Las especificaciones técnicas mínimas requeridas son de obligatorio cumplimiento (excluyentes), por tal motivo el proponente deberá indicar con una "X" y de no hacerlo, la propuesta se considerará no apta técnicamente y debe diligenciarse con las especificaciones técnicas ofertadas.

En una columna CUMPLE/NO CUMPLE, el comité técnico de la Policía Nacional designe, evaluara las especificaciones técnicas ofertadas por la firma.

El oferente deberá cumplir estrictamente con las especificaciones solicitadas atendiendo los factores descritos a continuación:

ITEM	CONDICIONES TECNICAS MINIMAS	CUMPLE	NO CUMPLE
1.	**LA SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM**		
1.1	El contratista deberá suministrar una (1) solución con soporte para cuarenta y cinco mil (45.000) equipos de cómputo (que soporte Sistema Operativo Windows, Linux y Macintosh) para uso continuo con derecho a actualizaciones y nuevas versiones (upgrade) por un término de dieciocho (18) meses y que cumpla las siguientes características: • Cuarenta y cinco mil (45.000) deben contar con módulo de Antivirus, Control de Dispositivos, Control de Aplicaciones y Data Lost Prevention (DLP) • Quince mil (15.000) debe contar con módulo de y Cifrado de Disco Duro • Veinte mil (20.000) de antispam para buzones de correo on-premise. La funcionalidad de la consola de administración antivirus, funcionalidad modulo antivirus en Windows server y Linux, La solución para estaciones de trabajo deben ser cumplidas por las cuarenta y cinco mil (45.000) licencias, estas deben ser administradas desde ambientes web, la diferencia en módulos se debe a las funcionalidades de cada uno de los equipos de cómputo, sus sistemas operativos y el nivel de riesgo al que se encuentran expuestos.		
2.	**MÓDULO ANTIVIRUS Y CONTROL DE DISPOSITIVOS**		
2.1	La solución debe ser desplegada mediante un agente.		
2.2	La protección antivirus debe tener compatibilidad con los sistemas operativos Windows, Linux y Macintosh, incluyendo las nuevas versiones y estaciones de trabajo (45.000), incluyendo servidores de archivos Linux y una herramienta de administración y gestión remota, adicionalmente la solución deberá realizar la identificación de equipos no gestionados y la instalación de la solución en los mismos.		
2.3	El módulo debe ser instalado en cuarenta y cinco mil (45.000) nodos, configurado y deberá quedar funcionando correctamente en los servidores Windows, Linux, así como en los clientes Windows, Linux en las versiones de 32 y 64 bits y Macintosh en las diferentes versiones con los que cuenta la Policía Nacional.		
2.4	La solución de antivirus debe ser además compatible con sistemas Linux CentOS, RedHat, SUSE y Ubuntu.		
2.5	Las políticas de antivirus definidas desde la consola deben poder ser aplicables para cualquier sistema operativo soportado. No se aceptará tener que definir políticas diferentes para diferentes sistemas operativos.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
2.6	La solución debe contar con un mecanismo de actualización que garantice la integridad y minimice la manipulación o alteración de las definiciones de virus por medio de cifrado y firmas digitales. Esta función deberá ser implementada y estabilizada en la solución para la Policía Nacional.		
2.7	La solución debe contar con tecnología de remoción y detección de virus, macros, troyanos, gusanos, ransomware y en general todo tipo de códigos maliciosos. Esta función deberá ser implementada y estabilizada en la solución para la Policía Nacional.		
2.8	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, la solución se debe instalar y en máquinas con recursos limitados.		
2.9	La solución debe permitir el aseguramiento de archivos, carpetas, elementos compartidos y evitar el desbordamiento de buffer. Esta función deberá ser implementada y estabilizada en la solución para la Policía Nacional.		
2.10	La solución debe permitir el acceso en demanda, en segundo plano, proactivo, subsistema de prevención de brotes de virus y filtrado de contenido, protección sobre los protocolos HTTP, HTTPS, FTP y SMTP.		
2.11	La solución 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.		
2.12	La solución debe tener la capacidad de explorar los procesos que se encuentren corriendo en memoria.		
2.13	La solución debe tener el control de la utilización de la CPU para tareas de exploración en demanda.		
2.14	La solución debe explorar múltiples formatos de compresión de archivos como: (zip, rar, tar, gzip entre otros).		
2.15	La solución debe permitir y quedar configuradas tareas calendarizadas de revisión y limpieza del sistema de archivos.		
2.16	La solución debe tener la capacidad de analizar Scripts de Java y VBScript antes de que se ejecuten.		
2.17	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.		
2.18	El antivirus debe permitirle al administrador las opciones de preguntas en cuanto a limpiar, borrar, denegar acceso, e inclusive debe manejar una carpeta de cuarentena para archivos infectados que se detecten a través de reglas y lista predefinidas y/o personalizadas por el administrador.		
2.19	El motor de exploración deberá utilizar distintas tecnologías de detección virus: Exploración de firmas y exploración heurística "busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos".		
2.20	La solución debe utilizar detección mediante técnica heurística que permita desenmascarar las amenazas evasivas mediante la combinación de análisis de reputación, con la clasificación dada por el aprendizaje automático y modelos de comportamiento.		
2.21	La solución debe permitir la restauración automática de cambios que pudieran ser ejecutados por elementos considerados maliciosos.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
2.22	Por cada producto debe entregarse una versión vigente en el mercado y soportada por la casa matriz.		
2.23	La solución debe tener soporte para comunicaciones bajo IPv6 y soporte para IPv6 Firewall toda vez que IPv6 es una migración tecnológica que se debe llevar a cabo sobre las arquitecturas actuales.		
2.24	La solución debe poder detectar comunicaciones a sitios de comando y control con el fin de evidenciar pérdidas de información en los clientes.		
2.25	La solución debe contar con los mecanismos de protección para no poder ser desinstalada o desactivada por el usuario.		
2.26	La solución debe avisar sobre los posibles conflictos que existan de la solución a otras soluciones de antivirus y firewall instalados previamente en la máquina.		
2.27	Se deben poder habilitar o deshabilitar los módulos de protección sin ser desinstalados del sistema.		
2.28	La solución debe poder desplegar una aplicación cliente STANDALONE que pueda gestionar cambios localmente en caso de que se necesite.		
2.29	Se debe poder restringir completamente o parcialmente el acceso a la consola cliente para configurar parámetros individuales sobre el host.		
2.30	La desinstalación de la aplicación puede ser protegida mediante contraseñas desplegadas por políticas configuradas por el administrador.		
2.31	Puede existir más de una configuración de idioma para la aplicación cliente.		
2.32	La solución debe permitir a los administradores configurar escaneos bajo demanda en modo "escanear en reposo", para que se ejecuten sólo cuando el sistema esté inactivo.		
2.33	El fabricante debe contar con centros de investigación globales con el objetivo de detectar incidentes en diferentes países/regiones y compartir inteligencia de amenazas con la organización.		
2.34	La solución debe basarse en una plataforma común sobre la cual se incorporan módulos de Prevención de Amenazas, y Firewall de escritorio, y que permita el intercambio de información entre cada uno de los módulos.		
2.35	La solución debe poder configurarse para realizar escaneos por demanda o programados, desde la consola de administración o desde la consola cliente. Dichos análisis pueden ser ejecutados en diferentes niveles de agresividad y umbral de consumos de recursos máximo sobre el sistema.		
2.36	Se debe poder configurar acciones sobre infecciones identificadas: Denegar acceso / limpiar / Eliminar / Ninguna.		
2.37	Se deben reportar eventos de amenazas directamente sobre la consola cliente y visibles desde la consola de administración de la solución.		
2.38	La solución debe poder habilitar la opción de escaneo de clic-derecho sobre archivos y carpetas específicas.		
2.39	Debe contar con mecanismos de protección de Exploits Generic Buffer Overflow Protección (GBOP) o integración con Microsoft DEP (Data Execution Prevention).		
2.40	La solución debe contar con características de protección para navegadores web (Active X).		
2.41	La solución debe contar con mecanismos de protección a ejecución de scripts maliciosos de Internet Explorer, sean JavaScript o VBScript.		
2.42	La solución debe poder configurar mediante reglas o políticas de protección de: • Entradas y llaves de registro de Windows. • Prevención de creación de ejecutables portables (.INI, .PIF)		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
	• Creación de archivos autorun • Prevención de uso de archivos TFTP (Trivial File Transfer Protocol) • Contra lectura de archivos en cache de navegadores de internet • Creación y modificación remota de archivos o carpetas • Acceso remoto de archivos o carpetas. .EXE, .BAT y otros ejecutables bajo la llave de registro HKEY_CLASSES_ROOT • Modificación de procesos Core de Windows • Modificación de configuraciones de exploradores y navegadores web • Proteger procesos con subreglas personalizadas Asignar las reglas por nombre de usuario.		
2.43	Utilizar modelos locales de aprendizaje en combinación con la clasificación de aprendizaje dada desde la nube, para identificar rápidamente el malware de día cero y comenzar la remediación.		
2.44	El sistema debe permitir la detección basada en el comportamiento anómalo en el punto final.		
2.45	Contener aplicaciones desconocidas impidiéndoles realizar cambios a nivel del sistema, mediante reglas de Protección de acceso a aplicaciones y monitoreo de procesos en ejecución desconocidos.		
2.46	La solución 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.		
2.47	La solución 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.		
2.48	La solución debe ser compatible con versiones soportadas de los navegadores Internet Explorer, Google Chrome, Mozilla Firefox.		
2.49	Disponer de un motor antimalware que detecte infecciones y analice virus, gusanos, spyware, malware, ransomware y otras amenazas ubicadas en las estaciones de trabajo.		
2.50	Debe estar diseñado para optimizar el rendimiento de los equipos y el consumo de ancho de banda.		
2.51	Proteger las estaciones de trabajo 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.		
2.52	La solución debe ser instalada, configurado y gestionado en cada estación de forma centralizada desde los servidores, sin tener que hacer un despliegue uno a uno.		
2.53	La solución debe tener la capacidad de generar exclusiones por nombre de archivos, carpetas y tipos de archivos.		
2.54	Debe contar con medidas de seguridad para que el usuario o cliente no pueda modificar políticas corporativas efectuadas desde la consola de administración.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
2.55	La solución debe ser capaz de detectar el 100% de los virus conocidos (reportados en listas), contra programas malignos especificados.		
2.56	Debe anticiparse a los virus desconocidos e intrusos mediante herramientas que supervisen los procesos en ejecución en busca de comportamientos maliciosos.		
2.57	La solución de protección de endpoint debe tener la capacidad de detectar, detener y eliminar códigos o aplicaciones maliciosas como: gusanos, troyanos, spyware, ad-ware, keyloggers, ramsonware y cualquier otro programa potencialmente peligroso.		
2.58	Debe permitir generar informes detallados con los datos referentes a la detección de virus tanto en tiempo real, como del análisis bajo demanda y programado.		
2.59	Análisis en tiempo real de amenazas sobre los dispositivos extraíbles antes de tener acceso a los archivos en ellos almacenados.		
2.60	La solución debe contar con mecanismos de protección de amenazas avanzadas tipo ransomware.		
2.61	La solución debe contar con mecanismos de borrado seguro de malware residente en memoria que sean difíciles de erradicar, evitando el reinicio de servidores críticos.		
2.62	La solución debe contar con tecnología de prevención/mitigación de EXPLOITS, que ataquen soluciones comúnmente usadas y que pueden no estar actualizadas, como acrobat, flash player, entre otras.		
2.63	La solución debe mitigar la explotación de vulnerabilidades sobre sistemas operativos cliente y servidor.		
2.64	La solución debe contar con mecanismos que permitan prevenir un evento destinado a aprovechar la ausencia de configuraciones y/o parches específicos de sistema operativo.		
2.65	La solución debe contar con funcionalidades de detección de amenazas avanzadas sin necesidad de requerir actualizaciones frecuentes de firmas de virus, de manera que se pueda garantizar la protección en máquinas que se encuentren desconectadas de la red la policía y/o internet por largos periodos de tiempo.		
2.66	La solución debe contar con la aplicación de políticas de acuerdo con la identificación de la red a la cual se encuentre conectada la máquina.		
2.67	La solución o servicio ofrecido deberá realizar la desinstalación de los productos de protección actualmente instalados sobre los dispositivos de la organización en caso de ofrecer una solución o versión de producto diferente a la utilizada.		
2.68	El módulo de Control de Dispositivos debe permitir la creación de excepciones para un usuario, maquina o dispositivo especifico.		
2.69	El módulo de Control de Dispositivos debe permitir asignar reglas y políticas para usuarios y grupos de Directorio Activo.		
2.70	El módulo de Control de Dispositivos debe tener la capacidad de monitorear las actividades del usuario relacionadas al dispositivo removible de manera silenciosa.		
2.71	El módulo de Control de Dispositivos debe tener la capacidad de bloquear los dispositivos de almacenamiento extraíbles, incluyendo CD / DVD y USB entre otras.		
2.72	El módulo de Control de Dispositivos debe tener la capacidad de bloquear los dispositivos "Plug and Play".		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
2.73	El módulo de Control de Dispositivos debe tener la capacidad de poner como de solo lectura a los dispositivos de almacenamiento removible.		
2.74	El módulo de control de dispositivos debe tener la capacidad de integrarse con el módulo de cifrado.		
2.75	El módulo de Control de Dispositivos debe permitir la creación de categorías de dispositivos a necesidad/personalizados.		
2.76	La solución debe permitir compartir de forma instantánea la información sobre amenazas con otras soluciones de seguridad conectadas, incluidas las de terceros.		
2.77	La solución de Control de Dispositivos debe permitir la protección de toda la red contra acceso y uso de los dispositivos USB, permitiendo solo los autorizados por la organización.		
2.78	El módulo de Control de Dispositivos debe permitir auditar la conectividad de los dispositivos de almacenamiento externo.		
2.79	El módulo de Control de Dispositivos debe poder ser desplegado de manera centralizada, a través de la consola de administración o a través de herramientas de distribución de software suministrada.		
2.80	El módulo de Control de Dispositivos debe tener la capacidad de inspeccionar en tiempo real, la carga de información hacia un medio removible, con el objetivo de identificar documentos confidenciales y tomar acciones tales como bloqueo, registro, notificación.		
2.81	El módulo de Control de Dispositivos debe permitir la creación y manejo de listas blancas y negras de dispositivos tomando en cuenta atributos tales como VID (Vendor ID) y PID (Product ID).		
2.82	El módulo de Control de Dispositivos debe tener la capacidad de permitir los dispositivos de almacenamiento removible al menos que se encuentren permitido a través de listas blancas.		
3. FUNCIONALIDAD MÓDULO ANTIVIRUS EN WINDOWS SERVER Y LINUX			
3.1	Disponer de un motor antimalware o antispyware que detecte infecciones y analice virus, gusanos, y otras amenazas ubicadas en los servidores.		
3.2	La remediación o creación de firmas para las amenazas de día cero no deberán superar veinticuatro (24) horas una vez reportada al fabricante.		
3.3	Actualización diaria, incremental y automáticamente, así como patrones de comportamiento de los nuevos virus.		
3.4	Gestión centralizada y remota de la red con múltiples vistas gráficas de los servidores para un fácil reparto de las tareas entre los administradores.		
3.5	Exclusión del análisis en base a extensiones o ficheros que no se desee ser analizados.		
3.6	Debe permitir definir el umbral de consumo de recursos del sistema analizado al momento de programación un análisis del sistema.		
3.7	Debe realizar el análisis de archivos comprimidos por demanda.		
3.8	En los casos que un fichero no se pueda desinfectar, en análisis de tiempo real o bajo demanda, debe permitir borrar y/o enviar a cuarentena dicho fichero.		
3.9	Debe disponer de un producto especializado para ser implementado en los servidores virtuales existentes en infraestructura tecnológica de la Policía Nacional (Oracle, Hyperv). que suman 200 servidores virtuales y 200 físicos.		
3.10	Debe quedar instalado en los servidores de archivos y sharepoint.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
4. FUNCIONALIDAD DE LA CONSOLA DE ADMINISTRACIÓN ANTIVIRUS			
4.1	Despliegue, actualización, administración y soporte a toda la solución de seguridad ofertada; funcionalidades que deben efectuarse a través de una consola de gestión de políticas de seguridad y tareas.		
4.2	Debe interactuar con las consolas de administración que tiene actualmente la Policía Nacional (Directorio Activo – Microsoft), a fin de poder forzar el despliegue de políticas de seguridad e instalación hacia los dispositivos a ser protegidos.		
4.3	Debe disponer de un filtrado de vistas de las estaciones de trabajo y servidores instalados como mínimo con las siguientes características: • Estado del cliente • Ultimas Conexiones • Dirección IPv4/IPv6		
4.4	Debe permitir la detección y bloqueo remoto de equipos infectados, evitando, de esta manera, la propagación de amenazas a través de la red.		
4.5	Permitir la ejecución de tareas de instalación, despliegue o desinstalación de forma remota, reconociendo a los equipos por su dirección o rango de direcciones IP, nombre, pertenencia a dominio, lista plana.		
4.6	La solución debe poder ser administrada de forma segura vía web utilizando el protocolo HTTPS		
4.7	Capacidad de detectar equipos no gestionados en la red y sobre los cuales no se ha desplegado las técnicas de protección requeridas.		
4.8	Capacidad para descargar las actualizaciones desde Internet a través de las versiones seguras de los protocolos FTP y/o HTTP, colocándolas en múltiples repositorios distribuidos donde los clientes puedan buscar las definiciones de manera local, lo cual permite un ahorro en el ancho de banda.		
4.9	Capacidad de programar las actualizaciones para que sean realizadas en diferentes momentos y horas específicas (diaria, semanal, mensual, cuando la máquina este inactiva, inmediatamente, entre otras).		
4.10	Capacidad de actualizar automáticamente los archivos de definiciones de virus, motor antivirus, ficheros de firmas y actualizaciones del producto antivirus de forma: automática, centralizada e incremental.		
4.11	Capacidad de generar reportes ilimitados, detallados y personalizados por fecha, tipo de amenaza, amenazas detectadas y/o eliminadas, equipos infectados y/o desinfectados.		
4.12	La solución debe quedar instalada en modo alta disponibilidad y balanceo de cargas, con el fin de garantizar un plan de recuperación y continuidad en caso de desastre. El oferente deberá garantizar todos los requerimientos para esta instalación.		
4.13	La solución deberá permitir manejar una estructura distribuida donde los sistemas en diferentes locaciones puedan replicar políticas y eventos desde un punto hacia la consola de gestión. La solución deberá permitir la instalación de múltiples consolas para mantener un esquema de gestión independiente en caso sea requerido.		
4.14	Disponer de información que permita ver el estado de seguridad y mantenimiento de los productos de toda la solución.		
5. MÓDULO CONTROL DE APLICACIONES			
5.1	El módulo de control de aplicaciones debe ser instalado para Dieciocho mil (18.000) nodos.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
5.2	El módulo de control de aplicaciones debe proporcionar un módulo de descubrimiento de aplicaciones instaladas en cada uno de los hosts, este reporte debe ser entregado al momento de la instalación, por demanda y/o definido a criterio del administrador, adicionalmente debe permitir la desinstalación remota desde la consola de administración del software que el administrador defina.		
5.3	La solución debe estar en la capacidad de generar lista blanca de aplicaciones, ejecutables y librerías independientemente si se encuentran instaladas y/o en uso.		
5.4	El módulo de control de aplicaciones debe permitir definir listas blancas de aplicaciones que pueden ser ejecutadas en los equipos de cómputo protegidos, esta lista podrá ser modificada en cualquier momento sin restricción.		
5.5	Las listas deben ser creadas de forma independiente por cada uno de los equipos protegidos, deben ser usadas para la realización de inventario de software y para el control de la ejecución de las mismas.		
5.6	El módulo de control de aplicaciones debe permitir definir listas negras de aplicaciones que no pueden ser ejecutadas, ni instaladas en los equipos de cómputo protegidos (de forma global para toda la plataforma), esta lista podrá ser modificada en cualquier momento sin restricción.		
5.7	La solución debe poder realizar inventario de las estaciones de trabajo el cual permitirá conocer las aplicaciones instaladas en estos.		
5.8	La solución permitirá proteger estaciones de trabajo mediante el control de la ejecución de aplicaciones, realizado a través de listas blancas y negras, por medio de la prevención de modificaciones hacia los archivos del punto final.		
5.9	La solución debe emplear un modelo de confianza y/o monitoreo de comportamiento para bloquear las aplicaciones no autorizadas o maliciosas.		
5.10	Debe contar con mecanismos de protección de memoria para contrarrestar los ataques de buffer overflow sobre las aplicaciones en lista blanca.		
5.11	Debe proteger contra las amenazas persistentes avanzadas y de tipo zero-day sin actualizaciones de firmas.		
5.12	La solución deberá permitir a los usuarios ser notificados sobre la razón por la cual la aplicación ha sido bloqueada.		
5.13	La solución deberá permitir a usuarios específicos que puedan instalar nuevo software en caso de que sea necesario, sin necesidad de autorización adicional.		
5.14	La solución deberá tener protección contra lectura y escritura de archivos.		
5.15	La solución deberá soportar los siguientes sistemas operativos Microsoft Windows server: 2008, 2008 R2, 2012, 2012 R2, y posteriores Además de los siguientes para estación de trábajo: 7, 8, 8.1, 10, 11 y posteriores.		
5.16	La solución deberá soportar los siguientes Sistemas Operativos de Microsoft los cuales ya no cuentan con soporte del fabricante: 2003, 2003 R2, Windows XP.		
5.17	La solución deberá soportar los siguientes sistemas operativos de Microsoft Windows Embedded: XPE, 7E, WEPOS, POS Ready 2009, WES 2009, 8 Industry, 8.1.		
5.18	La función de protección de escritura y cambios a los sistemas deberá proteger de: • Eliminar • Modificar Contenido • Cambiar Propietario • Truncar		
5.19	La solución debe proveer un panel de monitoreo para poder visualizar los cambios y violaciones en los equipos finales.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
5.20	El control de aplicaciones debe permitir realizar la desinstalación de software de forma remota.		
5.21	Reconocimiento de anomalías, detección y bloqueo de ataques de tipo Host Sweep, TCP or UDP port Scan, CGI Holes, entre otros.		
5.22	Detección de ataques de tipo Exploits hacia vulnerabilidades de sistema operativo como también de aplicaciones diferentes de Microsoft.		
5.23	El módulo de control de aplicaciones debe incluir un sistema de detección y prevención de intrusos basados en host que proteja los recursos del sistema y las aplicaciones de ataques internos y externos.		
5.24	El módulo de control de aplicaciones debe contar con una consola de administración o integrarse con la consola general de administración de la solución, adicionalmente deberá poder integrarse con sistemas de colección de eventos vía syslog o enviadas al SIEM (Enterprise Security manager McAfee) de la Policía Nacional.		
5.25	El módulo de control de aplicaciones debe contar con un Firewall personal para los equipos Windows.		
5.26	El módulo de control de aplicaciones debe permitir obtener estadísticas del software instalado en los equipos de cómputo, intentos de instalación de aplicativos que se encuentren en listas negras, entregando hora, máquina y usuario que intenta realizar la instalación.		
5.27	El módulo de control de aplicaciones debe contar con la opción de bloquear todas las aplicaciones por defecto y generar listas blancas creadas por la casa matriz de acuerdo a reputación del sitio de descarga, hash, checksum, nombre, lista blanca, definición del administrador, entre otros. Adicionalmente La solución deberá permitir a los usuarios ser notificados sobre la razón por la cual la aplicación ha sido bloqueada.		
5.28	Capacidad de generar reportes ilimitados, detallados y personalizados por fecha, tipo de amenaza, amenazas detectadas y/o eliminadas, equipos infectados y/o desinfectados.		
6. DATA LOST PREVENTION - DLP			
6.1	El módulo Data Lost Prevention - DLP debe ser instalado para Cuarenta y Cinco Mil (45.000) nodos.		
6.2	La solución debe basarse en un agente que se instala en cada computadora y servidor que servirá como medio de comunicación entre las estaciones de trabajo y la consola de administración.		
6.3	La solución debe tener una base de datos de Microsoft SQL u Oracle en la cual deberá guardar todos los informes sobre la detección de violaciones de políticas.		
6.4	La solución deberá permitir crear diferentes sets de permisos para asignar diferentes tipos de administración a usuarios y grupos.		
6.5	La solución deberá contar con un tablero de Analíticos, este tablero podrá mostrar los incidentes basados en la clasificación.		
6.6	La solución de protección de fuga de información del endpoint deberá contar con un agente para sistemas operativos MAC donde los usuarios de dicha plataforma puedan aplicar: Reglas de acceso por medio de aplicaciones, reglas de protección Cloud, reglas para protección de compartir en red y dispositivos removibles.		
6.7	La solución deberá integrarse con Active Directory y permitir hacer inicio de sesión a la consola de administración utilizando las credenciales de red con sus respectivos permisos.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
6.8	La solución debe tener la capacidad de administrar, configurar, instalar, desinstalar, actualizar, asignar políticas para el software de Control de dispositivos y Prevención de Fuga de Información (DLP).		
6.9	La solución debe llevar como mínimo 5 años consecutivos como líder en el cuadrante de Gartner o similares en la protección de endpoint.		
6.10	La solución debe identificar contenidos basados en tipo de contenido/documento.		
6.11	La solución debe monitorear el contenido que viaje a través del ENDPOINT, por dirección IP y protocolo.		
6.12	La solución debe monitorear el contenido que viaje a través el ENDPOINT, debido al acceso de aplicaciones.		
6.13	La solución debe permitir crear políticas para dispositivos extraíbles de almacenamiento, por fabricante.		
6.14	La solución debe poder identificar contenido usando expresiones regulares, palabras clave, las funciones hash, y la coincidencia de patrones.		
6.15	La solución debe poder identificar el contenido basado en localización.		
6.16	La solución debe poder identificar el contenido usando FINGERPRINT.		
6.17	La solución debe cumplir las políticas aplicadas de protección de fuga de información, sin importar que el equipo final se encuentre fuera de la red corporativa.		
6.18	La solución debe contar con una funcionalidad de Soporte de virtualización mejorada. Es decir que cada política por usuario debe ofrecer flexibilidad y un mejor control de los datos que fluyen a las terminales compartidas e infraestructuras de escritorio virtual (VDI). Así, las políticas por usuario deben aplicar a múltiples sesiones.		
6.19	La solución debe brindar protección a nivel de portapapeles para ambos: "copia de" y "pegar", además de protección de captura de pantalla para proteger el diseño de productos y códigos fuente contra la pérdida de datos intencional y no intencional. Garantizando esta protección incluso si se utilizan métodos alternativos como aplicaciones de recortes de office, one note, navegadores, entre otros.		
6.20	La solución debe permitir la configuración de incidentes de acuerdo con sus propiedades para una revisión posterior. Las propiedades deben ser como mínimo: • Severidad • Estatus • Resolución • Revisor		
6.21	La solución debe contar con mecanismos que prevengan la vista no autorizada de información confidencial, a través del módulo de manejo de incidentes, limitando la vista de incidentes sólo a revisores o administradores con un rol cuyos privilegios se lo permitan.		
6.22	La solución de contar con reglas de protección que estén basadas en: tipo de archivo, extensiones de archivo, propiedades de documento, tipos de encripción y asignación de usuarios o grupos.		
6.23	La solución debe permitir usar repositorios para evidencia.		
6.24	La solución deberá replicar de forma manual o automática a través de tareas el software para las actualizaciones e instalaciones.		
6.25	La solución deberá permitir crear políticas para clasificar el contenido sensible por medio de categorización de aplicaciones como; editores, exploradores, confiables y archivadores.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
6.26	La solución debe tener la capacidad de obtener información completa sobre las propiedades del documento sensible como; quien lo grabo de último, el título, autor, comentarios, etc.		
6.27	La solución debe permitir crear configuraciones por grupo, dominio o maquina sin afectar la estructura del árbol de administración.		
6.28	La solución debe controlar la impresión usando impresoras locales, en red, print screen e impresión en PDF.		
6.29	La solución no debe de requerir el reinicio de la computadora al instalar o hacer actualización.		
6.30	La solución debe controlar la carga de información sensible hacia aplicaciones de la nube como Box.inc, Dropbox, Google Drive, iCloud, OneDrive (personal) OneDrive for Business (groove.exe) y Simplicity.		
6.31	La solución debe contar con una lista de reglas de acción para realizar como mínimo lo siguiente: • Sólo lectura • Reportar a la consola central • Poner en cuarentena • Cifrar • Guardar la evidencia • Solicitar justificación • Notificar al usuario • Monitorear • Bloquear		
7. ARQUITECTURA			
7.1	La solución debe contar con una arquitectura distribuida para optimización de funcionalidades.		
7.2	Deberá contar con la creación de patrones avanzados para reducir los falsos positivos.		
7.3	La solución deberá tener mecanismos de control de incidentes para su revisión y operaciones como; Manejo de caso, comentarios, envió por correo, etc.		
7.4	La solución debe presentar un flujo de trabajo que debe contar con una fase de clasificación o definición, una fase de identificación y registro, una fase de protección y una fase de monitoreo.		
7.5	La solución debe integrarse con al menos una de las soluciones de Rights Management (IRM) como: • Microsoft Windows Rights Management Services • Seclore FileSecure information Rights Management Con el objetivo de aplicar políticas de RM a archivos detectados en escaneos de descubrimiento y poder incluir o excluir archivos protegidos por RM, de las reglas de protección de correo, almacenamiento removible, sistemas de archivos y web posting.		
7.6	Debe permitir la integración en algunos de los etiquetados de terceros como: • TITUS • Boldon James		
7.7	La solución debe contar con una consola de gestión centralizada, desde la cual sea posible gestionar políticas, reglas de protección de información.		
7.8	La interfaz de monitoreo de la solución debe proveer un panel para el manejo de incidentes, separado de un panel para eventos operacionales, donde se muestren eventos administrativos.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
7.9	La solución debe contar con la posibilidad de hacer control de acceso basado en roles.		
7.10	Se requiere que la solución posea una consola de administración vía web.		
7.11	Los revisores o administradores de la consola deberán poder auditar las siguientes acciones: • Entrada al servidor de administración • Cambio de perfiles o roles • Cambio de contraseñas • Cambios de políticas Esta característica es importante cuando se desea descubrir cambios ocurridos en el servidor de administración.		
7.12	El agente debe registrar todas las violaciones e informes en la base de datos central de la consola, cuando se establece una conexión a la red corporativa.		
7.13	La solución deberá contar con reportes predefinidos y la posibilidad de crear nuevos a partir de queries personalizados.		
7.14	La solución debe soportar reglas y exclusiones basadas en directorio de datos para reforzar las políticas basándose en cualquier atributo del documento y/o receptor.		
7.15	La solución debe incluir una biblioteca de plantillas predefinidas de detección orientadas al cumplimiento con regulaciones locales y globales como la Ley de protección de datos (Ley 1581, SOX, PCI y HIPAA.), Si la solución no incluye la plantilla el proveedor deberá crear dicha plantilla y dejarla en operación.		
7.16	La solución debe permitir detectar y analizar archivos y anexos de correo de tamaños mayores a 20 MB sin verse afectado el rendimiento de los equipos.		
7.17	La solución debe permitir especificar el grado de proximidad como una condición de una coincidencia para un incidente.		
7.18	La solución debe detectar la información sin importar que el orden de los datos haya sido alterado.		
7.19	La solución deberá estar en la capacidad de detectar contenido confidencial incluso si el nombre o tipo de archivo es modificado.		
7.20	La solución debe soportar la detección de coincidencias en un contenido con exactitud del 100% para documentos específicos tales como código fuente, documentos financieros, etc.		
7.21	Debe ser posible definir un umbral o porcentaje mínimo requerido de coincidencia de un documento para considerar que existe una violación a la política configurada.		
7.22	La solución debe permitir la detección basada en expresiones regulares.		
7.23	La solución debe permitir la detección o presencia de archivos cifrados.		
7.24	La herramienta podrá ser integrada con herramientas de cifrado de datos, para que en el caso de detectar contenido sensible tenga como respuesta el cifrado de la información.		
7.25	La solución debe permitir notificar automáticamente a remitentes administradores y jefes inmediatos de un usuario cuando este ha violado una política.		
8. CIFRADO			
8.1	El módulo de cifrado debe ser licenciado y configurado para quince mil (15.000) nodos.		
8.2	La solución de cifrado de discos debe permitir el cifrado en los sistemas operativos Microsoft y MAC.		
8.3	La solución debe permitir la integración con el directorio activo.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
8.4	La solución de cifrado debe permitir la creación de políticas a través de grupos del directorio activo.		
8.5	La solución de cifrado debe contar con una consola de administración centralizada.		
8.6	La solución debe permitir el envío de tareas remotas tales como cifrar y descifrar desde la consola de administración.		
8.7	La solución de cifrado debe permitir tener una recuperación centralizada a través de la consola de administración.		
8.8	La solución de cifrado debe permitir tener SSO (Single Sign-On) con el directorio activo para el acceso a las maquinas cifradas.		
8.9	La solución de cifrado de discos deberá integrar en el mismo licenciamiento la funcionalidad de cifrado de archivos que se copian a medios removibles.		
8.10	La solución de cifrado de discos debe tener una funcionalidad que se copie en los medios extraíbles para ver la información cifrada en equipos que no tengan ninguna solución de cifrado. Esta funcionalidad debe poder abrirse en Windows y MacOSX.		
8.11	La solución de cifrado debe permitir crear una contraseña para el cifrado de todos los archivos que se copian a los medios extraíbles o tener una contraseña según las preferencias del usuario.		
8.12	Las contraseñas que se crean para la copia de archivos a medios extraíbles deben permitir configurar complejidad.		
8.13	La solución de cifrado debe permitir generar informes del estado de los discos administrados y cifrados.		
8.14	La solución de cifrado debe permitir la configuración de un método de seguridad cuando se ingrese la contraseña incorrectamente un determinado número de veces. Ejemplo evitar la autenticación durante determinado tiempo.		
8.15	La solución de cifrado debe permitir configurar un tiempo de expiración de las contraseñas.		
8.16	La solución debe permitir la configuración del periodo de conexión entre los agentes de cifrado y la consola centralizada.		
8.17	La solución de cifrado debe permitir la autenticación en las maquinas cifradas con password, token o token y password.		
8.18	La solución de cifrado debe tener métodos de recuperación ante desastres, en caso de que exista daño en el sistema operativo, el usuario olvide su contraseña y/o los métodos de recuperación no funcionen.		
8.19	La solución de cifrado debe soportar cifrado AES 256 Bits.		
8.20	La ventana de Preboot debe permitir la personalización de logo y mensaje de bienvenida.		
8.21	La solución de cifrado de discos debe permitir el cifrado de solo el Boot de inicio o de todos los discos según se requiera.		
8.22	La consola de administración de cifrado de discos duros debe permitir visualizar las particiones cifradas y las no cifradas.		
8.23	El agente de cifrado de discos debe permitir visualizar las unidades que están cifradas y descifradas en la máquina.		
8.24	El agente de cifrado de discos debe permitir ver un porcentaje del proceso de cifrado de discos.		
8.25	La solución de cifrado de medios removibles debe permitir crear exclusiones para evitar que determinadas extensiones de archivos se cifren automáticamente.		

ÍTEM	CONDICIONES TECNICAS MÍNIMAS	CUMPLE	NO CUMPLE
8.26	La solución de cifrado de medios extraíbles debe permitir crear exclusiones de dispositivos que no se cifraran.		
8.27	El producto debe soportar las siguientes maquinas clientes: • Windows 7 and SP1 (32- and 64-bit), (Not XP Mode) • Windows 8 • windows 10 • Windows 11 y posteriores		
8.28	La solución debe poseer al menos las siguientes certificaciones: • Common Criteria EAL2 +, FIPS 140-1, FIPS 140-2 • AES CBC (e/d; 256).		
8.29	La solución debe soportar al menos los siguientes algoritmos de Encriptación: • AES-256.		
8.30	La solución de cifrado debe permitir el cifrado de archivos que sean transferidos a dispositivos de almacenamiento extraíble.		
8.31	La solución de cifrado debe permitir generar excepciones sobre dispositivos donde no se debe aplicar el cifrado.		
8.32	Debe tener la capacidad de cifrar el disco completo, reemplazando el Master Boot Record (MBR).		
8.33	La solución debe proveer mecanismos seguros que garanticen la recuperación del acceso en caso de pérdida de la contraseña. Estos mecanismos deben requerir la intervención y el intercambio de información con la consola de administración.		
8.34	Debe ser capaz de descifrar el disco en forma automática, desde la consola de administración y mediante mecanismos manuales.		
8.35	La solución debe solicitar autenticación al usuario antes de iniciar la carga del sistema operativo (SO). Luego de iniciar el SO, la solución debe poder configurarse de manera que solicite o no, nuevamente, las credenciales de autenticación del usuario.		
8.36	Las actualizaciones de la solución deberán realizarse remotamente y desde una consola de administración centralizada.		
8.37	La arquitectura de la solución debe ser cliente-servidor.		
8.38	La solución debe emplear el mínimo de utilización de recursos del CPU.		
8.39	La solución debe tener la capacidad de realizar single Sign-On en sistemas operativos Windows permitiendo el acceso a la maquina mediante las credenciales de Windows y reduciendo los procesos para ingresar.		
8.40	La solución debe soportar la unificación del usuario y contraseña utilizadas por el usuario en el directorio Activo de Microsoft.		
8.41	La solución debe contar con una herramienta externa que utilice las Llaves de Encriptación almacenadas en la consola de administración para ejecutar cualquier actividad de recuperación de discos o archivos.		
8.42	La solución debe soportar Single Sign-On (SSO) en integración con las políticas de grupo (GPO) del Directorio Activo de Microsoft.		
8.43	La solución debe contar con la opción de generar un "código de respuesta" para la recuperación del administrador.		
8.44	El acceso de los usuarios administradores a la consola de administración debe poder hacerse basado en roles.		
8.45	La consola de administración debe permitir la creación de políticas de autenticación que no sean de alcance global.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
8.46	La solución debe proveer reportes del estado de la solución en las maquinas administradas. Todos estos reportes deben ser exportables vía correo o a documentos PDF, XLS y CSV.		
8.47	La solución debe proveer un reporte de los sistemas cifrados, mostrando un estado de Cifrado o Descifrado.		
8.48	La solución debe ser capaz de enviar reportes y notificaciones por email en los siguientes formatos: • CSV • XLS • PDF		
8.49	La solución debe permitir generar reportes basados en eventos históricos.		
8.50	La solución debe contener reportes y consultas (query) que se puedan personalizar.		
8.51	La solución debe contar con la funcionalidad de que gestionar Native Encryption.		
8.52	La solución debe ofrecer beneficios en común para la gestión sobre FileVault y BitLocker: • Posibilidad de actualizar una versión OS X a la siguiente sin tener que descifrar y volver a cifrar el disco. • Compatibilidad de día cero con parches, actualizaciones y actualizaciones de firmware de Apple y Microsoft. • Característica de recuperación que permite a los usuarios restablecer el acceso a sus máquinas. • Fácil administración		
8.53	La solución debe ofrecer beneficios para entornos Mac: • Capacidad de hacer SSO desde el entorno de Pre-Boot de FileVault directamente al inicio del ambiente de OS X. • Administración de File Vault en un HW que puede ejecutar OS X Mountain Lion, Mavericks o Yosemite, desde una consola centralizada. • Generación de reportes de cumplimientos y elaboración de tableros de control. • Apoyo a las herramientas y flujos de trabajo para la recuperación de información proveídas por Apple (FileVault Recovery Key) • Permitir a los administradores la importación manual de FileVault Recovery Keys donde ya manualmente los usuarios han habilitado File Vault.		
8.54	Beneficios para entornos Windows: • Soportar dispositivos certificados Windows To Go • Administrar de BitLocker en hardware Windows 7 u 8, 10 y 11 desde una única consola • Proveer una experiencia transparente al usuario (Trusted Platform Module - TPM) • Soportar los requerimientos FIPS 140-2. • Soportar Microsoft eDrive. • Generación de reportes de cumplimientos y elaboración de tableros de control • Administración de BitLocker sin la necesidad de contar con un servidor Microsoft BitLocker Management and Monitoring (MBAM).		
9. SOLUCIÓN DE SEGURIDAD PERIMETRAL DE CORREO - ANTISPAM			
9.1	Se requiere una solución de tipo "Gateway" que permita la inspección profunda de los correos electrónicos contra las siguientes amenazas: spam, phishing, virus, ataques de directorio, ataques de rebote (bounce attacks) y filtrado de contenidos para 20.000 buzones.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
9.2	El fabricante de la solución deberá ofrecer detectar el 99,9% de Spam con un número de Falsos positivos menor o igual a 1 en un millón.		
9.3	El dispositivo deberá estar soportado para correr tanto en Hardware físico o a través de dispositivos virtualizados en plataformas Hyper-V. La Policía Nacional privilegiará el poder montar la solución en la infraestructura de virtualización existente o en la máquina suministrada por el contratante que cumpla los requerimientos necesarios para soportar la cantidad de usuarios de la Policía Nacional.		
9.4	El número de servidores virtuales de filtrado podrá incrementarse o disminuirse a discreción de la Policía Nacional sin incrementar el costo de la solución.		
9.5	La solución se deberá sincronizar con el Directorio Activo de la Policía Nacional para permitir el acceso a la cuarentena por cada usuario, además de detectar y evitar ataques de directorio.		
9.6	La solución podrá controlar y dilatar las conexiones y el envío de direcciones IP que se hayan detectado envíen Spam principalmente.		
9.7	Además de listas blancas de IP, La solución podrá, sin intervención de administración, tener estadísticas de direcciones IP que envíen correo bueno para privilegiar el envío de correos hacia el interior de la Policía.		
9.8	La Policía Nacional podrá generar direcciones de correo que actualmente no estén uso y sean altamente atacadas para que sean analizados directamente contra problemas de SPAM por parte del fabricante de la Solución.		
9.9	La Policía podrá crear exclusiones de SPAM para buzones dedicados al reporte y análisis de problemas de SPAM y Phishing de los que sufra la ciudadanía.		
9.10	El dispositivo podrá identificar máquinas internas que estén generando ataques al interior de la red de la compañía y rechazar temporalmente dichas conexiones.		
9.11	La solución permitirá la firma de correos electrónicos de salida con el estándar DKIM y así mismo podrá chequear la validez de los correos entrantes para las firmas DKIM.		
9.12	La solución contará con plantillas que permitan examinar los contenidos de los correos y sus adjuntos para evitar fugas de información.		
9.13	La solución incluirá la ejecución de reportes. Dichos reportes podrán dar una idea del estado del servicio y número de correos detenidos, número de correos que presentan malware, correos que no se pudieron escanear, reporte de reputación IP entre otros.		
9.14	La solución tendrá un sitio de cuarentena tipo Web para retener los correos de acuerdo a las Políticas de seguridad de la Policía. Los usuarios podrán acceder a dicha cuarentena bien para eliminar los correos o dejarlos pasar.		
9.15	La solución deberá contar con mecanismos de auditoría detallados para reconocer correos enviados, asunto, disposición de filtrado.		
9.16	La solución tendrá mecanismos de detección antispam basada en firmas, heurísticas que se actualicen frecuentemente de los servicios del fabricante.		
9.17	El dispositivo a través del tiempo podrá aprender de los comportamientos de las direcciones IP de los remitentes para rechazar la comunicación de direcciones IP reconocidas como Spammers		
9.18	El dispositivo a través del tiempo tendrá la capacidad de clasificar direcciones IP que envían principalmente correo no spam y privilegiar el paso del correo y haciendo solo la detección antivirus		
9.19	El dispositivo debe permitir la limpieza de amenazas dentro archivos adjuntos (javascript dentro de archivos PDF o Microsoft Word, por ejemplo)		
9.20	El soporte de la solución antispam será 7x24x365 con un tiempo de respuesta de no superior a más de una hora, La solución debe contar con un soporte que permita		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
	accesos directos a los especialistas de producto cuando sea requerido por los diferentes medios de atención por la Policia Nacional.		
9.21	La solución de filtrado de correo electrónico deberá proteger el correo entrante contra amenazas como virus, spyware, malware, spam, phishing y permitirá crear reglas de filtrado dependiendo los destinatarios, remitentes, contenidos.		
9.22	La solución deberá estar en capacidad de cifrar correo electrónico y sus adjuntos para al menos 500 usuarios simultáneos.		
9.23	La solución podrá identificar archivos sin importar su extensión identificando su verdadero contenido.		
9.24	Para archivos cuyo contenido sean ejecutables la solución podrá identificarlos y remover el contenido ejecutable dentro de dichos correos o eliminar el correo.		
9.25	La solución de filtrado de correo electrónico podrá inspeccionar el contenido de los correos para detectar URLs que se consideren maliciosas y actuar de acuerdo a las políticas de la Policía Nacional.		
9.26	La solución podrá ser instalada en al menos un appliance físico o virtual, pero podrá ser distribuida en tantos appliance requiera la Policía, administrados de manera centralizada.		
9.27	La solución contará con consola y/o carpetas de cumplimiento. Una carpeta de cumplimiento es un espacio dentro de la solución en la que se retienen correos electrónicos que caen dentro de la detección de una política (filtran datos sensibles, se requieren para auditoría).		
9.28	La solución no deberá requerir licenciamiento adicional del sistema operativo sobre el que corre.		
9.29	El Software de la solución deberá estar asegurado por el fabricante y el acceso a las cuentas privilegiadas (root) deberá estar deshabilitada como mecanismo de aseguramiento.		
9.30	La solución seguridad perimetral de correo no podrá ser instalada en los servidores de Correo de la Policía Nacional. La idea es disminuir el impacto de este procesamiento y proteger la infraestructura de la Policía.		
9.31	La solución deberá clasificar los mensajes recibidos en categorías dentro de las cuales debe existir una categoría para identificar correos relacionados con marketing (publicidad).		
9.32	La solución tendrá mecanismos de reputación de IP que impedirán o retrasarán la conexión de los atacantes.		
9.33	La solución debe tener listas negras de remitentes tanto locales como globales para ser usadas en las políticas de filtrado.		
9.34	La solución debe ser configurada para tomar acciones diferentes con correos de publicidad y/o boletines de noticias.		
9.35	La solución debe permitir autenticación de remitentes a través de SPF tanto como política general para todos los correos recibidos como para una lista de dominios específicos.		
9.36	El filtrado de correo electrónico deberá permitir enviar muestras de SPAM al fabricante de la solución para obtener reglas personalizadas contra SPAM.		
9.37	La solución debe permitir crear reglas de filtrado de correo de acuerdo con su contenido, tanto para información estructurada como no estructurada, expresiones regulares, diccionarios y palabras clave; y deberá generar un reporte con las posibles violaciones a la política.		
9.38	Debe permitir crear y aplicar políticas de prevención de fuga de información.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
9.39	La solución antispam debe contar con una consola de administración o integrarse con la consola general de administración de la solución, adicionalmente deberá poder integrarse con sistemas de colección de eventos vía syslog o enviadas al SIEM (Enterprise Security manager McAfee) de la Policía Nacional.		
10.	**GENERALIDADES**		
SOPORTE Y MANTENIMIENTO			
10.1	El personal que realizará la instalación y configuración de la solución, deberán ostentar el título de Ingeniero de Sistemas, Electrónico y/o a fines, con una experiencia mínima de un (1) año en la configuración e instalación la solución y contar con capacitación certificada por la casa matriz. Para lo cual el oferente deberá presentar con la oferta copia del título de pregrado en ingeniería de sistemas, electrónica y/o a fines, tarjeta profesional vigente, copia de la certificación de la casa matriz sobre la idoneidad en la implementación y administración solución y una certificación de experiencia en la instalación y soporte de la misma de la persona propuesta para la implementación.		
10.2	Los soportes serán generados por los usuarios de la red de la PONAL (Policía Nacional) a través de la herramienta de help desk de la Policía Nacional (SIGMA) para la gestión por parte del ingeniero de soporte asignado por el oferente, el cual deberá proporcionar un soporte 5x8 en sitio durante la misma vigencia de la garantía, derecho a actualizaciones de la licencias de los productos adquiridos, a partir del recibo a satisfacción del contrato, el cual se debe prestar en sitio con tiempos de respuesta no superiores a 30 minutos, y tiempos de solución no mayores a las setenta y dos (72) horas debiéndose dar respuesta oportuna y orientación precisa a los diferentes casos que se reporten. Los soportes e incidentes generados a través de la herramienta SIGMA deberán ser gestionados por el ingeniero de soporte asignado por la empresa contratista desde la red LAN y/o WAN de la Policía Nacional (no se permiten VPN para el soporte), se evaluarán los casos de soporte remoto únicamente para asistencia por parte de la casa matriz.		
10.3	El soporte, mantenimiento y actualizaciones de la solución objeto del contrato será por un término de dieciocho (18) meses a partir del recibo a satisfacción de la solución.		
10.4	El mantenimiento y actualización debe permitir de manera proactiva y centralizada desde la consola de gestión mantener la plataforma tecnológica de la Policía Nacional debidamente asegurada, mediante actividades que permitan validar los niveles de actualización y cobertura de los productos implementados en todas las estaciones y servidores que tengan conectividad con la consola.		
10.5	El servicio de soporte telefónico debe darse directamente por la casa matriz para todos los niveles de prioridad de los incidentes, problemas, inquietudes, dudas que se reporten durante el término de vigencia del contrato.		
10.6	En caso de existir urgencia respecto a incidentes que involucren las soluciones ofertadas el oferente deberá proporcionar en caso de necesitarlo apoyo de casa matriz (remoto o presencial) hasta solucionar el incidente.		
10.7	El soporte de la solución será 8x5 con un tiempo de respuesta no superior a más de una hora por parte del fabricante, La solución debe contar con un soporte que permita accesos directos a los especialistas de producto cuando sea requerido por los diferentes medios de atención por parte la Policía Nacional.		

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
10.8	El oferente informará periódicamente vía e-mail al correo ponal.csirt@policia.gov.co de la entidad, acerca de los nuevos virus, suministrando los medios para combatirlos y evitar próximos ataques, informando dentro de las dos (02) horas siguientes después de presentarse la alerta mundial.		
11. SERVICIOS DE IMPLEMENTACIÓN			
11.1	La solución ofertada deberá ser instalada y configurada de forma centralizada por el oferente, realizando los despliegues en todos los repositorios a nivel nacional. El oferente en caso de ofrecer un producto diferente al existente en la Policía Nacional deberá realizar la desinstalación del mismo durante el período de implementación.		
11.2	El oferente deberá garantizar total compatibilidad con la infraestructura de red, sin degradar el rendimiento de los equipos bajo las diferentes plataformas tanto de estaciones de trabajo como de servidores e infraestructura de red que se encuentran instalados. Para lo cual deberá soportar técnicamente mediante la realización de pruebas.		
11.3	Se deben incluir Cuarenta y ocho (48) horas de servicios profesionales directamente del fabricante de la solución ofertada, con el fin de realizar actividades que vaya orientadas al mejoramiento continuo de la implementación, despliegue y configuración de la solución adquirida		
12. TRANSFERENCIA DE CONOCIMIENTOS			
12.1	El oferente deberá incluir una capacitación por el oferente o la casa matriz para al menos diez (10) funcionarios de soporte técnico de la solución que incluya el uso y administración del software, antivirus, control de dispositivos, Control de Aplicaciones, Data Lost Prevention - DLP, Cifrado, Antispam, las actualizaciones, funcionalidades de los productos adquiridos en el presente contrato. La intensidad horaria no debe ser inferior a 30 horas.		
13. LICENCIAMIENTO			
13.1	Todo el software que compone la solución debe ser licenciado de manera perpetua a nombre de la Policía Nacional.		
14. ASPECTOS DE CONFIDENCIALIDAD			
14.1	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,si se considera pertinente someter a estudio de seguridad al personal que prestará los servicios, el contratista permitirá y facilitará todos los medios que la Entidad le solicite para este fin.		
14.2	En virtud del presente estudio previo, el Oferente 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 firmar un acuerdo de confidencialidad y no revelación de la información, para lo cual deberá diligenciar el formulario "ACUERDO DE CONFIDENCIALIDAD".		
15. SERVICIOS PROFESIONALES			
15.1	Se debe presentar junto con el acta de iniciación del contrato, un cronograma de trabajo que relacione la instalación, configuración y las respectivas pruebas de aceptación.		
15.2	El oferente debe garantizar y certificar que el personal que prestará el servicio de soporte y mantenimiento son ingenieros debidamente certificados por la casa matriz del producto solicitado.		

ITEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
16. DOCUMENTACIÓN TÉCNICA – ENTREGABLES			
16.1	Se debe entregar totalmente documentada la metodología de implementación y configuración de la herramienta ofertada siguiendo las recomendaciones de mejores prácticas de la casa matriz.		
16.2	El oferente deberá disponer de un sitio web de base de conocimiento en el cual se pueda realizar consulta de la documentación de la solución implementada, a su vez la metodología de implementación y configuración de la herramienta ofertada siguiendo las recomendaciones de mejores prácticas de la casa matriz.		
16.3	Toda la documentación debe entregarse en idioma español.		
16.4	Para el acta de inicio del contrato se debe anexar el cronograma detallado de actividades, indicando actividad, tiempo y responsables de la ejecución del contrato		
16.5	Manual de procedimientos de administración y operación de la solución ofrecida.		
17 SEGURIDAD DE INSTALACIONES			
17.1	Durante el tiempo de garantía el contratista deberá cumplir con el protocolo de seguridad de instalaciones y normas internas de seguridad física en cada una de las unidades policiales en todo el territorio colombiano y Manual del Sistema de Gestión de Seguridad de la Información para la Policía Nacional (Resolución No. 08310 del 28/12/2016), para lo cual deberá diligenciar el formulario "SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO"		
18. SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO			
18.1	El contratista deberá cumplir con la implementación del sistema de Gestión de la Seguridad y Salud en el Trabajo, para lo cual deberán diligenciar el fomulario "SISTEMA DE GESTIÓN DE LA SEGURIDAD Y SALUD EN EL TRABAJO"		

21. EXPERIENCIA MÍNIMA DEL PROPONENTE

PROPONENTE NACIONAL

El Registro Único de Proponentes es el instrumento a través del cual los proponentes deberán acreditar el requisito de experiencia, para tal efecto las Personas Naturales, las Personas Jurídicas, las Uniones Temporales, los Consorcios, que participen en este proceso, para efectos de verificación de este requisito, deberán acreditar experiencia como se menciona a continuación:

El oferente deberá demostrar su experiencia específica hasta la fecha de cierre de la presente contratación, mediante la celebración de máximo tres (3) contratos identificados con el códigos del clasificador de bienes y servicios de Naciones Unidas descrito en el numeral 1.1 DESCRIPCIÓN GENERAL DEL OBJETO del presente estudio previo, cuyo objeto sea igual o similar al objeto del presente proceso y se relacione con LA SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO y ANTISPAM, celebrados con Entidades públicas y/o privadas, ejecutados y/o liquidados, para tal efecto se verificará en el Registro Único de Proponentes donde se acredite que dichas operaciones comerciales fueron realizadas antes del cierre de la presente contratación y que su valor sumado sea igual o superior al item a ofertar conforme al cuadro que se relaciona a continuación

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	VALOR EXPRESADO EN SMMLV
43233200	Difusión de Tecnologías de información y telecomunicaciones	Software	Software de seguridad y protección	700

Nota 1: el Certificado de Registro Único de Proponentes constituye plena prueba respecto de la información verificada documentalmente y cuyo registro se encuentra vigente y en firme.

Nota 2: en la presentación de la oferta el oferente deberá diligenciar y entregar los formularios, donde relacionará los contratos que considere para la evaluación de la experiencia mínima requerida.

Cuando los documentos no indiquen su valor en SMMLV, o si estos son de años anteriores a 2022, se hará la respectiva conversión de acuerdo al año en que término el contrato. La verificación será realizada por el comité evaluador técnico.

Nota 3: si los contratos acreditados fueron realizados bajo la modalidad de Consorcio o de Unión Temporal, La Dirección Administrativa y Financiera tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del Consorcio o de la Unión Temporal, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del Consorcio o de la Unión Temporal, donde deberá constar el porcentaje de participación de cada uno de los integrantes para la ejecución del contrato.

Nota 4: en el caso que el proponente haya participado en procesos de fusión o escisión empresarial, debe tomar para estos efectos, exclusivamente los contratos que le hayan asignado en el respectivo proceso de fusión o escisión, para ello debe aportar el certificado del contador público o del revisor fiscal (si la persona jurídica tiene revisor fiscal) que así lo acredite.

Nota 5: si en la Información relacionada en el RUP para acreditar la experiencia mínima, se requiere verificar, la entidad se reserva el derecho de solicitar documentación adicional para verificar la información de la documentación entregada.

Nota 6: circular Externa No. 12 del 5 de mayo 2014 Colombia Compra Eficiente "La experiencia es un requisito habilitante. Los proponentes deben inscribir en el RUP su experiencia usando los códigos del Clasificador de Bienes y Servicios. Por su parte, las Entidades Estatales al establecer el requisito habilitante de experiencia deben incluir los códigos específicos del objeto a contratar o el de bienes, obras o servicios afines al Proceso de Contratación respecto de los cuales los proponentes deben acreditar su experiencia".

Nota 7: la Entidad podrá solicitar información adicional (que no conste en el RUP) para verificar la experiencia mínima requerida.

Nota 8: cuando el adjudicatario sea una persona natural, dentro de los tres días siguientes a la suscripción del acta de inicio, debe informar mediante documento a quien otorga facultades legales de representación en eventos de fuerza mayor a ocaso fortuito.

EXPERIENCIA PARA PERSONAS NATURALES O JURÍDICAS, EXTRANJERAS SIN DOMICILIO O SIN SUCURSAL EN COLOMBIA

Las personas naturales o jurídicas, extranjeras sin domicilio o sin sucursal en Colombia, que aspiren a celebrar contratos con las entidades estatales no requieren estar inscritos en el Registro Único de Proponentes, por ello se verificará la experiencia mediante la certificación de máximo tres (3) contratos celebrados y ejecutados con entidades públicas y/o privadas, que deban contener como mínimo la siguiente información:

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE	VALOR EXPRESADO EN SMMLV
43233200	Difusión de Tecnologías de información y telecomunicaciones	Software	Software de seguridad y protección	700

- Identificación de cada uno de los contratos.
- Nombre o razón social del contratante.
- Nombre o razón social del contratista.
- Objeto del Contrato
- Cuantía o valor del contrato.
- La certificación debe venir debidamente suscrita por la persona facultada para expedir dicho documento.

- Si la certificación incluye varios contratos, se deberán indicar los requisitos aquí exigidos para cada uno de ellos y se ponderará por contrato suscrito relacionado.
- Si la certificación incluye el contrato principal con sus adiciones se entenderá como un solo contrato certificado.
- Porcentaje del valor del contrato que ejecutó como miembro de un Consorcio, Unión Temporal, Sociedad de Objeto único, Empresa Unipersonal o Sociedades en general (Si es el caso).

Nota 1: si son contratos realizados bajo la modalidad de Consorcio o de Unión Temporal, la DIRECCIÓN ADMINISTRATIVA Y FINANCIERA tomará para la verificación, el porcentaje (%) de participación en la ejecución del contrato del oferente que haga parte del Consorcio o de la Unión Temporal, y luego sumará el valor obtenido para así establecer el total acreditado. Para lo anterior, deberá presentar el documento que acreditó la conformación del Consorcio o de la Unión Temporal, donde deberá constar el porcentaje de participación de cada uno de los integrantes para la ejecución del contrato.

Nota 2: no podrá acumularse a la vez, la experiencia de los socios y la de la persona jurídica cuando estos se asocien entre sí para presentar propuesta

Nota 3: no se aceptarán auto certificaciones.

Nota 4: no se tendrán en cuenta las certificaciones de contratos en ejecución.

Nota 5: no se aceptan certificaciones con enmendaduras o que presenten inconsistencias no subsanadas de acuerdo con este pliego de condiciones.

Nota 6: en el caso que el proponente haya participado en procesos de fusión o escisión empresarial, debe tomar para estos efectos, exclusivamente los contratos que le hayan asignado en el respectivo proceso de fusión o escisión, para ello debe aportar el certificado del contador público o del revisor fiscal (si la persona jurídica tiene revisor fiscal) que así lo acredite

Nota 7: en el caso de sociedades que se escindan, la experiencia de la misma se podrá trasladar a cada uno de los socios escindidos, y se contabilizará según se disponga en los respectivos pliegos de condiciones del proceso

Nota 8: los proponentes extranjeros deben diligenciar el Formulario "CERTIFICACIÓN DE CONTRATOS PARA ACREDITACIÓN DE EXPERIENCIA PROPONENTE EXTRANJERO SIN SUCURSAL O DOMICILIO EN COLOMBIA" y/o "CLASIFICACIÓN PROPONENTE EXTRANJERO."

Nota 9: la entidad podrá solicitar información adicional para verificar la experiencia mínima requerida

Nota 10: cuando el adjudicatario sea una persona natural, dentro de los tres días siguientes a la suscripción del acta de inicio, debe informar mediante documento a quien otorga facultades legales de representación en eventos de fuerza mayor a ocaso fortuito.

La Policía Nacional **se reserva el derecho** de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin constatar el contenido de la misma.

Patrullero **JOJAN DANIEL PRADO FULA**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Patrullero **WILMER ALEXANDER BARACALDO CIFUENTES**
Analista de Seguridad de la Información
Estructurador Estudio Previo

Intendente **ALEXANDER DIAZ CASTILLO**
Analista de Seguridad de la Información
Estructurador Estudio Previo

