPALES ACTIVIDADES POR EJECUTAR Y ALCANCE:
SE REQUIEREN LA ADQUISICIÓN DE LICENCIAS DE ANTIVIRUS GRAVITYZONE BITDEFENDER PARA EL CUMPLIMIENTO DE LAS FUNCIONES MISIONALES DE LAS DISTINTAS DEPENDENCIAS DE LA GOBERNACIÓN DE BOLIVAR.

Se requiere la siguiente adquisición:

- 400 licencias del antivirus Bitdefender GravityZone

LICENCIAS DE SOFTWARE DE ANTIVIRUS BITDEFENDER GRAVITYZONE.
(Cloud Bitdefender GravityZone Enterprise Security 250 - 499, 1 Año)

1. Cumplir de buena fe el objeto contratado.
2. Constituir las pólizas pactadas en el contrato.
3. Pagar los tributos que para tal efecto requiera la Ley 80/93 y la normatividad distrital, Departamental y nacional vigente.
4. Obrar con diligencia y el cuidado necesario en los asuntos que le asigne la supervisión del contrato.
5. Garantizar la calidad de los servicios contratados y responder por ellos, de conformidad con lo estipulado en el artículo 5º, numeral 4, de la Ley 80 de 1993.
6. Desarrollar las actividades señaladas por el supervisor del contrato.
7. Acreditar el aporte al Sistema de Seguridad Social (Pensión, Salud y ARL). Si es persona Jurídica debe adjuntar Certificación Firmada por el Representante Legal o revisor Fiscal en la que se especifique que la empresa cumplió con el pago de los aportes a seguridad social y Parafiscales. Si se trata de personas Naturales independientes sin empleados a su cargo, deberán acreditar con los documentos que correspondan que se encuentran al día con el pago de sus aportes al sistema de seguridad social. La base de Liquidación para acreditar los pagos debe corresponder al 40% del valor del contrato.
8. Asumir los gastos y riesgos que implica el desarrollo del contrato bajo su propia responsabilidad.
9. Disponer lo necesario para que el objeto del contrato se cumpla a cabalidad conforme las obligaciones derivadas del contrato.

OBLIGACIONES ESPECÍFICAS:

10. Realizar la entrega de las licencias de antivirus Bitdefender Gravityzone de conformidad con las especificaciones técnicas.
11. Proveer el acceso a los sistemas de Bitdefender Gravityzone para descargar los medios de instalación sobre todos los productos que aplique.
12. El contratista debe entregar un documento en donde se consignen las diferentes formas para recibir soportes sobre problemas relacionados con el licenciamiento adquirido y en especial los canales y formas de comunicación para recibir soporte especial.

13. El contratista será responsable de configurar y vincular las nuevas licencias adquiridas a la consola (GravityZone Control Center) de administración existente de la entidad, asegurando una integración efectiva con los sistemas preexistentes.
14. El contratista debe realizar la instalación y despliegue adecuados de los servicios de seguridad en los equipos de escritorio físicos, portátiles, servidores, así como en los entornos virtualizados y dispositivos móviles, según las necesidades de la entidad.
15. El contratista deberá garantizar la disponibilidad de actualizaciones regulares del software y proporcionar el mantenimiento necesario para asegurar el óptimo funcionamiento de las licencias adquiridas durante el período contractual.
16. El contratista debe ofrecer soporte técnico oportuno y eficiente para resolver cualquier problema o incidencia relacionada con el funcionamiento de las licencias de antivirus, incluyendo asistencia remota si es necesario.
17. El contratista deberá asegurar que las licencias adquiridas cumplan con las normativas de seguridad vigentes y proporcionen la protección necesaria contra amenazas informáticas para salvaguardar la información sensible de la entidad.
18. Se requiere que el contratista integre las licencias de antivirus con los sistemas y plataformas existentes de la entidad.
19. El contratista deberá proporcionar capacitación adecuada al personal de la entidad para el uso eficiente de las herramientas de administración y configuración de las licencias de antivirus, asegurando así su correcta operación y mantenimiento
20. El contratista se compromete a cumplir con todas estas obligaciones de manera diligente y eficaz, asegurando así el adecuado funcionamiento de las licencias de antivirus y el cumplimiento de los objetivos de seguridad de la Gobernación de Bolívar.

2. PLAZO PARA LA EJECUCIÓN DEL CONTRATO

El plazo previsto para la ejecución de las actividades que se deriven del presente proceso es el establecido en la sección 2.1 de los PLIEGOS DE CONDICIONES, el cual se contará a partir del cumplimiento de los requisitos para dar inicio a la ejecución del contrato.

3. FORMA DE PAGO

La forma de pago del contrato será la siguiente:

El DEPARTAMENTO DE BOLÍVAR, pagará al contratista el valor del contrato mediante un único pago, una vez el proveedor cumpla con la entrega del producto y la entidad pueda acceder a los equipos para verificar la instalación y constatar su adecuado

funcionamiento o uso, el pago debe estar precedido de presentación de la factura acompañada del certificado de recibido a satisfacción expedido por el supervisor del contrato. De igual manera se puede señalar que los pagos se realizaran de acuerdo con el PAC.

El Contratista para cada factura deberá presentar el pago de los impuestos cancelados de acuerdo a la liquidación de la **TESORERÍA DEPARTAMENTAL** y las pólizas debidamente aprobadas y vigentes de acuerdo a lo señalado en el Contrato.

La totalidad de la documentación requerida deberá ser presentada por el Contratista al Supervisor dentro de los cinco (05) días siguientes a la fecha de corte o según lo establecido contractualmente.

En forma previa a la autorización de cada pago el Contratista deberá acreditar el cumplimiento en los aportes relativos al Sistema de Seguridad Social Integral y de obligaciones parafiscales (salud, riesgos profesionales, pensiones, aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje) para lo cual debe tenerse en cuenta lo señalado en el artículo 50 de la Ley 789 de 2002 y artículo 23 de la ley 1150 de 2007. El **DEPARTAMENTO DE BOLÍVAR** no se responsabilizará por la demora en el pago al Contratista y/o Contratistas, cuando ella fuere provocada por encontrarse incompleta la documentación que sirva de Soporte para el trámite de las facturas y no se ajuste a cualquiera de las condiciones establecidas en el presente Contrato.

4. CONDICIONES PARTICULARES DEL PROYECTO

5. ACREDITACIÓN DE CONDICIÓN DE DISTRIBUIDOR AUTORIZADO

El Proponente, deberá acreditar mediante certificación expedida por el fabricante, importador directo o subsidiario del fabricante que se encuentra autorizado para ser distribuidor oficial o autorizado o representantes comerciales para Colombia de la marca, o marcas, que representen y oferte en el presente Proceso.

El Certificado deberá permitir validar como mínimo la siguiente información: (i) Marca de las licencias (ii) Fecha de expedición (iii) Fecha de autorización (iv) Razón social, o Casa Matriz, que brinda la autorización o condición de Distribuidor (v) Razón social, o persona a la cual se otorga la condición de Distribuidor Autorizado. (vi) El documento deberá encontrarse debidamente suscrito por la persona competente. (vii) Los

documentos y comunicaciones en un idioma distinto al castellano deben ser presentados en su lengua original junto con la traducción oficial al castellano.

En constancia, se firma en Barranquilla, a los 15 días del mes de julio de 2024.



CARLOS ALBEERTO COGOLLO ARISTIZABAL

PC STORE IT SAS