ANEXO No 2
CONDICIONES TÉCNICAS

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
1.	**SOFTWARE DE ANTIVIRUS** **Marca: especificar por el oferente** **Referencia: especificar por el oferente**		
1.1	Se requieren el software de antivirus para setenta (70) equipos de cómputo, con las siguientes funcionalidades:		
1.2	El antivirus debe contar con un mecanismo de actualización frecuente de antimalware que garantice la integridad y minimice la manipulación o alteración de las definiciones de virus por medio de cifrado y firmas digitales.		
1.3	El antivirus debe permitir el acceso en demanda, en segundo plano, proactivo, sub-sistema de prevención de brotes de virus, análisis de phishing y filtrado de contenido, protección sobre los protocolos HTTP, HTTPS, FTP.		
1.4	La solución debe analizar tipo de archivo verdadero y eliminar si da el caso, archivos ejecutables con extensiones como: *.EXE, *.APP, *.VB, *.VBS, *.SCR, *.BAT, *.DLL, *.COM, *.BIN, *.EBS., entre otros que aprovechan los diferentes tipos de extensiones de un sistema operativo, camuflándose para afectar a los sistemas.		
1.5	La solución debe ejecutar detección de archivos con base al tipo y no solo a la extensión.		
1.6	Debe anticiparse a los virus desconocidos e intrusos mediante herramientas que supervisen los procesos en ejecución en busca de comportamientos maliciosos.		
1.7	Escanee sitios Web en busca de código malicioso; Control y Protección Web.		
1.8	Compruebe la reputación de los vínculos antes de navegar en ellos.		
1.9	Detecte y bloquee los vínculos de phishing que intentan robar información confidencial y datos financieros.		
1.10	Reconocimiento de anomalías, detección y bloqueo de ataques de tipo Host Sweep, TCP o UDP port Scan, CGI Holes.		
1.11	Utiliza técnicas de análisis avanzadas para comprobar si un sitio presenta las características típicas de las operaciones de phishing.		
1.12	La solución de antivirus debe soportar la instalación de los agentes en estaciones de trabajo, portátiles y equipos de cómputo. Así como garantizar la compatibilidad en los dispositivos mencionados.		
1.13	La protección antivirus debe tener compatibilidad con sistemas operativos Windows y Mac.		
1.14	La solución permite el monitoreo en tiempo real de los procesos en memoria para capturar los virus que son ejecutados en memoria sin necesidad de escribir el archivo.		
1.15	El módulo de comportamiento debe ser capaz de detectar amenazas de día cero tipo Ransomware		
1.16	Detección y reacción contra Ransomware que inicie el cifrado de información, así no se tenga firma de detección de malware para detenerlo. Este módulo debe terminar el proceso de cifrado malicioso de forma automática.		
1.17	Protección contra la explotación permitiendo finalizar programas que se identifiquen con comportamiento anormal asociado a ataques de Exploit.		
1.18	Evitar o monitorear que un programa con comportamiento sospechoso pueda duplicar o inyectar archivos.		
1.19	Evitar o monitorear que un programa con comportamiento sospechoso pueda incrustar complementos en los navegadores.		
1.20	Evitar o monitorear que un programa con comportamiento sospechoso pueda instalar librería del programa malicioso.		
1.21	Para aquellos programas válidos y que por su comportamiento el Antimalware no permita su ejecución, deberá de permitirlos agregándolos a una lista blanca.		
1.22	Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.		
1.23	Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.		
1.24	Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA).		
1.25	Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing).		
1.26	Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.		
1.27	Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo las potencialmente no deseadas (PUA).		
1.28	Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente y desinstalación de los componentes de protección.		
1.29	Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad		

	conocida.		
1.30	Debe ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.		
1.31	Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.		
1.32	Debe brindar protección de amenazas de día cero (0) a través de tecnología de deep learning (signature less).		
1.33	Debe tener la funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología de Deep Learning.		
1.34	Debe tener la capacidad de detección y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.		
1.35	Debe tener la capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.		
1.36	Debe detectar el malware en pre-ejecución un tiempo aproximado de no más de 20 milisegundos.		
1.37	No debe requerir descarga de firmas de ningún tipo para la parte de protección por comportamiento.		
1.38	Debe tener la capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.		
1.39	Debe contar con bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).		
1.40	Se debe garantizar la generación de excepciones ante falsos positivos.		
1.41	El software debe tener la capacidad de protección AMSI contra scripts maliciosos.		
1.42	El software debe poseer un IPS de Host.		
1.43	El software debe disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas.		
1.44	El software debe disponer de capacidad de remediación de la acción de encriptación maliciosa del ransomware.		
1.45	El software a instalar en equipos de cómputo debe disponer de capacidad de prevención contra la acción de cifrado malicioso ejecutado por ransomware, posibilitando el bloqueo de las computadoras de donde parte tal acción.		
1.46	El software debe contar con protección anti-ransomware para el sector de booteo.		
1.47	El software debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.		
1.48	Detección y protección de técnicas de explotación: Enforce Data Execution Prevention; Mandatory Address Space Layout Randomization; Bottom-up ASLR; Null Page (Null Deference Protection); Heap Spray Allocation; Dynamic Heap Spray; Stack Pivot; Stack Exec (MemProt); Stack-based ROP Mitigations (Caller); Branch-based ROP Mitigations (Hardware Assisted); Structured Exception Handler Overwrite (SEHOP); Import Address Table Filtering (IAF); Load Library; Reflective DLL Injection; Shellcode; VBScript God Mode; Wow64; Syscall; Hollow Process; DLL Hijacking; Squiblydoo Applocker Bypass; APC Protection (Double Pulsar / AtomBombing);		
1.49	El software debe garantizar la mitigación de inyección de códigos en procesos.		
1.50	El software debe garantizar la protección contra robo de credenciales.		
1.51	El software debe garantizar la protección contra malware escondido en aplicaciones legitimas (code cave).		
1.52	El software debe evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.		
1.53	El software debe evitar la escalada de privilegios y acceso elevado a recursos.		
1.54	El software debe evitar la modificación de las claves de registro para la ejecución de código		

	arbitrario.		
1.55	El software debe cumplir con todos los Ítems anteriores que apliquen a estaciones de trabajo bajo S.O. Windows.		
1.56	El antivirus debe tener la capacidad de analizar Scripts de Java y VBScript antes de que se ejecuten.		
1.57	El software debe controlar las actividades realizadas por aplicaciones vulnerables.		
1.58	El antivirus debe contar con tecnología de remoción y detección de virus, macros infecciosas, troyanos, gusanos informáticos, Keyloggers, Spyware y adware, Rootkits, Bots y otras amenazas. Mitigar ataques y neutralizar los objetos maliciosos por medio de tecnologías de desinfección a niveles bajos del sistema operativo de un equipo.		
1.59	El antivirus deberá ser estable, de tal manera que no afecte ni perjudique el rendimiento de las máquinas y/o aplicativos que estén instalados en las mismas.		
1.60	El antivirus debe contar y quedar configurado con un módulo de exploración en tiempo real, que ofrezca protección continúa frente a los virus que llegan a través de dispositivos de almacenamiento extraíbles, en la red y de las diversas fuentes en Internet.		
1.61	El antivirus debe tener la capacidad de explorar los procesos maliciosos que se encuentren corriendo en memoria.		
1.62	El antivirus debe correr con un recurso de CPU bajo para tareas de exploración en demanda		
1.63	El antivirus debe permitir y quedar configurado para tareas calendarizadas de revisión y limpieza del sistema de archivos.		
1.64	El software de antivirus debe poseer mecanismos o técnicas como buffer overflows que sirven como protección contra vulnerabilidades en memoria.		
1.65	El software debe consumir recursos mínimos de máquina.		
1.66	El software debe permitir en su configuración la exclusión del análisis de extensiones o ficheros no deseados. Esto desde su configuración local protegida por una contraseña.		
1.67	El antivirus debe explorar archivos descargados desde todas las plataformas de correo, análisis de Onedrive y/o de almacenamiento en la nube instalados por aplicaciones como Dropbox, Drive Gmail a las cuales se tiene acceso desde las estaciones de trabajo.		
1.68	El antivirus debe contar con un módulo de exploración bajo demanda que, permita iniciar una exploración en cualquier momento, especificar los objetivos (discos duros, carpetas, memoria, unidades extraíbles) y las exclusiones de la exploración, así como también determinar cómo debe responder el explorador cuando detecte un virus mostrando el informe detallado.		
1.69	El software debe garantizar un análisis por demanda en los dispositivos extraíbles y almacenamiento en línea, antes de tener acceso a ellos una vez conectados a los equipos de cómputo.		
1.70	El software debe garantizar la detección de ataques de tipo Exploits hacia vulnerabilidades de sistema operativo como también de aplicaciones diferentes de Microsoft.		
1.71	El software debe proporcionar un módulo de bloqueo de aplicaciones para proporcionar un mayor nivel de protección, seguridad y control a los usuarios.		
1.72	El antivirus deberá permitir la desactivación del agente por medio de una contraseña, en caso de que se requiera o necesite.		
1.73	El software deberá entregar contexto de la amenaza detectada mediante la visualización de todo el ataque, como inicio y como se comportó. Debe proveer detalle de los equipos involucrados en el ataque tales como llaves de registro, procesos y conexiones de red.		
1.74	El software debe proveer respuesta automática a incidentes como actividades de limpieza del endpoint hasta obtener su estado de salud original.		
1.75	El software debe explorar múltiples formatos de compresión de archivos como: (zip, rar, tar, gzip entre otros).		
1.76	El software debe tener la capacidad de explorar los procesos que se encuentren corriendo en memoria.		
1.77	El software debe ser capaz de detectar y bloquear ataques de fileless basados en PowerShell, Windows Management Instrumentations (WMI), VBScript y System Exploits para las plataformas cliente y servidores soportadas por Microsoft.		
1.78	El software debe ser capaz de retornar el sistema a un estado saludable, mediante técnicas de remediación de archivos que eventualmente puedan llegar a ser modificados durante la ejecución de una amenaza.		
1.79	El motor de exploración del software deberá utilizar distintas tecnologías de detección de virus: Exploración de firmas y exploración heurística “busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos”.		
1.80	El software debe permitir la toma de decisiones correctas sobre la ejecución de archivos y personalizar las directivas o políticas, en función del nivel de tolerancia al riesgo.		
1.81	El software debe tener soporte para comunicaciones bajo IPv6		
1.82	El software debe avisar sobre los posibles conflictos que existan con otros de antivirus y firewall instalados previamente en la máquina.		
1.83	El software debe poder restringir completa o parcialmente el acceso a la consola cliente para configurar parámetros individuales sobre el host.		

1.84	El software debe permitir configurar idioma dentro de la aplicación, entre ellos idioma español.		
1.85	El software debe poder configurar acciones sobre infecciones identificadas: Denegar acceso / limpiar / Eliminar / Ninguna.		
1.86	El software debe ofrecer opciones de envío de infecciones a cuarentena y ejecutar acciones sobre ítems enviados allí.		
1.87	El software debe poder habilitar la opción de escaneo de clic-derecho sobre carpetas específicas en sistemas operativos soportados.		
1.88	El software debe contar con características de protección para navegadores web (Active X) o detecciones que se realicen por comportamiento.		
1.89	El software debe permitir la detección basada en el comportamiento anómalo en el punto final.		
1.90	El software debe emplear una arquitectura multicapa, para defenderse de ataques basados en comportamientos, evitando cambios a nivel de sistema, restringiendo el acceso a procesos, archivos, recursos compartidos, valores y claves de registro específicos.		
1.91	El software debe poder identificar patrones similares de comportamiento dentro de diferentes variantes, usando reglas que pueden configurarse para evitar la instalación y / o la carga de nuevas variantes históricas, actuales y en evolución de amenazas de día cero.		
1.92	El software debe ser compatible con todas las versiones de los navegadores Internet Explorer, Google Chrome, Mozilla Firefox.		
1.93	El software debe garantizar en las estaciones de trabajo protección contra infecciones a través descargas de internet, archivos adjuntos de e-mail, redes, archivos compartidos, CD-ROM, USB, dispositivos extraíbles, carpetas públicas y carpetas personales de todo tipo de correo, almacenadas localmente, mensajes de correo electrónico entrante y saliente, servicios en línea, entre otros tipos de almacenamiento.		
1.94	El software debe ser capaz de detectar el 100% de los virus conocidos (reportados en listas), contra programas malignos especificados.		
1.95	El software debe contar con mecanismos de borrado seguro de malware residentes en memorias que sean difíciles de erradicar, evitando el reinicio, en caso de no contar con la herramienta, deberá prever que el técnico experto en antimalware esté presente en el reinicio del equipo de cómputo verificando y garantizando la erradicación del mismo.		
1.96	El software debe contar con tecnología de mitigación de EXPLOITS, que ataquen soluciones comúnmente usadas y que pueden no estar actualizadas, como Acrobat, Flash Player, entre otras.		
1.97	El software debe contar con mecanismos de detección de ausencia de configuraciones y/o parches específicos de sistema operativo.		
1.98	El software debe ofrecer una solución para controlar dispositivos en sistemas operativos Windows (32/64 bits).		
1.99	El software debe permitir la limpieza de amenazas dentro archivos adjuntos (JavaScript dentro de archivos PDF o Microsoft Word, por ejemplo).		
2	**SOFTWARE CONGELADOR DE DISCO** **Marca: especificar por el oferente** **Referencia: especificar por el oferente**		
2.1	Se requieren software de congelar discos para setenta (70) equipos de cómputo, con las siguientes funcionalidades:		
2.2	El contratista debe proveer el software permita protección avanzada para estaciones de trabajo de sistema operativo Windows 7, 8 a 10 en sus últimas versiones estables. La cual debe garantizar que se preserve la configuración, actualizaciones del sistema operativo (Update) y base de datos de antivirus.		
2.3	El software debe garantizar que cada vez que se reinicie el equipo el software debe restaurar la configuración.		
2.4	El software debe proporcionar a los usuarios un acceso ilimitado a los cambios de configuración permanentes.		
2.5	El software debe evitar los cambios de configuración, permitiendo a los usuarios guardar su trabajo sin que se altere la configuración de base de los equipos.		
2.6	El software debe garantizar la eliminación de las amenazas de día cero, garantizando reversar todos los cambios maliciosos realizados en el sistema, incluidas las amenazas día cero.		
2.7	El contratista debe garantizar que el software no degrade el rendimiento de los equipos.		
2.8	El software debe garantizar la eliminación de todo el software instalado sin autorización, al momento de reiniciar el equipo.		
2.9	El software debe permitir el reinicio sin borrado de la configuración y un reinicio borrando la configuración del equipo.		
2.10	El software debe garantizar el 100 % de recuperación de las estaciones de trabajo al reiniciar.		
2.11	El software debe proporcionar la protección con contraseña y seguridad completa para el acceso a la configuración.		
2.12	El software debe proteger el registro de arranque maestro (MBR), los múltiples discos duros y particiones del equipo.		

2.13	El software debe admitir discos duros SCSI, ATA, SATA e IDE.		
2.14	El software debe admitir discos FAT, FAT32, NTFS, básicos y dinámicos.		
2.15	El software debe permitir preseleccionar unidades a congelar y, de forma selectiva, cuáles deben ser congeladas o descongeladas unidades fijas.		
2.16	El software debe tener la opción de instalación silenciosa para una conexión rápida como parte de una imagen maestra o implementación por demanda.		
2.17	Creación de ThawSpaces visibles u ocultos en una estación de trabajo para almacenar programas, guardar archivos o realizar cambios permanentes.		
3	**SOFTWARE VPN** **Marca: especificar por el oferente** **Referencia: especificar por el oferente**		
3.1	Se requieren el software VPN de EndPoint para setenta (70) equipos de cómputo, con las siguientes funcionalidades:		
3.2	El software debe proporcionar a los usuarios la conexión a sus dispositivos a través de ubicaciones de servidores iguales o mayores a 60 países.		
3.3	El software de VPN no debe recopilar ni compartir datos privados, y por ningún motivo hacer seguimiento de ellos. De igual forma no debe registrar datos de tráfico o solicitudes a DNS		
3.4	El software de VPN no debe realizar control del ancho de banda. Este debe garantizar un ancho de banda ilimitado.		
3.5	El software de VPN debe garantizar el enmascaramiento de la dirección IP en todo momento.		
3.6	El software de VPN debe contar con Kill Switch automático. Lo que significa que, si se bloquea accidentalmente una conexión VPN, la función Kill Switch impide que tu dispositivo acceda a la web., mediante el bloqueo de tráfico en internet hasta su restauración.		
3.7	El software de VPN actuará como un proxy, para su actividad web: en lugar de la dirección IP y ubicaciones reales, las páginas web que se vayan a visitar solo verán la dirección IP y la ubicación del servidor VPN.		
3.8	El software de VPN garantizará la protección a la conexión entre el cliente y el servidor utilizando tunelización y cifrado (protocolo AES- 256 bits)		
3.9	El software de VPN debe garantizar como mínimo los siguientes protocolos: IKEv2, L2TP/IPsec, OpenVPN, Lightway.		
3.10	El software de VPN debe contar con soporte 7x24 con chat en vivo.		
3.11	El software de VPN debe permitir el cambio ilimitado de servidores de conexión.		
3.12	El software de VPN debe operar son sus propios DNS, los cuales deben manejar tráfico cifrado.		
3.13	El software de VPN debe brindar protección de fugas de DNS y WebRTC.		
3.14	El software debe brindar un informe de errores, test de velocidad y la opción de escoger el más rápido.		
3.15	El software de VPN debe poseer la opción de evitar la detección de la dirección IPv6 mientras se esté conectado.		
4	**SOFTWARE DE HIPERVISOR DE MÁQUINA VIRTUAL** **Marca: especificar por el oferente** **Referencia: especificar por el oferente**		
4.1	Se requieren el software hipervisor de máquina virtual para treinta (30) equipos de cómputo, con las siguientes funcionalidades:		
4.2	Soporte básico por un año de suscripción.		
4.3	El software hipervisor deberá permitir crear máquinas virtuales hasta de 16 CPU, 64 GB de RAM, 3 GB de vRAM).		
4.4	Posibilidad de crear VM restringidas con fecha y hora de caducidad predefinidas.		
4.5	El software hipervisor de máquina virtual deberá tener compatibilidad con DirectX 11 y gráficos 3D acelerados con OpenGL 4.1, una nueva interfaz de usuario con modo oscuro, compatibilidad con el modo Hyper-V de Windows en hosts Windows 7, Windows 10, y las últimas versiones estables en el mercado.		
4.6	El software hipervisor de máquina virtual deberá permitir: Crear nuevas máquinas virtuales. Convertir PC en máquina virtual.		
4.7	El software hipervisor de máquina virtual deberá tener integración de host/invitado: Uso compartido de archivos de host/invitado. Carpetas compartidas/reflejadas. SSH de un solo clic a máquina virtual Linux. Ejecutar máquinas virtuales con distintos modos de visualización. Modo de visualización unificado (solo para sistemas Windows invitados).		
4.8	El software hipervisor de máquina virtual deberá tener compatibilidad con: Compatibilidad con una amplia gama de dispositivos virtuales. Compatibilidad con lector de tarjetas inteligentes USB.		

	Compatibilidad con dispositivos USB 3.1 Compatibilidad con dispositivos de asistencia. Dispositivo de módulo de plataforma segura virtual. Dispositivo NVMe virtual.		
4.9	El software hipervisor de máquina virtual deberá tener funciones de seguridad como: Compatibilidad con seguridad basada en la virtualización de Microsoft (invitado). Módulo de plataforma segura virtual (vTPM). Compatibilidad con arranque UEFI. Compatibilidad con arranque seguro UEFI. Procesador de gráficos en el entorno de pruebas de la GPU Instantánea. Crear y gestionar máquinas virtuales cifradas.		
4.10	El software hipervisor de máquina virtual deberá tener funciones específicas de host Windows: Host de Windows 10. Motor de representación DX12. Compatibilidad con el modo Hyper-V (Device Guard, WSL). Compartir máquina virtual (servidor de Workstation).		
4.11	El software hipervisor de máquina virtual deberá tener Funciones avanzadas: Operación desde la línea de comandos: vmrun y VIX. Personalización de redes virtuales (NAT, cambio de nombre de red). Simulación de redes virtuales (pérdida de paquetes, latencia, ancho de banda). Conectar con el servidor ESXi. Creación de clones asociados. Creación de clones completos. Cifrar máquinas virtuales.		
4.12	El software hipervisor de máquina virtual deberá tener version comercial y de prueba.		
4.13	El sistema debe contar con un soporte y actualizaciones por un periodo mínimo de 1 año.		
4.14	El software hipervisor de máquina virtual deberá ser la última versión disponible por el fabricante y en el evento que el fabricante genere nuevas actualizaciones o versiones, el proveedor deberá suministrar el licenciamiento para ejecutar la última versión disponible y estable del hipervisor de máquina virtual.		
4.15	El contratista deberá entregar una certificación directamente emitida por el fabricante, en donde conste que el software adquirido por la entidad tiene suscripción de uso por el término de (1) año contado a partir de la entrega del software al supervisor del contrato.		
4.16	El contratista deberá garantizar que las mejoras de software a nuevas versiones (más recientes), releases y parches, entre otros, son de una versión igual o superior a las últimas versiones liberadas por la casa matriz en el mercado colombiano.		
4.17	El contratista deberá hacer entrega del software objeto del contrato, previa suscripción del acta de inicio y durante el plazo de ejecución del contrato.		
5	**SERVICIOS DE IMPLEMENTACIÓN**		
5.1	Los softwares ofertados deberán ser instalados, configurados y puestos en funcionamiento en las instalaciones de la Dirección de Inteligencia Policía ubicada en la Av. Boyacá 142ª 55 por el contratista		
6	**ASISTENCIA TÉCNICA Y GARANTÍA**		
6.1	El contratista deberá brindar soporte técnico de los softwares por un periodo de un año, contado a partir de la firma del recibido a satisfacción del supervisor del contrato por concepto de los softwares, donde se certifique la entrega de los softwares adquiridos mediante el presente proceso contractual.		
6.2	El servicio de soporte debe ser telefónico/sitio web y darse directamente por el contratista para todos los niveles de prioridad de los incidentes, problemas, inquietudes, dudas que se reporten durante el término de vigencia del contrato.		
6.3	En caso de existir urgencia respecto a incidentes que involucren las soluciones ofertadas, el contratista deberá proporcionar en caso de necesitarlo apoyo de casa matriz (presencial) hasta solucionar el incidente.		
6.4	El soporte de los softwares será 7x24 con un tiempo de respuesta no superior a 2 horas por parte del contratista. Los softwares deben contar con un soporte que permita accesos directos a los especialistas de producto cuando sea requerido por los diferentes medios de atención por parte de la dirección de inteligencia policial.		
7	**TRANSFERENCIA DE CONOCIMIENTOS**		
7.1	El contratista deberá incluir una transferencia de conocimientos de cuatro (4) horas virtuales, para dos (2) funcionarios, en el manejo, instalación y operación del software de antivirus, congelador de disco, hipervisor de máquina virtual y red privada virtual (VPN).		
8	**ASPECTOS DE CONFIDENCIALIDAD**		
8.1	El personal que realice la instalación y configuración de los productos ofertados deberá someterse a un estudio de seguridad realizado por la Dirección de Inteligencia de la Policía Nacional, durante la vigencia del contrato.		
8.2	En virtud del presente estudio previo, el contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato; así como sobre los		

	lugares a los cuales tenga acceso con ocasión de su desarrollo. El oferente deberá diligenciar el formulario acuerdo de confidencialidad.		
8.3	La Dirección de Inteligencia Policial de la Policía Nacional - DIPOL se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin de garantizar la transparencia del proceso de contratación.		
9	**NIVEL EDUCATIVO**		
9.1	El funcionario que realizará la instalación y configuración de los softwares, deberán ostentar el título de tecnólogo o ingeniero en Sistemas y/o Electrónico y/o a fines, para lo cual el oferente deberá presentar con la oferta, copia del diploma y/o acta de grado del título de dicho funcionario		
9.2	La Dirección de Inteligencia Policial de la Policía Nacional – DIPOL podrá solicitar el cambio del personal ofrecido en cualquier momento a partir de la suscripción del contrato y el mismo podrá ser sustituido por el proponente por uno con iguales o mejores capacidades, condiciones y calificaciones a las presentadas en la oferta.		
10	**EXPERIENCIA DEL PERSONAL**		
10.1	Con el fin de garantizar la idoneidad del funcionario encargado de las actividades de instalación, configuración de los software de antivirus, congelador de discos, hipervisor de máquina virtual, red privada virtual (VPN) e hipervisor de máquina virtual ofertada, el proponente deberá certificar que esta persona cuente con experiencia en Colombia de haber participado mínimo en un (1) proyecto relacionado con el objeto del presente contrato; para lo cual el oferente debe anexar a la propuesta, una (1) certificación de proyectos en los cuales haya participado, expedidas por el oferente, durante los últimos tres (3) años anteriores a la fecha de apertura del presente proceso.		
11	**DOCUMENTACIÓN TÉCNICA – ENTREGABLES**		
11.1	El contratista debe entregar los manuales de uso en idioma español.		
11.2	Toda la documentación debe entregarse en idioma español.		
12	**EXPERIENCIA DEL OFERENTE**		
12.1	Con el fin de garantizar la calidad de los bienes a contratar y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en la venta software similares al objeto del presente estudio previo, tal acreditación será avalada con la presentación de certificaciones que acrediten la participación en contratos suscritos en los últimos tres (03) años (2019 y/o 2020 y/o 2021) con empresas públicas o privadas para lo cual el oferente deberá presentar máximo tres (03) certificaciones expedidas por la entidad que adquirió los software, con concepto favorable de la recepción de los servicios cuya suma o valor individual sea igual o superior al 100% del presupuesto oficial asignado.		
13	**REQUERIMIENTOS AMBIENTALES**		
13.1	El contratista deberá entregar los manuales de manera digital con el fin de aportar a la política de cero papeles establecida en directiva presidencial 04/2012.		
14	**SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO**		
14.1	El contratista aplicará el protocolo de bioseguridad establecido en la Dirección de Inteligencia Policial, teniendo en cuenta lo establecido por el Ministerio de Salud y Protección Social, a través de la Resolución 0000223 del 25/02/2021 “Por medio de la cual se modifica la Resolución 000666 del 24!04/2020 en sentido de sustituir el anexo técnico” y la Resolución 777 del 02/07/.2021 “Por la cual se definen los criterios y condiciones para el desarrollo de las actividades económicas, sociales y del estado y se adopta el protocolo de bioseguridad para la ejecución de estas”.		
14.2	El contratista deberá entregar los documentos que evidencien objetivamente, la afiliación a la Seguridad Social Integral del personal que ejecutará el objeto contractual, (E.P.S., A.F.P., A.R.L., C.C.F.), obligándose a mantener dicha afiliación, durante la totalidad del tiempo necesario para la ejecución de la actividad contratada.		
14.3	El contratista correrá con los gastos médicos, de hospitalización y procedimientos médicos a que haya a lugar, en caso de que uno de sus funcionarios sufra un accidente laboral durante la ejecución del presente contrato.		
14.4	En caso de presentarse un accidente de trabajo dentro de las instalaciones de la Dirección de Inteligencia, le corresponde al contratista realizar el respectivo reporte e investigación dentro del tiempo reglamentario, presentará una copia de la documentación al Grupo de Seguridad y Salud en el Trabajo de la Dirección de Inteligencia Policial, según lo establecido en la Resolución 1401 del 14 mayo de 2007 o cualquiera que la modifique, reemplace o sustituya.		
14.5	El contratista deberá colaborar en las auditorias de cumplimiento al Sistema de Gestión de Seguridad y Salud en el Trabajo, que se realicen en el centro de trabajo donde se encuentre desempeñando las actividades		

CUMPLIMIENTO ESPECIFICACIÓN TÉCNICA.

PROPONENTE _____

Declaramos bajo nuestra responsabilidad personal, y comprometiendo la responsabilidad institucional de las personas jurídicas que representamos, que cumplimos en su totalidad con las especificaciones técnicas de verificación y de obligatorio cumplimiento

REQUISITOS GENERALES

a. Las especificaciones técnicas requeridas son de obligatorio cumplimiento, de no hacerlo la propuesta se considerará no apta técnicamente.

b. En la columna **CUMPLE / NO CUMPLE**, se evaluará las especificaciones técnicas ofertadas por la firma.

Firma Representante Legal _____
C.C. N° _____