ANEXO 1— ANEXO TÉCNICO

1. OBJETO: "CONTRATAR LA RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER, CON ACTUALIZACION, SOPORTE, CAPACITACION Y ASISTENCIA TECNICA POR EL TERMINO DE UN AÑO, PARA LAS ESTACIONES DE TRABAJO Y SERVIDORES DE LA PLATAFORMA TECNOLOGICA DE LA GOBERNACION DE BOLIVAR", teniendo en cuenta las cantidades y especificaciones técnicas descritas.

2. ESPECIFICACIONES TÉCNICAS:

A continuación, se relacionan las condiciones técnicas para cumplir con el objeto del contrato, las que se constituyen en requisitos mínimos de orden técnico que debe ofertar cada proponente al momento de la presentación de su propuesta:

ITEM	DESCRIPCION	CANT.
1	**SUMINISTRO DE LICENCIAS DE ANTIVIRUS PARA WINDOWS** 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 (imagen virtual). 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.	800 licencias

	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 vCenter, 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 maquinas 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 kits se 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). 2. Requisitos del sistema: • Sistemas operativos para estaciones de trabajo: Windows 11, Windows 10, Windows 8.1, Windows 8, Windows 7 Service Pack 3. • Sistemas operativos de servidor: Windows Server 2022, Windows Server 2019 Core, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Small Business Server (SBS) 2008, Windows Server 2008 R2.	

3. Administración e instalación remota:

1. Antes de la instalación, el administrador puede personalizar los paquetes de instalación incluyendo solo los módulos deseados: análisis basado en el comportamiento, cifrado completo del disco, firewall, control de contenido, control de dispositivos, control de aplicaciones, administración de parches.
2. La instalación se puede realizar de varias formas:
    a. Al descargar el paquete antimalware directamente a la estación de trabajo donde se instalará.
    b. Mediante la instalación remota, directamente desde la consola web.
3. La instalación en máquinas desde una ubicación remota se realizará utilizando un cliente instalado existente en estas ubicaciones para minimizar el tráfico WAN.
4. La consola de administración informará el número de estaciones de trabajo que tienen el antimalware instalado y el número de estaciones de trabajo que están desprotegidas.
5. La consola de administración incluirá en los paneles / widgets configurables del panel de control.
6. La consola de administración incluirá información detallada sobre las estaciones de trabajo / servidores: nombre, IP, sistema operativo, módulos instalados, política aplicada, información de actualización, etc.
7. La consola de administración permitirá al administrador enviar una política para configurar todo el producto antimalware, tanto para estaciones de trabajo como para servidores.
8. La consola de administración permitirá tres tipos de cuentas, Administrador de compañía, administrador de red y auditor de seguridad, que pueden asignarse a qué grupos de usuarios pueden cambiar la configuración o generar informes.
9. La consola de administración incluirá una sección de registro donde se mencionarán todas las acciones, con información detallada: iniciar sesión, editar, crear, cerrar sesión, mover, etc.
10. La consola de administración permitirá la posibilidad de crear un paquete único, utilizado para sistemas operativos de 32 bits y de 64 bits, Windows, MAC y Linux.
11. La consola de administración permitirá al administrador crear grupos o subgrupos para la administración de estaciones de trabajo.
12. Tenga la posibilidad de seleccionar qué cliente descubrirá las otras computadoras en la red.

Las principales características y funcionalidades del antimalware y el módulo antispyware:

1. El administrador de la solución puede configurar el escaneo automático en tiempo real para que no analice archivos o archivos con un tamaño mayor que "x" MB.
2. El escaneo automático en tiempo real puede admitir escanear archivos con hasta 16 niveles de profundidad.
3. Escaneo basado en firmas.
4. Escaneo heurístico del comportamiento y monitoreo de procesos.
5. Escaneo en la nube y tecnología de aprendizaje automático.
6. Tecnología anti-ransomware y anti-exploit para firmas o familias conocidas
7. Tecnologías de Hyperdetect para APT, Ransomware, Exploits Avanzados para ataques de día 0 o desconocidos.
8. Capacidad para detectar ataques sin archivos, incluidos aquellos que utilizan herramientas legítimas del sistema operativo, como Powershell o intérpretes de scripts. La solución no debe bloquear globalmente los scripts para lograr esto.
9. Capacidad de realizar mitigación de ransomware, permitiendo reestablecer archivos afectados a través de los ajustes de políticas definidos por el administrador; la mitigación de ransomware de tener la capacidad de ajustar la recuperación de los archivos ante un incidente de forma manual o automática.
10. Capa de seguridad adicional de próxima generación, basada en heurísticas

agresivas y tecnología de aprendizaje automático, para detectar y bloquear la nueva generación de ataques avanzados o dirigidos y malware sofisticado antes de la ejecución. Debe proporcionar:

a. Clasificación de los tipos de ataque.
b. Posibilidad de informar únicamente sobre amenazas detectadas, sin bloquearlas.
c. Capacidad para ajustar la agresividad de detección para cada categoría de ataque, con opciones para tomar medidas en detecciones de mayor confianza y también informar todas las demás detecciones de menor confianza. Al menos 3 niveles de detección estarán disponibles.
d. Capacidad para realizar diferentes acciones sobre los archivos detectados y las amenazas basadas en la red.

11. Escaneo bajo demanda y en acceso de cualquier medio de almacenamiento de información (CD, discos duros externos, disco compartido). Además, el proceso de exploración se puede detener si los dispositivos de medios de almacenamiento contienen información de más de "x" MB.
12. Escaneo automático de correos electrónicos a nivel de estación de trabajo, independientemente del cliente de correo electrónico, para los protocolos SMTP y POP3.
13. Configuración de las rutas a escanear, hasta el nivel de archivo.
14. La solución debe proporcionar Exclusiones incorporadas para roles de servidor de Microsoft (DNS, DHCP, AD, Exchange, Sharepoint).
15. El producto antimalware permitirá definir la lista de exclusión del análisis, tanto para el análisis "en acceso" como para el análisis "a pedido", para ciertas carpetas, discos, archivos, extensiones o procesos.
16. Con una base de datos completa de firmas de spyware y detección heurística de estos programas, el producto tendrá que ofrecer protección antispyware.
17. Para no sobrecargar los recursos del sistema, el producto antimalware debe contener un solo motor de análisis. Podrá ejecutar exploraciones programadas con baja prioridad y puede apagarse automáticamente después de explorar la estación de trabajo.
18. Para una mayor protección, antimalware debe tener 4 tipos de detección: basada en firmas, basada en heurísticas, procesos de monitoreo continuo y escaneo en la nube.
19. Para una mayor protección, antimalware debería poder escanear HTTP y SSL también.
20. Para una mejor administración del antimalware instalado en las estaciones de trabajo, el producto incluirá la opción de establecer una contraseña para la protección de la desinstalación.
21. Para la seguridad del usuario, el cliente incluirá un módulo antiphishing que tendrá la opción de verificar los enlaces buscados con los motores de búsqueda (Asesor de búsqueda).
22. La aplicación antimalware debería ofrecer acceso para el sistema operativo Linux.

5. Firewall:

1. El módulo se puede instalar / desinstalar de acuerdo con las preferencias del administrador.

6. Cuarentena:

1. El producto antimalware debe permitir el envío automático de los archivos en cuarentena al laboratorio de virus.
2. El envío de los archivos en cuarentena se realizará automáticamente en un intervalo de tiempo predefinido (número de horas) establecido por el administrador.
3. El producto antimalware debe permitir la eliminación automática de archivos en

cuarentena más antiguos que un período determinado, sin ocupar espacio de almacenamiento innecesario.
4. La capacidad de mover un archivo de la cuarentena a su ubicación original.
5. Cuarentena centralizada. La capacidad de recopilar de forma segura todos los archivos en cuarentena desde puntos finales protegidos a una ubicación única para una investigación más profunda.
6. La cuarentena permitirá que los objetos se escaneen después de cada actualización de la firma.
7. El producto antimalware debe poder guardar una copia de un archivo de malware y enviarlo a cuarentena antes de realizar acciones de Eliminar o Desinfectar.

Protección de datos:

1. Permite el bloqueo de datos confidenciales (tarjeta de identificación personal, cuenta bancaria, etc.) tanto para HTTP como para SMTP, mediante la creación de reglas específicas.

7. Control de Usuario:

1. El producto habrá integrado un módulo de control de usuario con las siguientes características:
   a. Bloqueo del acceso a Internet para clientes específicos o grupos de clientes.
   b. Bloqueando el acceso a ciertas aplicaciones.
   c. Bloqueando el acceso a internet por ciertos periodos de tiempo.
   d. Bloqueo de páginas web que contengan determinadas palabras clave.
   e. Permitiendo el acceso a páginas web específicas especificadas por el administrador.
   f. Restringir el acceso a ciertos sitios web por algunas categorías predeterminadas (por ejemplo, citas en línea, violencia, etc.).

8. Control de aplicación e inventario:

1. Capacidad para descubrir aplicaciones y procesos en ejecución y organizarlos en grupos.
2. Organice y busque aplicaciones y procesos por nombre, versión, editor / autor, etc.
3. Permitir o negar que un proceso comience.
4. Autorizar una aplicación basada en un hash.
5. Autorizar una solicitud basada en un certificado.
6. Capacidad para aplicar reglas a procesos secundarios generados, subprocesos.
7. El módulo puede ejecutarse en modo de prueba e informar la aplicación, pero no el bloque.
8. El módulo puede ejecutarse en modo de producción y puede bloquear todas las aplicaciones desconocidas.
9. Excluir automáticamente los procesos del sistema operativo de Microsoft.

9. Control de dispositivos:

1. Prevenga las fugas de datos confidenciales y las infecciones de malware a través de dispositivos conectados.
2. Aplique reglas de bloqueo y exclusiones a través de políticas a una amplia gama de dispositivos y tipos.
3. Enviará información como el nombre del dispositivo, ID de clase, fecha y hora de conexión.
4. Tenga tipos predefinidos de dispositivos como: CDROM, dispositivos de imagen, unidades de cinta, puertos COM / LPT, incursión SCSI, impresoras, NIC,

almacenamiento interno y externo, etc.

5. Admite diferentes configuraciones y privilegios como Permitido, Bloqueado o Personalizado
6. Admite el modo de solo lectura para dispositivos de almacenamiento.
7. Capacidad para bloquear solo el USB y permitir que se utilicen todos los demás puertos.
8. Permitir la configuración de exclusiones para diferentes tipos de dispositivos.
9. Soporte para definir exclusiones de dispositivos:
    a. Por ID de producto
    b. Por ID de dispositivo, ID de hardware
10. Habilidad para descubrir dispositivos.

10. Análisis automático de Sandbox de archivos sospechosos:

1. La solución debe tener la capacidad de realizar un análisis en profundidad de los archivos sospechosos.
2. La solución debe tener la capacidad de enviar archivos de forma automática o manual a los servidores de sandbox.
3. La solución puede configurarse para permitir que los usuarios accedan a los objetos enviados o bloquearlos hasta que se devuelva el análisis.
4. La solución debe permitir diferentes acciones de remediación si un archivo enviado es una amenaza.
5. La solución debe tener la capacidad de usar un servidor proxy para el tráfico de la zona de pruebas.
6. La solución debe tener la capacidad de detonar archivos individualmente o en grupo.
7. La solución ofrece un informe detallado sobre los archivos enviados.

11. Actualizar:

1. Posibilidad de esperar a que se reinicie la computadora después de la actualización, sin notificar al usuario.
2. Sistema de actualización en cascada utilizando un servidor de actualización local (Relay).
3. Actualice los clientes en una ubicación remota a través de un cliente existente con la función de servidor de actualización integrada.
4. La función del servidor de actualización del cliente debe estar disponible para los sistemas operativos Windows y Linux.

12. Gestión de parches:

1. Habilidad para funcionar en modo automático
    a. Evaluación del horario para el parche perdido
    b. Programar la instalación automática separada según la categoría de parches (seguridad / no seguridad)
    c. Posibilidad de posponer el reinicio, si la instalación del parche lo solicita.
2. La solución debe permitir el modo manual: descubrimiento e instalación de parches bajo demanda
3. La solución debe ofrecer la posibilidad de ver todos los parches que faltan en el entorno. Esta información debe ser agregada en un inventario de parches.
    a. La solución ofrecerá visibilidad de los puntos finales que tienen instalados o les falta un parche específico.
    b. La solución ofrecerá información y razones si un parche no se instala.
    c. La solución le dará al usuario la capacidad de instalar rápidamente parches faltantes
    d. El usuario debe poder incluir en la lista negra uno o más parches.
4. La solución ofrecerá informes de los parches faltantes desde la perspectiva del punto final (parches instalados / faltantes en cada punto extremo)

5. La solución enviará notificaciones periódicamente, si faltan parches en los puntos finales del entorno.
6. La solución proporcionará la posibilidad de almacenamiento en caché, de esta manera los parches se descargarán de Internet solo por algunos puntos finales asignados.

13. Módulo de Analizador de Riesgos:

1. Habilidad para identificar y remediar una gran cantidad de riesgos de red y sistema operativos a nivel de endpoint (estaciones de trabajo y servidores). El modulo debe:

    a. Tener Dashboard o tablero de control con información accesible y de manera concreta sobre los indicadores de riesgos globales de la entidad
    b. Validar la puntuación de riesgo de acuerdo a la ponderación de los riegos evidenciados en la entidad.
    c. Proporciona una descripción general de la seguridad de su red y la información de evaluación de riesgos
    d. Enviar tareas de escaneo basadas en indicadores de riesgo en toda su red
    e. Identificar los puntos finales con configuraciones incorrectas.
    f. Posibilidad de realizar acciones para corregir las configuraciones incorrectas de manera asistida por la solución.
    g. Posibilidad En caso de no poderlas corregir las configuraciones incorrectas, muestra las rutas o acciones que se debe realizar para corregir las configuraciones incorrectas.
    h. Identificar los puntos finales con aplicaciones vulnerables
    i. Muestra de manera concreta como corregir los riesgos basados en vulnerabilidades y que tipo de vulnerabilidades afectan el equipo de escritorio o servidor.
    j. Identificar los riesgos ocasionados por factor humano.
    k. Evidenciar la evolución semanal del número de dispositivos afectados detectados como vulnerables tras los análisis de riesgo.
    l. Evidenciar los 15 resultados principales de los indicadores que activaron una alerta de riesgo después de escanear los dispositivos, ordenados por la cantidad de dispositivos afectados para configuraciones erróneas y vulnerabilidad de aplicaciones.
    m. Evidencia los 15 resultados principales de riesgos potenciales causados por el comportamiento no intencional o imprudente de los usuarios activos en su red, ordenados por la cantidad de usuarios vulnerables.
    n. Evidencia la gravedad de los riesgos que amenazan a los servidores y estaciones de trabajo de la entidad.
    o. Evidencia los servidores y estaciones de trabajo más vulnerables de su entorno, según la puntuación general calculada después de escanear en busca de configuraciones erróneas y vulnerabilidades.
    p. Evidenciar los usuarios más vulnerables de su entorno, según la puntuación global calculada tras analizar su comportamiento y actividad.

14. Protección de Servidor Exchange On-premise:

1. La solución debe proporcionar filtrado antimalware para el tráfico de correo electrónico entrante, interno y saliente.
2. La solución debe ser compatible con las capacidades de análisis bajo demanda y programadas para buzones y carpetas públicas, incluida la posibilidad de excluir buzones específicos o carpetas públicas, así como opciones para analizar solo los correos electrónicos con adjuntos o correos electrónicos recibidos en las últimas horas / días.
3. Posibilidad de configurar diferentes acciones a tomar en archivos infectados,

	sospechosos o que no se pueden analizar. 4. Capacidad para excluir aplicaciones potencialmente no deseadas (PUA) del filtrado de antimalware. 5. Capacidad de escanear en busca de malware dentro de los archivos. 6. La solución debe proporcionar un filtro antispam para el tráfico de correo electrónico, con la posibilidad de incluir en la lista blanca direcciones de correo electrónico y dominios específicos. 7. Capacidad para consultar los servidores de listas de Blackhole en tiempo real (RBL) definidos por los administradores y filtrar los mensajes de correo electrónico como spam según la reputación del servidor del remitente. 8. Posibilidad de marcar automáticamente como mensajes de correo electrónico no deseado escritos en Asia o Cirílico. 9. Capacidad para realizar consultas basadas en la nube para mejorar la protección contra el nuevo correo no deseado. 10. Capacidad para realizar diversas acciones en correos electrónicos no deseados detectados, incluido el prefijo del asunto del correo electrónico con una etiqueta específica, eliminar, poner en cuarentena o redirigir el correo electrónico a un buzón específico. 11. La solución debe proporcionar capacidades de filtrado de contenido para el tráfico de correo electrónico entrante, interno y saliente, basado en texto específico o expresiones regulares que coincidan con el asunto del correo electrónico y / o el contenido del cuerpo. 12. Capacidad para realizar diversas acciones en los correos electrónicos que coincidan con las reglas de filtrado de contenido, incluido el prefijo del asunto del correo electrónico con una etiqueta específica, eliminar, poner en cuarentena o redirigir el correo electrónico a un buzón específico. 13. La solución debe proporcionar capacidades de filtrado de archivos adjuntos para el tráfico de correo electrónico entrante, interno y saliente, según el tipo de archivo adjunto o nombre de archivo. 14. Capacidad para realizar diversas acciones en los correos electrónicos que coinciden con las reglas de filtrado de archivos adjuntos, incluida la eliminación o el reemplazo del archivo adjunto, el prefijo del asunto del correo electrónico con una etiqueta específica, la eliminación, la puesta en cuarentena o la redirección del correo electrónico a un buzón específico. 15. Capacidad para bloquear conexiones SMTP según la dirección de correo electrónico o el dominio del remitente. 16. Capacidad para definir direcciones IP autorizadas para enviar correos electrónicos para dominios propios para chequeos antispoofing. 17. Capacidad para definir reglas de filtrado personalizadas basadas en grupos de usuarios. 18. Capacidad para ver estadísticas e informes sobre la actividad de filtrado de correo electrónico. 19. Capacidad para ver y administrar de manera centralizada los elementos en cuarentena, incluida la capacidad para descargar o restaurar elementos en cuarentena. 15. Threats Xplorer: 1. Ofrece una visibilidad sobre las amenazas detectadas en la red. La función centraliza los eventos de detección y los clasifica por categoría, tipo de amenaza, acciones correctivas y muchos otros: Identifica y analizar fácilmente cualquier evento de la entidad durante un intervalo de tiempo específico utilizando los filtros disponibles a. Centraliza los eventos de detección de los siguientes módulos: antimalware, protección de almacenamiento, Exchange Protection, control de dispositivos, firewall.	

b. Threats Xplorer proporciona una amplia variedad de columnas y filtros para ayudar a navegar por la lista de eventos. Se puede seleccionar filtros en el menú desplegable o escribir palabras clave que coincidan con los resultados deseados.

16. MODULO DE INCIDENTES:

1. Solución debe ofrecer un modulo que ayuda a filtrar, investigar y tomar medidas sobre todos los eventos de seguridad detectados por Incidents Sensor durante un intervalo de tiempo específico, el modulo debe ofrecer las siguientes caracteristicas:

    a. Incidentes : ver e investigar incidentes.
    b. Lista de bloqueo : gestionar archivos bloqueados por incidentes.
    c. Buscar : consultar la base de datos de eventos de seguridad.
    d. Reglas personalizadas : crear reglas personalizadas para exclusiones o detecciones.
    e. El módulo de incidentes debe proporcionar una cuadrícula altamente personalizable que muestre una lista de incidentes de EDR/XDR generados para la organización en los últimos 90 días.
    f. Debe contar con un botón de alternancia del panel SMART VIEW . Esta función le permite personalizar, guardar y cambiar entre diferentes configuraciones de la página de Incidentes.
    g. La grilla de incidentes muestra todos los incidentes que no tengan más de 90 días y que se ajusten al filtro aplicado actualmente

    h. Identifica y analizar fácilmente cualquier evento de la entidad durante un intervalo de tiempo específico utilizando los filtros disponibles.
    i. Centraliza los eventos de detección de los siguientes módulos: antimalware, protección de almacenamiento, Exchange Protection, control de dispositivos, firewall.
    j. Threats Xplorer proporciona una amplia variedad de columnas y filtros para ayudar a navegar por la lista de eventos. Se puede seleccionar filtros en el menú desplegable o escribir palabras clave que coincidan con los resultados deseados.
    k. Debe contar con un menú Ver que permite múltiples acciones para trabajar con la vista: guardar, guardar como, descartar cambios, agregar a favoritos, mostrar u ocutar filtros, abrir configuración.
    l. Debe contar con un menú de Filtros: esta opción debe permitir personalizar los incidentes que se presentan en la grilla con los siguientes filtros: IDENTIFICACION, creado en, ultima actualización, estado, cesido de, prioridad, puntuación de gravedad, incidentes correlacionados, recursos, ultima fase de cadena de muerte, tipo de incidente, parámetros.
    m. Acciones de incidente . El botón proporciona las siguientes opciones: ver eventos y alertas
    n. Boton cambiar estado: la solución debe permitir cambiar el estado del incidente: abierto, investigando, falso positivo y cerrado.

16. MODULO DE EDR:

1. La solución debe contar con Endpoint Detección y Respuesta (EDR) correlación de eventos, capaz de identificar amenazas avanzadas o ataques en progreso.

    a. Sensor de incidentes debe monitorear continuamente la actividad de los terminales
    b. Sensor de incidentes debe monitorear procesos en ejecución
    c. Sensor de incidentes debe monitorear cambios en el registro.
    d. Sensor de incidentes debe monitorear comportamiento de usuarios

e. Sensor de incidentes debe recopilar, informar y procesar los datos mediante algoritmos de machine learning y tomar acciones automáticas de las actividades sospechosas detectadas.
f. El sensor de EDR debe entregar las incidencias o comportamientos sospechosos y presentarlas en el panel de Incidentes.
g. El sensor debe ser desplegable desde la administración de los puntos finales.

PROTECCIÓN PARA ESTACIONES DE TRABAJO Y SERVIDORES VIRTUALIZADOS

1. Protección antimalware dedicada a entornos virtualizados: requisitos mínimos:

1. El producto se integra con VMware VShield o VMware NSX y ofrece la posibilidad de escaneo antimalware sin instalar un agente de escaneo en la máquina virtual.
2. El componente de administración central de la solución se integra con varios vCenters de VMware.
3. Para todos los sistemas que ejecutan Windows y Linux, el producto incluye:
    a. Proceso de escaneo;
    b. Escaneo de memoria;
    c. Escaneo en tiempo real de archivos;
    d. Escanear archivos bajo demanda;
4. Exploración en tiempo real y bajo demanda para máquinas virtuales Linux.
5. Introspección de Linux a través de VMware NSX.
6. El producto se integra con varios servidores Citrix Xen (los inventarios se importan en el producto).
7. El producto también es compatible con Microsoft Hyper-V, Red Hat Virtualization, Oracle VM y KVM.
8. El producto debe incluir una única máquina de escaneo virtual que:
    a. Contiene las firmas antimalware;
    b. Proporciona una protección completa, actualizada, al abrir una máquina virtual;
    c. Proporciona escaneo optimizado.
9. El producto de software que se instala en las máquinas virtuales, para facilitar la transmisión de la información que se va a escanear, debe ocupar unos 10 MB de RAM.

2. Características generales:

1. Métodos para la detección de virus, spyware, rootkits y otros programas maliciosos.
2. El producto debe permitir la actualización automática del dispositivo virtual de seguridad, para firmas de antimalware y para el sistema operativo del dispositivo virtual de seguridad.
3. El producto debe informar el estado actual del host de seguridad: VMs protegidos / desprotegidos y dispositivos virtuales de seguridad.

3. Requisitos mínimos del sistema:

A. Plataformas de virtualización:

- VMware vSphere,6.5,6.0, 5.5, 5.1, 5.0 P1 (Patch # 474610-1) or 4.1 P3 (433,742-Patch # 3)

incluyendo ESXi 4.1 and ESXi 5.0 con:

- VMware vCenter Server 6.5,6.0, 5.5, 5.1, 5.0 or 4.1
- VMware VShield Manager 5.5, 5.1, 5.0

- VMware VShield VShield Endpoint Manager instalado en el equipo
- VMware Tools 8.6.0 build 446312 o reciente
- VMware NSX 6.2.4(6.3 para Linux support) o reciente

- VMware View 5.1, 5.0 o reciente
- Citrix XenDesktop 5.5, 5.0 o reciente
- XenServer 7.2, 7.1, 7.0, 6.0, 5.6 or 5.5 (incluyendo Xen Hypervisor)
- Citrix XenApp
- Microsoft Hyper-V Server 2012, Microsoft Hyper-V Server 2008 R2 or Windows 2008 R2 (incluyendo Hyper-V Hypervisor)
- Oracle VM 3.0
- Red Hat Enterprise Virtualization 4.1, 4.0, 3.0 (incluyendo KVM hypervisor)

B. Sistemas Operativos para Máquinas Virtuales (32/64 bit):

- Windows 10, 8.1, 8, Windows 7, Windows Vista, Windows XP (SP3)
- Windows Server 2016, Windows Server 2012, Windows Server 2012 R2 Windows Server 2008, Windows Server 2008 R2
- Windows Server 2003, Windows Server 2003 R2
- Oracle Solaris 11, 10
- Distribuciones Linux:
  - Red Hat Enterprise Linux 5.6 o reciente
  - CentOS 5.6 o reciente
  - Ubuntu 12.04 o reciente
  - SUSE Linux Enterprise Server 11 o reciente
  - OpenSUSE 12, 11
  - Fedora 16, 15
  - Debian 7.0 o reciente

4. Las principales características y funcionalidades del módulo antimalware:

1. Exploración automática de archivos que se copian en soporte externo y de LAN o WAN.
2. La exploración automática en tiempo real de los archivos se puede configurar para analizar solo tipos de archivos específicos, con extensiones específicas, definidas por el administrador.
3. La exploración automática en tiempo real de los archivos se puede configurar para que no analice archivos con un tamaño superior a «x» Kb, el administrador de la solución puede definir los tamaños de los archivos.
4. El escaneo bajo demanda incluirá las siguientes opciones:
   a. Escanee cualquier medio de almacenamiento conectado a la máquina virtual;
   b. Escaneo de correos electrónicos;
5. Configuración de las rutas a escanear, a nivel de archivo;
6. Debe permitir que el administrador defina ciertas carpetas, discos, archivos y extensiones que se excluirán del análisis en tiempo real y el análisis bajo demanda.
7. Para no sobrecargar los recursos del sistema, el producto antimalware debe contener un solo motor de análisis.
8. Para permitir la optimización de la cantidad de tráfico enviado a la red a través de un mecanismo de almacenamiento en caché en la máquina de escaneo y la máquina virtual.
9. Agente de conmutación por error / conexiones de equilibrio de carga a la máquina de escaneo.
10. Las políticas pueden aplicarse a un grupo de recursos de VMware vCenter.

5. Cuarentena:

1. El producto antimalware debe permitir la eliminación automática de archivos en cuarentena más antiguos que un período determinado, sin ocupar espacio de almacenamiento innecesario.
2. La capacidad de mover un archivo de la cuarentena a su ubicación original.
3. Cuarentena centralizada. La capacidad de recopilar de forma segura todos los archivos en cuarentena desde puntos finales protegidos a una ubicación única en la red para una investigación más profunda.
4. Capacidad para descargar el archivo directamente a la estación de trabajo del administrador (solo para la integración de VMware vShield o NSX).
5. Capacidad para volver a analizar los archivos en cuarentena después de cada actualización de la firma.
6. Posibilidad de envío automático de archivos de cuarentena a los laboratorios del fabricante en un intervalo de tiempo establecido por el administrador.

7. Gestión e instalación remota:

1. El dispositivo virtual de seguridad se puede personalizar antes de la instalación. Se escala automáticamente según varias características: número de máquinas virtuales en el host, redes, direcciones IP asignadas a recursos (CPU, memoria), etc.
2. La consola de administración informará el número de máquinas virtuales que han instalado o no la solución de protección antivirus y el estado de la máquina: activado o desactivado.
3. La posibilidad de que la consola de administración informe si el módulo antimalware está habilitado o no en la máquina virtual.

C. SEGURIDAD PARA DISPOSITIVOS MOVILES

1. Requisitos mínimos del sistema:

- Apple iPhone y tabletas iPad (iOS 8.1+)
- Google Android smartphones y tabletas (2.2+)

2. Caracteristicas:

1. Permite asociar un dispositivo con un usuario de Active Directory.
2. La instalación se realiza enviando un correo electrónico al usuario, con los detalles de la instalación.
3. La activación del dispositivo a la consola de administración se realizará mediante un código QR.
4. Los paquetes de instalación se pueden descargar desde Apple App Store y Google Play.
5. Se pueden tomar las siguientes acciones:
    a. Imponer el bloqueo de pantalla y la autenticación;
    b. Restaurar a la configuración de fábrica;
    c. Localice el dispositivo;
    d. Escaneo de dispositivos (para el sistema operativo Android);
    e. Cifrado de memoria del dispositivo (para el sistema operativo Android).
6. La Consola de administración informará sobre los dispositivos que están activos, inactivos, desconectados o con jailbreak.

3. Configuraciones de seguridad:

1. Si un dispositivo no cumple con la configuración deseada, se pueden realizar

las siguientes acciones:

a. Ignorar;
b. Bloquear el acceso;
c. Dispositivo de bloqueo;
d. Restaurar la configuración de fábrica;
e. Elimine el dispositivo de la consola de administración.

2. Se pueden realizar dispositivos de bloqueo con una acción de contraseña. Esta contraseña se puede configurar para contener:
   a. Contraseña simple o compleja (específica para el sistema operativo);
   b. Números y caracteres;
   c. Longitud mínima definida por el administrador;
   d. Mínimo de caracteres especiales, definidos por el administrador;
   e. Período de caducidad de la contraseña. El período será definido por el administrador;
   f. Configuración de restricción de reutilización de contraseña;
   g. El número de intentos de entrada de contraseña incorrectos;
   h. Período de bloqueo del dispositivo después de una cantidad de minutos definidos por el administrador.
3. Se pueden generar varios perfiles, que establecerán reglas de seguridad para la conectividad Wi-Fi o VPN (solo para el sistema operativo iOS), pero también algunos relacionados con el acceso a ciertos sitios web.
4. Los perfiles de Wi-Fi contendrán las siguientes opciones:
   a. General: se definirá el SSID, así como el tipo de seguridad de la red;
   b. Configuración de TCP / IP - para los protocolos IPv4 e IPv6;
   c. Configuración de proxy - deshabilitada, automática o configurada manualmente.
5. Los perfiles relacionados con el acceso a sitios web (sistema operativo Android) incluyen características como:
   a. Permitir, bloquear o programar para días y franjas horarias específicos el acceso a ciertos sitios web;
   b. Creación de excepciones para bloquear o permitir el acceso a sitios web específicos.
6. Los perfiles con respecto al acceso a sitios web (sistema operativo iOS) incluyen opciones para habilitar o deshabilitar:
   a. Uso del navegador Safari;
   b. Opciones de autocompletar;
   c. Alertar a los usuarios al acceder a sitios web maliciosos;
   d. JavaScript;
   e. Pop-ups;
   f. Cookies.

D. INTROSPECCIÓN DE MEMORIA CON HYPERVISORES

Requerimientos mínimos

- CPU microarchitecture: – cualquier Intel® Sandy Bridge processor o reciente, con soporte para Intel® Virtualization Technology. – VT-x or VT-d las extensions deben estar activadas en la BIOS.
- Citrix XenServer 7 Enterprise Edition o reciente.
- Las máquinas deben ejecutar un sistema operativo compatible:
  - ● Windows Desktop Operating Systems – Windows 10 – Windows 8.1 – Windows 8 – Windows 7 ● Windows Server Operating Systems – Windows Server 2016 – Windows Server 2012 / Windows Server 2012 R2 – Windows Server 2008 / Windows Server 2008 R2
  - Linux Operating Systems – Debian 9, 64-bit – Debian 8, 64-bit – Ubuntu 16.04 LTS, 64-bit – Ubuntu 14.04 LTS, 64-bit – CentOS 7, 64-bit – Red

	Hat Enterprise Linux 7, 64-bit – SUSE Linux Enterprise Server 12, 64-bit – Oracle Linux 7.3, 64-bit Caracteristicas: 1. La solución se integra con la tecnología de hipervisor para proporcionar protección sin agente para las máquinas virtuales invitadas (no hay agente y / o controlador instalado dentro de la máquina virtual hosteada) 2. La solución protege la memoria de los sistemas operativos Windows y Linux. 3. La solución controla el modo de usuario del sistema operativo y la memoria del modo kernel 4. La solución supervisa y protege los siguientes componentes del espacio del kernel a. Registros de control b. Registros específicos del modelo c. IDT / GDT integridad d. Drivers cargados 5. La solución ofrece detalles forenses adicionales, informados en la consola de administración a. Eventos fallos del sistema operativo b. Eventos del conductor c. Eventos de bloqueo de aplicación 6. La solución ofrece mecanismos de introspección de hipervisores para acceder a la memoria de la máquina virtual sin procesar y detecta violaciones de memoria provocadas por técnicas de ataque como el desbordamiento de búfer, el desbordamiento de búfer o la inyección de código. 7. La solución ofrece alertas, notificaciones e informes de eventos disponibles en una consola de administración centralizada. 8. Sobre la base de la detección de violación de memoria, la solución es capaz de inyectar una herramienta de remediación en la máquina virtual en ejecución para recopilar detalles forenses adicionales y realizar un análisis completo del sistema antimalware; La herramienta de remediación tiene la capacidad de eliminarse una vez que se realiza la remediación. 9. La solución permite a los administradores de TI o los equipos de seguridad inyectar herramientas de terceros en máquinas virtuales sin ninguna interacción del usuario o conexión de red. 10. Las herramientas de terceros deben tener la opción de ser inyectadas manualmente, automáticamente o programadas.	
2	**CAPACITACIÓN DE SOFTWARE DE ANTIVIRUS**	

Se requiere que el contratista realice capacitación del antivirus a suministrar (tanto para las 800 licencias de sistema operativo Windows.

La capacitación se debe realizar en las oficinas de la Dirección TIC de la gobernación, y será dirigida al personal técnico de sistemas.

La capacitación debe abarcar las siguientes temáticas:

- Introducción al antivirus a suministrar
- Mecanismo de instalación, configuración y parametrización segura de antivirus
- Identificación de ataques y vulnerabilidades
- Administración de ambientes
- Protección contra amenazas basada en Aprendizaje automático (Machine Learning – ML)
- Protección de datos
- Capacidad de instalar la solución de seguridad en smartphones y tablets Android, IOS
- Creación de perfiles
- Configuración de seguridad y protección para correos electrónicos
- Capacidad Control de funciones y Control web
- Activación de Cloud
- Políticas y configuraciones

1

SOPORTE Y ASISTENCIA TÉCNICA DE SOFTWARE DE ANTIVIRUS POR UN (1) AÑO

Se requiere que el contratista ofrezca el servicio de soporte y asistencia técnica del software antivirus a suministrar.

El servicio de soporte y asistencia técnica debe contar con las siguientes características:

- Jornadas de asistencia técnica de revisión preventiva cada tres (3) meses.
- Soporte técnico por problemas técnicos.
- Habilitación de Help Desk sobre las demandas más comunes de los usuarios, el cual debe contener un centro de ayuda (documento) donde los usuarios encuentran asistencia sobre las funcionalidades y módulos del antivirus a suministrar.
- Posibilidad de ofrecer el servicio de soporte y asistencia técnica habilitado con múltiples canales.
- Atención las expectativas del personal de la dirección TIC con respecto a la experiencia.

3 1 año

Tiempo validez de soporte y asistencia técnica (12 meses).

2.1. EXPERIENCIA DEL PERSONAL TECNICO:

Debido a los requerimientos técnicos descritos anteriormente se requiere personal altamente calificado que pertenezca al equipo de trabajo del oferente.

Con el objeto de seleccionar un proveedor que garantice estabilidad de los servicios a RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER, CON ACTUALIZACION, SOPORTE, CAPACITACION Y ASISTENCIA TECNICA POR EL TERMINO DE UN AÑO, PARA LAS ESTACIONES DE TRABAJO Y SERVIDORES DE LA PLATAFORMA TECNOLOGICA DE LA GOBERNACION DE BOLIVAR, los cuales son de misión crítica para el funcionamiento de la entidad, es necesario que el proponente cuente con personal altamente calificado, capacitado y experimentado, para lo cual se requiere, adjuntar las hojas de vida y certificados

Para garantizar la correcta ejecución del contrato, La Gobernación de Bolívar, se requiere que el oferente presente dentro de su equipo de trabajo, un Ingeniero Gerente de Proyectos de TI, con el objeto de servir de enlace entre el supervisor del contrato por parte de La Gobernación de Bolívar y la empresa oferente; realizando entrega de los documentos solicitados en el presente proceso al igual que los informes mensuales de funcionamiento general del antivirus a contratar.

El oferente debe contar con certificado que permita garantizar que cuenta con personal de Bitdefender Certified Technical Specialist.

Descripción del Personal requerido:

- **Gerente de proyecto**: ingeniero de sistemas, electrónico, industrial o afín, con estudios en antivirus y cloud computing, especialista en seguridad informática, con 10 años de experiencia en administración y configuración de antivirus, debe contar con certificación BITDEFENDER CERTIFIED TECHNICAL SPECIALIST, con certificación especializada en Cyber Security Foundation, con estudios como auditor en la norma internacional ISO 27001, con estudios en Ethical Hacking, experiencia en administración de servidor y soporte remoto.

2.2. EXPERIENCIA TECNICA:

Debido a los requerimientos técnicos descritos anteriormente se requiere que el oferente sea altamente calificado. La Gobernación de Bolívar, para garantizar la correcta ejecución del contrato, requiere que el oferente presente certificado que conste que el oferente es categoría GOLD RESELLER STATUS del antivirus Bitdefender.

3. ALCANCE DEL OBJETO:

El contratista para cumplir con la ejecución del contrato debe:

- Efectuar la entrega del servicio contratado de acuerdo con las especificaciones técnicas requeridas y en los tiempos exigidos por la Gobernación de Bolívar.
    - Atender las observaciones y requerimientos de la supervisión del contrato.
    - Responder por la calidad de los servicios suministrados.
    - Responder por el perfecto funcionamiento del servicio de suministro.

4. CLASIFICACIÒN DEL BIEN O SERVICIO DE ACUERDO CON EL CLASIFICADOR DE BIENES Y SERVICIOS

La clasificación de los bienes y servicios, objeto del Proceso de Contratación según el Sistema de codificación de las Naciones Unidas para estandarizar productos y servicios, conocido por las siglas UNSPSC, es la siguiente:

GRUPO	SEGMENTO	FAMILIA	CLASE	PRODUCTO	DESCRIPCIÓN PRODUCTO
E	43	23	32	00	Software de seguridad y protección
E	43	23	32	05	Software de seguridad de transacciones y de protección contra virus
F	81	11	25	00	Servicios de alquiler o arrendamiento de licencias de software de computador

5. IDENTIFICACIÒN DEL CONTRATO A CELEBRAR

El objeto del contrato es satisfacer las necesidades que requiere la entidad, por lo tanto, el tipo de contrato a celebrar es de prestación de servicio.

6. PLAZO DE EJECUCIÒN DEL CONTRATO
El plazo oficial de ejecución será hasta el 31 de diciembre de 2023 o hasta agotarse el presupuesto destinado para esta contratación, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución, término durante el cual el contratista seleccionado deberá cumplir con el objeto contratado y el cual no podrá sobrepasar el 31 de diciembre de 2023. Este plazo se empezará a contabilizar una vez se expida el correspondiente registro presupuestal, y se aprueben las garantías exigidas

7. LUGAR DE EJECUCIÒN:

GOBERNACIÓN DE BOLÍVAR
El domicilio contractual es el Municipio de Turbaco, en las instalaciones del Centro Administrativo Departamental - CAD, ubicado en la siguiente dirección: Carretera Cartagena - Turbaco, Km 3, Sector Bajo Miranda - el Cortijo

En constancia, se firma en _____, a los ____ días del mes de _____ de 2023

Atentamente,

Nombre del Proponente

Nombre del Representante Legal

C. C. No. de

Dirección de correo

Correo electrónico

Ciudad

_____

[Firma del proponente o de su Representante Legal