



FICHA TÉCNICA RENOVACIÓN ANTIVIRUS

<i>Item</i>	<i>Solución</i>	<i>Descripción</i>	<i>Cantidad de licencias actual</i>	<i>Ubicación</i>
1	Trellix CEB (Complete EP Protect Business)	Renovar y actualizar la solución de seguridad completa a la solución Trellix Native Drive Encryption la cual ofrece una solución centralizada y ligera para gestionar la tecnología de cifrado de disco completo nativa de los dispositivos Microsoft (BitLocker) y Apple (FileVault), con especial atención al bajo mantenimiento y a la rápida adaptación a las normativas. La solución se gestiona desde la consola unificada de ePO con la cual ya la entidad tiene sus equipos gestionados.	20	Equipos de cómputo la Personería de Bogotá
2	Trellix EDR (Endpoint Detection and Response)	TrellixEDR (Endpoint Detection and Response) Renovar y actualización de la versión Trellix EDR a la versión Enterprise EPEN(Trellix Endpoint Enterprise Cloud) cuya finalidad es identificar, detectar y prevenir amenazas avanzadas con mayor facilidad. Protección unificada para Windows, macOS y Linux. Consola de administración 100% en la nube(SaaS) con opción on-Premises. Protección avanzada contra malware, ransomware y amenazas de día cero mediante IA, machine learning y análisis de comportamiento. EDR con investigación guiada, threat hunting y respuesta automática a incidentes. Control de aplicaciones y dispositivos (USB, periféricos y listas blancas). Firewall personal y control web con filtrado por categorías, reputación y protección contra phishing. Análisis forense con recolección de evidencias memoria, procesos y remediación remota.	1300	Equipos de cómputo la Personería de Bogotá



Requerimiento técnico mínimo

1. Especificaciones del Software

- a. Término de licenciamiento por un lapso de un (1) año contado a partir de la fecha de inicio de ejecución del contrato para cada una de las licencias tanto para la renovación como para las nuevas licencias adquiridas por la Entidad.
- b. Disponibilidad de la solución antivirus, como mínimo el 99.8%
- c. La renovación de las licencias deberá contar con la actualización a su versión comercial liberada del software antivirus, tanto para estaciones de trabajo como para servidores y las consolas de administración, mejoras del producto y correcciones durante el tiempo de vigencia del licenciamiento. SIN COSTO ADICIONAL.
- d. Desde la consola se debe administrar en cada uno de los clientes y/o grupos, la actualización de los clientes, en su versión de antivirus, actualización de los archivos, servicios de definición y/o firmas de virus, motor de búsqueda, parches y actualizaciones extraordinarias por el término de vigencia del licenciamiento.
- e. El producto debe estar en capacidad de actualizar automáticamente las políticas de prevención sin congestionar la red, ni afectar el rendimiento de las estaciones por el término de vigencia del licenciamiento.
- f. El software debe generar reporte de los virus detectados y acciones realizadas por el término de vigencia del licenciamiento.
- g. Los agentes deberán ser instaladas en cada uno de los equipos de la entidad bajo las mejores prácticas del fabricante y los lineamientos del cliente. Esta instalación deberá ser realizada por personal certificado por el fabricante para lo cual se deberá presentar al supervisor del contrato la respectiva certificación de idoneidad, sobre la versión que esté instalando o sobre la que realice el soporte técnico

2. Requerimiento de actividades técnicas a realizar

- a. El contratista en desarrollo y ejecución del contrato deberá tramitar ante el fabricante la renovación del licenciamiento por suscripción a nombre de la Personería de Bogotá D.C., remitiendo la documentación y soportes correspondientes de dicha gestión a la Dirección de Tecnologías de la Información y las Comunicaciones de la Personería de Bogotá, D.C., de la siguiente manera:
 - Renovar por doce (12) meses veinte (20) licencias Trellix Complete Endpoint Protection Business (CEB).
 - Renovar por doce (12) meses, mil trescientas (1300) licencias Trellix Endpoint Detection and Response (EDR).
- b. Acompañar a la Entidad durante la totalidad del plazo de ejecución del contrato y del período de renovación de las licencias en los procesos de actualización a las versiones liberadas por el fabricante y en la instalación o actualización de los agentes en los equipos cubiertos por el licenciamiento, de acuerdo con la compatibilidad, los requisitos técnicos del fabricante y las condiciones de hardware y sistema operativo de cada equipo.
- c. Proporcionar el acceso al sitio de la plataforma (<https://www.trellix.com/en-us/downloads/my-products.html>) con registro(s), usuario(s) y clave(s) para administrar el soporte, actualizaciones, parches y demás



- herramientas que tengan que ver con los productos de la Personería de Bogotá, D.C.
- d. El contratista deberá realizar un monitoreo proactivo de la solución Trellix implementada en la Entidad, verificando el correcto funcionamiento de la consola de administración, el estado de los agentes, la operación de los módulos licenciados, la generación de alertas relevantes de seguridad y la aplicación de actualizaciones, con el fin de identificar posibles incidentes, anomalías o fallas operativas y presentar las recomendaciones correspondientes para su tratamiento o remediación.
 - e. Reportar de forma mensual y/o periódica la disponibilidad de los componentes monitoreados, eventos de seguridad que incluyan clasificación, los análisis de riesgos y amenazas emergentes que incluyan nuevas técnicas que pueden afectar los servicios de la entidad, recomendaciones orientadas a contención, erradicación, recuperación y prevención ante eventos e incidentes de seguridad de la información.
 - f. Realizar un análisis de vulnerabilidades a los activos críticos definidos por la Supervisión del contrato, que incluya la identificación y clasificación de las vulnerabilidades encontradas, el respectivo plan de remediación, así como la presentación y socialización de los resultados al personal técnico encargado de los temas de seguridad de la Personería de Bogotá D.C. el documento debe contener como mínimo la siguiente información: Dirección IP, nombre del sistema de información/equipo/servicio evaluado, nivel de riesgo, numero de vulnerabilidades clasificadas en alto, medio, bajo, descripción de la vulnerabilidad, impacto según CVE, tratamiento de la vulnerabilidad, remediaciones y controles compensatorios en cada vulnerabilidad.
 - g. El análisis de vulnerabilidades deberá ser con herramientas de propiedad del proveedor y contar con la respectiva licencia de uso, y realizar dos ciclos de escaneo y análisis de vulnerabilidades uno inicial y otro posterior a la implementación de las remediaciones correspondientes y efectuar la presentación y socialización al equipo de Seguridad de la Información de la Entidad.
 - h. Entregar documento con el plan de trabajo del análisis de vulnerabilidades y cronograma de ejecución, alcance, relación de las herramientas a ser utilizadas en cada etapa.
 - i. Entregar Informe técnico del desarrollo del análisis de vulnerabilidades.
 - j. Ejecutar revisiones mensuales, sin costo adicional para la Personería de Bogotá D.C., durante toda la vigencia contractual, para realizar el mantenimiento preventivo y correctivo de la plataforma de administración del antivirus y de los equipos cliente (computadores y/o servidores).
 - k. Realizar actividades de transferencia de conocimiento y acompañamiento técnico al personal designado por la Entidad, de acuerdo con los niveles de servicio establecidos y requeridos por la Personería de Bogotá D.C.
 - l. Realizar durante la vigencia del contrato, el servicio soporte técnico, de acuerdo con el licenciamiento de los productos renovados, y que cubra como mínimo prestar la atención de manera virtual o presencial para la corrección de fallas que se puedan presentar en el funcionamiento de las herramientas Trellix instaladas en los equipos y servidores de la entidad, así como en la consola de administración de dichas herramientas. Se deben realizar a pedido de la entidad cada vez que se necesario teniendo en cuenta la matriz de escalamiento que surta el contratista.
 - m. Ejecutar durante la vigencia del contrato, un (1) mantenimiento preventivo, el cual consiste en sesiones presenciales o virtuales, para que las herramientas se



mantengan actualizadas y funcionando correctamente para prevenir ataques y amenazas cibernéticas e incluir las siguientes actividades:

- Validar que los servicios que utiliza la consola ePo para el normal funcionamiento
 - Depuración de máquinas que no se han comunicado con la consola ePo por más de 90 días.
 - Verificación del estado de ejecución de las tareas automáticas de despliegue de productos trellix.
 - Ejecución y verificación de consulta acerca del top 10 de amenazas detectadas mensualmente.
 - Ejecución y verificación de consulta acerca del top 10 de equipos con mayores detecciones durante el mes.
 - Verificación del número de sistemas que aún no cuentan con la herramienta de protección antivirus trellix endpoint security.
 - Verificación del estado de la sincronización entre la consola y el directorio activo (si se tiene un AD).
- n. El proveedor debe estar disponible para brindar asesoría en el manejo y configuración de la herramienta durante la vigencia del contrato, sin que esto genere costos adicionales a la Entidad.
- o. Suministrar, para el cumplimiento del contrato, personal técnico especializado, necesario ante eventuales ataques de virus o cualquiera de sus derivados y que llegue a afectar la solución informática, hasta el restablecimiento del servicio en un 100%.

3. Soporte

El cual deberá ser informado al supervisor de contrato en Kick off en los primeros 5 días calendario posterior a la firma del acta de inicio.

- El soporte requerido deberá ser 7x24.

El soporte incluirá lo siguiente:

- **Servicio de asistencia telefónica, virtual y/o por correo electrónico**, para solución de reporte de fallas, notificación de problemas sobre cualquier aspecto del certificado y solicitudes sobre uso del producto.
- **Conexión remota**: Servicio de asistencia telemático a través de conexión remota segura para resolución de problemas relacionados con la solución tecnológica
- **Soporte técnico** para problemas de instalación, configuración, reinstalación e implementación de actualizaciones, y que cubra como mínimo prestar la atención de manera virtual o presencial para la corrección de fallas que se puedan presentar en el funcionamiento de las herramientas Trellix instaladas en los equipos y servidores de la entidad, así como en la consola de administración de dichas herramientas. El servicio deberá brindarse de manera presencial o remota, cuando sea requerido por la Personería de Bogotá D.C., de conformidad



con los acuerdos de nivel de servicio y la matriz de escalamiento presentada por el contratista

- Registrar los casos reportados por la entidad y asignar un número de caso por medio del cual, la entidad podrá hacer el respectivo seguimiento.
 - En caso de ser necesario, el contratista escalará los incidentes reportados al área de soporte del fabricante y con el equipo de desarrollo de producto, para diagnosticar e identificar el problema reportado.
 - El contratista estará encargado del seguimiento al caso hasta su solución y cierre, y reportará a la entidad.
- a. Realizar un (1) mantenimiento preventivo, el cual consiste en sesiones presenciales o virtuales, para que las herramientas se mantengan actualizadas y funcionando correctamente para prevenir ataques y amenazas cibernéticas.
- b. Realizar los mantenimientos correctivos que se generen durante la ejecución del contrato, los cuales deberán ser atendidos con respuesta 7 x 24 (. Siete días por veinticuatro horas)

4. Niveles de soportes

a. Nivel 1. Será brindado por la mesa de servicio de la entidad y corresponde a una primera validación técnica del caso; de ser necesario el Supervisor del Contrato contactará al Contratista por los canales de comunicación establecido para que preste el soporte Nivel 2 que se detalla a continuación. En cualquier caso, la entidad realizará seguimiento hasta el cierre del incidente.

b. Nivel 2. Este servicio será prestado por el contratista, mediante atención telefónica, remota o por correo electrónico, a partir del reporte de la incidencia realizado por la Entidad. La asistencia será brindada por personal técnico especializado y certificado en la solución ofertada, quien atenderá y realizará el seguimiento de los incidentes hasta su respectiva solución o escalamiento.

Dicho personal procederá a registrar el requerimiento de soporte, reunir la información pertinente, y atender el caso hasta su resolución.

c. Nivel 3. Este servicio será brindado por el área de Soporte del ente certificador o fabricante y en caso de ser necesario, con el equipo de soporte de Nivel 1 y 2 del producto. El contratista será el encargado de escalar el caso y de hacerle seguimiento al mismo, hasta su resolución. Los tiempos de respuesta asociados a este nivel no puede superar las 48 horas

5. Acuerdos de Niveles de servicio

a. Crítico. Identificado como falla operativa o técnica de algún componente de la solución antivirus, que indica que se ha producido una condición que afecta total o severamente el servicio y requiere una acción correctiva inmediata, la entidad puede según la urgencia o situación, solicitar al contratista que el caso sea clasificado en un nivel de atención CRÍTICO, en caso de que al inicio del evento no se pueda determinar con claridad cuál es su adecuada clasificación. Si por alguna omisión no queda establecido el nivel en el momento de registro del caso, se asumirá que es CRÍTICO y deberá cumplir con los tiempos



establecidos para éste. El tiempo de respuesta para la atención de un requerimiento categorizado como crítica es máximo de una (1) hora y el tiempo de solución máximo de un (1) día.

b. Intermedio. Indica la existencia de una condición que afecta el servicio en forma parcial o la presencia de una posible degradación que puede llegar a afectar el servicio, requiere la implementación de una acción correctiva. El tiempo de respuesta para la atención de un requerimiento categorizado como intermedio será entre 2 a 4 horas y el tiempo de solución máximo de un (1) día.

c. Leve. Falla operativa o técnica de algún proceso o servicio, sin impedimento apreciable de funcionamiento o de la prestación del servicio y no percibida por el usuario externo. El tiempo de respuesta para la atención de un requerimiento categorizado como leve es máximo de 8 horas y el tiempo de solución máximo de dos (2) días.

6. Transferencia de Conocimiento

El contratista que resulte seleccionado deberá realizar transferencia de conocimiento básico a dos (2) personas en Hacking ético, el cual debe ser dictado por un profesional, certificado ISO 27001 y Ethical Hacking.