Interior

FICHA TECNICA

Clasificación de Bienes y Servicios - Clasificación UNSPSC

La solución entregada debe estar codificada en el clasificador de bienes y servicios UNSPSC como se indica a continuación:

Grupo	Segmento	Familia	Clase	Producto
E	[43000000] Difusión de tecnologías de información y telecomunicaciones	[43230000] Software;	[43233200] Software de Seguridad y Protección	[43233205] Software de Seguridad de transacciones y de protección contra virus
F	[81000000] Servicios Basados en Ingeniería, Investigación y Tecnología	[81110000] Servicios informáticos	[81112200] Mantenimiento y soporte de software	[81112208] Mantenimiento de software de protección de seguridad
E	[43000000] Difusión de tecnologías de información y telecomunicaciones	[43210000] Equipo informático y accesorios	[43211500] Computadores	[43211501] Servidores de computador
E	[43000000] Difusión de tecnologías de información y telecomunicaciones	[43200000] Componentes para tecnología de la información, difusión o telecomunicaciones	[43201800] Dispositivos de almacenamiento	[43201835] Dispositivo de almacenamiento unido a la red más
F	[81000000] Servicios Basados en Ingeniería, Investigación y Tecnología	[81110000] Servicios informáticos	[81112000] Servicio de datos	[81112006] 81112006 Servicios de almacenamiento de datos

La solución de antivirus para la protección de puestos de servicios ofertada debe contar con al menos las siguientes capacidades o funcionalidades de protección:

Ítem	Descripción	Requerimiento Mínimo
1	**Nombre comercial del producto**	Renovación Kaspersky Next EDR Optimum - 1 año

2	**Número de licencias**	1.500
3	**Idioma de la solución**	Al cierre del proceso, los diferentes componentes y herramientas de la solución antivirus deben estar disponible en idioma español Latinoamérica.
4	**Consola de administración**	La consola de administración de la herramienta antivirus debe cumplir con: Ejecutar tareas de administración y mantenimiento básicas en la red de una organización de forma centralizada. La aplicación proporciona al administrador acceso a información detallada sobre el nivel de seguridad de la red d e la organización; permite configurar todos los componentes de protección desarrollados usando las aplicaciones. Crear una jerarquía de los Servidores de administración para administrar la red de la organización, como también las redes en las oficinas remotas o en las organizaciones cliente. La organización cliente es una organización cuya protección antivirus está garantizada por un proveedor de servicios. Crear una jerarquía de grupos de administración para administrar una selección de dispositivos cliente como si fueran una sola entidad. Administrar un sistema de protección antivirus. Llevar a cabo el despliegue centralizado de las claves de licencia de las aplicaciones de Endpoint en dispositivos cliente, supervise su utilización y renueve las licencias. Recibir estadísticas e informes sobre el funcionamiento de las aplicaciones y dispositivos. Protección Endpoint Administrar dispositivos móviles. Administrar el cifrado de la información almacenada en unidades extraíbles y en los discos duros de los dispositivos, y el acceso de los usuarios a los datos cifrados. Realizar el inventario del hardware conectado a la red de la organización. Administrar de forma centralizada los archivos puestos en Cuarentena o Copia de seguridad por las aplicaciones de seguridad, y los archivos para los cuales se haya aplazado el procesamiento de parte de las aplicaciones de seguridad.
5	**Características de los componentes tecnológicos**.	La solución antivirus debe proteger a los siguientes sistemas operativos Windows 32 y 64 bits, puestos de trabajo fijo y móvil (portátiles) en las plataformas Intel y AMD, los sistemas operativos: Windows 7 Sp1 o posteriores, Se debe garantizar que se pueda efectuar la instalación en la última versión del Sistema Operativo Windows con que cuente el Ministerio, así como también proteger sistemas operativos MacOS y Linux en sus diferentes versiones.
		El sistema de firmas de malware basado en reputación de archivos, podrá manejarse de manera integrada y visualizada desde la misma consola de antimalware.
		El sistema de firmas de malware basado en reputación de archivos, podrá manejarse de manera independiente (standalone) y visualizada desde la misma consola de antimalware.
		Capacidad de identificar vulnerabilidades en productos Microsoft instalado en las estaciones de trabajo y servidores.
6	**Cifrado de datos**	La solución antivirus debe estar en capacidad de cifrar datos de manera segura en dispositivos tanto fijos como extraíbles aplicando como mínimo las siguientes reglas: Cifrar/Descifrar Unidad completa Cifrar/Descifrar todos los archivos Cifrar/Descifrar archivos seleccionados Cifrar/Descifrar solo archivos nuevos
7	**Aprendizaje Automático**	Utilización de tecnologías avanzadas de predicción que permita el aprendizaje automático para detectar amenazas desconocidas que generen riesgos de seguridad en los procesos o archivos sospechosos originados desde medios de almacenamiento externos, internos, servicios web o canales de correo.
8	**Control de**	Proporcionar o restringir desde la consola de administración el acceso y/o permisos a dispositivos extraíbles tales como USB, Floppy, CD´s, SD, MTP Siendo esta configuración independiente para cada uno de los dispositivos a proteger.
		La solución Antimalware deberá evitar una infección provocada por la ejecución del archivo Autorun.inf u

	dispositivos	otros archivos infectados contenidos en dispositivos extraíbles tales como USB, Floppy, CD, SD, al momento de ser conectado en la estación de trabajo.
9	**Protección por comportamiento**	Detección y reacción contra ransomware que inicie el cifrado de información, así no se tenga firma de detección de malware para detenerlo. Proteger documentos contra cifrado o modificación no autorizada Evitar o monitorear que un programa con comportamiento sospechoso pueda modificar el archivo de HOST. Evitar o monitorear que un programa con comportamiento sospechoso modifique archivos de sistema. Para aquellos programas válidos y que por su comportamiento el Antimalware no permita su ejecución, deberá de permitirlos agregándolos a una lista blanca.
10	**Reporte de amenazas a los laboratorios.**	Capacidad de reportar eventos de amenazas aún no identificadas, de manera automática a través del comportamiento, a los laboratorios de antimalware para el análisis e identificación de la fuente y generación de una protección proactiva y oportuna. Capacidad de limitar los recursos utilizados para la notificación a los laboratorios, respetando la confidencialidad de la información.
11	**Uso de Rendimiento**	Selección del nivel de uso de rendimiento mientras se realiza un escaneo programado, manual o desde la consola: a. La solución de antimalware podrá manejar niveles de uso de rendimiento cuando el usuario ejecute un escaneo manual, dicha configuración deberá manejarse de manera centralizada por el administrador. b. La solución de antimalware podrá manejar niveles de uso de rendimiento cuando se programen los escaneos a las estaciones de trabajo, dicha configuración deberá manejarse de manera centralizada por el administrador. c. La solución de antimalware podrá manejar niveles de uso de rendimiento cuando el usuario ejecute desde la consola de antimalware, dicha configuración deberá manejarse de manera centralizada por el administrador.
12	**Seguridad:**	Garantizar que los clientes tengan los servicios activos, últimos componentes, consistencia en configuraciones y que han corrido escaneos regularmente. La solución debe garantizar la seguridad a través de SSL para las comunicaciones entre el servidor y la dirección web de la consola Integración con Active Directory para la asignación de roles y permisos de Acceso a las configuraciones de la consola.
13	**Configuraciones**	Aplicar configuración de políticas por servidor o estación de trabajo, por grupo o por usuario de manera independiente. Manejo de configuraciones: • Importar o Exportar configuraciones de políticas de un grupo de estaciones de trabajo a otro. • Personalizar los permisos de los clientes para realizar acciones en el software local. • Personalización de opciones de escaneo y Acción para una detección en los modos: Manual, en Tiempo Real y Programado. • Integración de la solución con un dominio de Active Directory. • Distribución de actualizaciones a los clientes de manera Automática y Manual.
14	**Control de aplicaciones**	Compatibilidad con Sistemas Operativos Windows 32 y 64 bits Windows 7 Sp1 y posteriores Windows Server 2008 R2 y posteriores La solución debe contar con la capacidad de definir listas blancas y negras de forma manual para la ejecución de aplicaciones, como mínimo requerido las siguientes: Indicando la ruta del ejecutable, ya sea la ruta completa o utilizando expresiones regulares para definir la ruta. Indicando el HASH del archivo. Indicando los atributos del certificado con el que está firmado el archivo. A través de un servicio de reputación del fabricante donde se identifiquen archivos pertenecientes a software de los sistemas operativos y aplicaciones más populares.

15	**Protección contra explotación de vulnerabilidades en estaciones de trabajo**	La solución debe permitir escaneo profundo avanzado de vulnerabilidades y distribución automatizada de parches tanto de productos Microsoft como de los fabricantes más vulnerados por ciberataques. Capacidad de aplicar parches de productos de software en un entorno controlado con el fin de probar la integridad de los mismos y garantizar su funcionalidad para llevar a cabo el despliegue general.
16	**Soporte Técnico**	Soporte Telefónico, lunes a viernes de 8:00 AM a 5:00 PM. Suministrar un número de PBX y/o Línea Nacional. Soporte por Correo Electrónico, lunes a viernes de 8:00 AM a 5:00 PM, suministrar un correo electrónico para efecto de formular peticiones de soporte. Tiempo de Respuesta del Estado de la Solicitud: no superior a 4 horas hábiles. Soporte Presencial, lunes a viernes de 8:00 AM a 5:00 PM, Tiempo de respuesta: no superior a 8 horas hábiles. Debe contar con una oficina en la ciudad de Bogotá o municipios circunvecinos, con personal local para atender los requerimientos en los tiempos requeridos. La empresa oferente debe estar catalogada por el fabricante de la solución ofertada como Partner (Platinum, Gold), en todo sentido debe presentar una certificación expedida por el fabricante que garantice conocimiento certificado en la solución al momento de que se escalen incidentes o requerimientos; adjuntar certificación expedida por el fabricante. Soporte Página Web, radicación de problemas e Inquietudes por medio del mecanismo de “Envío de Tickets”. Soporte Remoto, asistencia técnica vía internet, 8:00 AM a 5.00 PM. El Proveedor debe contar con una Mesa de Servicio certificada garantizando la utilización de las mejores prácticas ITIL para la Gestión de Requerimientos de Servicio. El Proveedor deberá acreditar una experiencia especifica presentando mínimo 3 certificaciones de contratos suscritos, cuyo objeto haya sido el suministro o renovación de licencias antivirus Kaspersky de mínimo 1000 nodos. El proveedor debe garantizar la actualización de versión del software de antivirus, tanto para PC's, portátiles, Workstations, como para servidores y la(s) consola(s) de administración, mejoras del producto, correcciones, sin costo adicional mínimo durante el tiempo del contrato. El proveedor deberá incluir 2 análisis y diagnóstico de vulnerabilidades para 10 activos críticos con herramientas especializadas para tal fin. Este análisis se deberá realizar durante la vigencia del contrato y se realizan con el fin de mitigar posibles ataques a la plataforma del Min. Interior. Visita Mensual: Se requiere efectuar un visita mensual de dos (2) horas mínimo, durante la vigencia del licenciamiento para revisar el funcionamiento de la consola de distribución, verificar y resolver problemas que se encuentren registrados en dicha consola con respecto al control que ejerce el solución antivirus y en general malware detectado, eliminado o en cuarentena, con el fin de efectuar potenciales ajustes a la parametrización del entorno, que permita un control más efectivo de acuerdo con los casos que se van presentando. Nota: El servicio técnico post venta se prestará durante los 12 meses siguientes, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, con los requerimientos técnicos descritos en el numeral 2.1.1 del estudio previo. Así mismo, el proponente deberá prestar el servicio de capacitación presencial en la administración de las herramientas del antivirus.
17	**ENDPOINT DETECTION AND**	La solución debe contar con un sensor independiente que se integre al Endpoint para validar el comportamiento de las aplicaciones

	RESPONSE (EDR)	Debe ser capaz de realizar Análisis de raíz de la causa, en por lo menos dos niveles de profundidad Debe ser capaz de realizar Escaneo de indicadores de compromiso (IoC), importarlos y validarlos en servidores públicos para visualizar el impacto y las referencias de los indicadores Acciones de respuesta automáticas y configurables Debe realizar Aislamiento de los dispositivos con tiempo programados, Debe realizar escaneos del host Debe impedir que procesos seleccionados se ejecuten en los dispositivos protegidos Debe ser capaz de realizar Aislamiento del Endpoint en caso de malware o comportamientos sospechosos que puedan desencadenar un brote de malware Debe ser administrado desde la misma consola del Endpoint Compatibilidad con estaciones de trabajo Windows y servidores Windows Descubra las conexiones de la amenaza y su historial con la visualización de ruta de propagación de ataques.
18	**Control Adaptativo**	Detectar y bloquear acciones sospechosas que no son típicas de los equipos conectados a una red corporativa. diseñadas para buscar comportamientos que no se consideran usuales (por ejemplo, la regla Inicio de Microsoft PowerShell desde una aplicación de ofimática).
19	**Borrado Seguro**	Posibilidad de configurar tareas de borrado remoto de datos en estaciones de trabajo Windows La eliminación se puede hacer de manera inmediata, programada o Eliminación de datos pospuesta (cuando el dispositivo no se conecte a la consola en un tiempo definido)
20	**SEGURIDAD EN LA NUBE**	Facilitar la detección y restricción del uso inapropiado o no autorizado de recursos en la nube, así como el tiempo perdido en redes sociales y mensajeros. Monitorear más de 2700 servicios en la nube. Cada servicio en la nube detectado ahora tiene una calificación que indica qué tan peligroso es su uso. Esto significa que el administrador de IT puede evaluar fácilmente los riesgos potenciales y decidir permitir o bloquear un servicio en particular. Bloquear el acceso del usuario a recursos en la nube inapropiados o no autorizados, redes sociales o mensajeros. Proporciona visibilidad y control sobre los datos almacenados en la nube para prevenir el incumplimiento de los estándares de cumplimiento. La detección de datos gana visibilidad y control sobre los datos sensibles en MS Exchange Online, SharePoint Online, OneDrive y Teams. Los resultados de detección se pueden encontrar en informes y en la lista de detección, así como en los widgets del tablero. Tipos de archivos auditados: doc, docx, ppt, pptx, xls, xlsx, odt, odp, ods, PDF, RTF, jpeg, tiff, png, jp2.
21	**Protección para MS Office 365**	La solución de protección para Microsoft Office 365 debe ser completamente cloud La integración de la solución de protección para Microsoft Office 365 se debe realizar a través de Graph API La Solución debe contar por los menos con las siguientes características: o Protección Antimalware o Protección Anti Phishing o Protección Anti Spam o Protección Anti Spoofing o Protección contra correos masivos o Protección contra ataques BEC o Filtrado de Archivos Adjuntos La solución debe poder ejecutar acciones de protección sobre las siguientes aplicaciones: o Exchange Online o Microsoft Team o Sharepoint Online o One Drive Online La solución debe hacer validación de los correos recibidos a través de SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DMARC (Domain-based Message Authentication Reporting and Conformance) La plataforma Cloud debe estar disponible en múltiples idiomas, requeridos Inglés y Español, el cambio de idioma en la interfaz no debe suponer un cambio significativo en el espacio de trabajo La plataforma Cloud debe permitir múltiples administradores La plataforma Cloud debe tener un apartado tipo dashboard para visualizar los eventos recientes de

<table>
<tr><td></td><td></td><td>detecciones y tráfico del correo.
La creación de directivas de protección debe ser selectiva permitiendo escoger los buzones de correo que se van a proteger con determinadas características de proteger y debe permitir crear exclusiones
La solución de protección para Microsoft Office 365 debe permitir la creación de listas negras y blancas
La implementación de la solución debe ser trasparente para los usuarios y no generar afectación de los servicios
la solución debe realizar Análisis heurísticos y de comportamiento avanzados</td></tr>
<tr><td>22</td><td>Plataforma de Entrenamiento</td><td>La solución propuesta debe incluir formación en ciberseguridad dentro de la aplicación.
La solución propuesta debe dividir el entrenamiento en varios módulos, donde cada uno de los modulo debe estar en una serie de secciones.
Los módulos propuestos deben incluir teoría relevante y capacidad de realizar tareas interactivas en un entorno simulado.
La solución propuesta debe permitir descargar un certificado que acredite los logros una vez completadas todas las secciones de un módulo.
La solución propuesta debe ser 100% en nube
Los módulos propuestos deben ser de entrenamientos en ciberseguridad agnósticos entre los que se encuentren Respuestas a Incidentes, Software Malicioso, Aseguramiento de Directorio Activo y Seguridad para servidores, entre otros</td></tr>
<tr><td colspan="3">ALCANCE DE LOS SERVICIOS DE ANTIVIRUS</td></tr>
<tr><td>20</td><td>Instalación</td><td>Instalación/Revisión Consola en Sitio y configurada a las necesidades del Ministerio.
Lunes a viernes 8:00 AM a 6:00 PM. Este servicio se prestará cuando se requiera.

Instalación Consola en Sitio + solución de antivirus en las Estaciones de Trabajo.
Lunes a viernes 8:00 AM a 6:00 PM.</td></tr>
<tr><td>21</td><td>Inducción (Transferencia de conocimiento)</td><td>Transferencia de conocimiento presencial en la administración de las herramientas del antivirus ofertada: seis (6) horas en total para 4 funcionarios del área de sistemas de la entidad, en un horario comprendido de lunes a viernes 8:00 AM a 5:00 PM.
La Transferencia de conocimiento se debe desarrollar sobre las siguientes temáticas:
1. Administración de consola antivirus,
2. Instalación configuración pruebas y puesta en producción de los agentes de antivirus de acuerdo con la versión de los sistemas operativos que tiene en producción en los computadores del Ministerio.</td></tr>
<tr><td>22</td><td>Materiales de Apoyo</td><td>- Debe entregar: memoria USB con los Instaladores de antivirus, una memoria USB con los manuales del Fabricante antivirus.
-Debe entregar: Documento donde estén los sitios de consulta para Soporte del antivirus vía WEB.</td></tr>
<tr><td>23</td><td>Informe</td><td>Entrega de un informe mensual de las actividades realizadas.

TIEMPOS DE RESPUESTA Y SOLUCIÓN

<table>
<tr><th>Prioridad</th><th>Detalle</th><th>Tiempo Respuesta</th><th>Tiempo Solución</th></tr>
<tr><td>Crítico</td><td>Falla en la Consola de Kaspersky que hace imposible administrar la Solución Antivirus.

Protocolo se activará mediante llamada telefónica, si no es posible la solución, se procederá a solicitar visita en sitio.</td><td>Inmediata</td><td>Inmediata</td></tr>
<tr><td>Alto</td><td>Problema de Virus de gran impacto donde continúa operando la Solución de Kaspersky, pero de una manera imperfecta; impacto significante a MINISTERIO DEL INTERIOR. Que amenaza aspectos de Seguridad futura.
Visita en sitio.</td><td>2 horas</td><td>4 horas</td></tr>
</table>
</td></tr>
</table>

Medio	El producto antivirus Kaspersky continúa funcionando con impedimentos menores. Las tareas pueden continuar con una mínima disminución de performance. Visita en sitio y/o asistencia remota.	4 horas	8 horas
Bajo	Consulta técnica y/o de uso. Las tareas se desarrollan normalmente	8 horas	16 horas
Planificado	Implementación de una solicitud de cambios que no es requerida de manera urgente. Las tareas se desarrollan normalmente	Planificado	Planificado

CERTIFICACIÓN DEL FABRICANTE DEL SOFTWARE

CERTIFICACIÓN DEL FABRICANTE DEL ANTIVIRUS - KASPERSKY: El oferente debe presentar carta directa del fabricante en la que éste certifique que es distribuidor autorizado nivel platinum o gold en el territorio colombiano y que cuenta con ingenieros certificados para prestar soporte técnico del software antivirus requerido y la garantía, en caso de que el oferente resulte adjudicatario por toda la vigencia del contrato y la garantía. La certificación no debe superar una antigüedad mayor de 30 días hacia atrás desde la fecha del cierre del presente proceso de selección.

LA ENTIDAD se reserva el derecho de verificar la autenticidad de las certificaciones aportadas o de solicitar los respectivos contratos o documentos que la soporten, cuando lo considere necesario.

Personal Mínimo Requerido

Durante la ejecución del contrato se debe garantizar el personal idóneo para el desarrollo de mismo y contar con equipos y herramientas necesarios para la efectiva ejecución del objeto.

De acuerdo con lo anterior, el personal que se requiere para el desarrollo de objeto contractual es:

Personal Técnico "es obligación":

El oferente que resulte adjudicatario debe contar como mínimo con un (1) profesional en ingeniera de sistemas, electrónica y/o telecomunicaciones, y un (1) tecnólogo en sistemas, computación, electrónica y/o telecomunicaciones, ambos con tarjeta profesional, uno de los cuales al menos debe poseer las certificaciones que lo avalen como administrador sénior o su equivalente, en la administración e instalación de la solución ofertada.

El personal debe acreditar experiencia profesional en xxxxx, mediante certificaciones debidamente firmadas que incluyan objeto, obligaciones /o funciones, plazo de ejecución, fecha de inicio y fin, información de quien expide la certificación, y debe estar debidamente suscrita.

Asi mismo deberá aportar copia de las cédulas de ciudadanía, los títulos profesionales que acrediten su profesión y el certificado de antecedentes profesionales de su equipo de trabajo.

Las certificaciones que avalen a la persona como administrador senior o su equivalente deben ser emitidas directamente por el fabricante de la solución de antivirus ofertado.

GARANTÍA MÍNIMA EXIGIDA

El proponente deberá ofrecer para todo el plazo de ejecución del servicio, una licencia y soporte mínimo, así:

		DESCRIPCIÓN
		Un (1) año para renovación de licencia de antivirus Kaspersky, contado a partir de su instalación y su respectivo soporte técnico.
		El proponente avalará su cumplimiento, mediante certificación debidamente firmada por el representante Legal de la empresa.