

ANEXO 1 - ANEXO TÉCNICO

Contratar la renovación de las licencias de la solución de endpoint de nueva generación actual de la Alcaldía Distrital de Santiago de Cali, requeridas para la protección de los equipos de cómputo, servidores y correo electrónico que conforman la infraestructura tecnológica a cargo del Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones (DATIC).

Objeto

Establecer las especificaciones técnicas mínimas que deberá cumplir el proponente para la renovación de las licencias de la solución de endpoint de nueva generación de la Alcaldía Distrital de Santiago de Cali, requeridas para proteger los equipos de cómputo, servidores y correo electrónico que conforman la infraestructura tecnológica a cargo del DATIC.

Alcance, cantidades y vigencia del licenciamiento

El proponente deberá ofertar y, en caso de resultar adjudicatario, suministrar la totalidad de las licencias relacionadas en la siguiente tabla, con gestión centralizada cien por ciento (100 %) en la nube y una vigencia de doce (12) meses, de acuerdo con las condiciones del proceso.

Nombre	Unidades
XDR for Email (EmDR) [#of users, mailbox if AD sync is unavailable]	6.600
Endpoint Security Essentials [# of endpoints including servers]	4.000
Endpoint Security Pro [# of endpoints including servers]	460
Email and Collaboration Security Core [#of users]	6.600

Las cantidades corresponden a 4.000 licencias para equipos de cómputo, 460 licencias para servidores y 6.600 licencias para cuentas de correo electrónico con XDR. La oferta deberá cubrir todos los componentes y cantidades indicados, sin omisiones.

Requisitos técnicos mínimos de la solución

La solución ofertada deberá cumplir integralmente con todos los requisitos que se enumeran a continuación. Las expresiones “deberá”, “debe” y “se requiere” establecen condiciones obligatorias.

Requisitos generales y consola de administración

- La solución propuesta deberá alcanzar una tasa mínima del 91 % en el componente de analítica de los resultados de la evaluación MITRE Wizard Spider & Sandworm Evaluation Results 2025.
- La consola de administración deberá ser cien por ciento (100 %) en la nube y permitir la administración centralizada de endpoints, servidores y correo electrónico.
- La consola deberá ser accesible mediante navegador web desde cualquier ubicación.
- Deberá permitir crear grupos, importar grupos desde Active Directory y asignar políticas diferenciadas a los mismos.
- Deberá permitir la creación de múltiples usuarios administradores con distintos niveles de acceso, roles, permisos y estructura jerárquica de control.
- Deberá contar con un módulo de generación de reportes.

ANEXO 1 - ANEXO TÉCNICO

Contratar la renovación de las licencias de la solución de endpoint de nueva generación actual de la Alcaldía Distrital de Santiago de Cali, requeridas para la protección de los equipos de cómputo, servidores y correo electrónico que conforman la infraestructura tecnológica a cargo del Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones (DATIC).

- Deberá notificar los intentos de infección de virus de acuerdo con los parámetros definidos por el administrador, así como generar notificaciones inmediatas y centralizadas sobre ataques masivos de virus o código malicioso.
- Deberá contar con un dashboard que muestre en tiempo real la incidencia de virus, el estado de actualización de las máquinas, alertas, avisos y errores.
- Deberá permitir visualizar de forma sencilla el estado de las estaciones de trabajo y servidores, las estadísticas de infecciones y los equipos en los que ocurrió una detección o infección.
- Deberá mostrar el estado de actualización de firmas, identificando la cantidad de equipos actualizados y desactualizados.
- Deberá permitir agregar, modificar y eliminar grupos de clientes, aplicando políticas diferentes.
- Deberá permitir la configuración y modificación remota de los antivirus en los clientes, mediante reglas aplicables a un equipo o a un grupo de equipos.
- Deberá incluir actualizaciones automáticas de las listas de definiciones de virus desde una ubicación en la nube y permitir que los equipos móviles obtengan actualizaciones desde el servidor local más cercano o directamente desde Internet.
- Deberá permitir la integración con Active Directory mediante LDAP.
- Deberá ser compatible con ambientes virtualizados y permitir la aplicación de políticas por computador.
- Deberá proteger los procesos y archivos propios de la herramienta contra manipulaciones y contra la remoción no autorizada del agente mediante contraseña.

1. Protección antimalware y capacidades de prevención

- Deberá ofrecer protección antimalware para endpoints con Windows y macOS, y para servidores con Windows y Linux.
- Deberá integrar protección antivirus, antispyware, prevención de intrusos y control de dispositivos en un solo agente, sin requerir aplicaciones adicionales para la comunicación con la consola.
- Deberá contar con un único agente para la protección y comunicación con la consola; la herramienta deberá presentar un único ícono en el área de notificación de la barra de tareas.
- Deberá incluir servicios de limpieza de daños en tiempo real para eliminar remanentes de virus, troyanos, spyware y entradas maliciosas en el registro del sistema.
- Deberá permitir ejecutar acciones posteriores a la detección de virus o ataques, como limpiar archivos infectados, enviarlos a cuarentena, eliminarlos o no tomar acción, según la configuración autorizada.
- Deberá permitir excluir archivos, carpetas y procesos específicos de la exploración.
- Deberá detectar y eliminar programas potencialmente no deseados, incluidos adware, spyware, joke programs, keyloggers, trackware, hacktools, herramientas de acceso remoto y dialers.
- Deberá permitir la programación de tareas de exploración y actualización, entre otras.
- Deberá registrar eventos y mostrar, como mínimo, riesgos, amenazas, fecha y hora del evento, host (IP, MAC, sistema operativo y usuario), tipo de amenaza, acción afectada, número de detecciones, ubicación y nombre del archivo.

ANEXO 1 - ANEXO TÉCNICO

Contratar la renovación de las licencias de la solución de endpoint de nueva generación actual de la Alcaldía Distrital de Santiago de Cali, requeridas para la protección de los equipos de cómputo, servidores y correo electrónico que conforman la infraestructura tecnológica a cargo del Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones (DATIC).

- Deberá escanear y bloquear en tiempo real el acceso e instalación de spyware, adware, malware, keyloggers, herramientas de administración remota, dialers, trackware y hacktools, entre otros.
- Deberá evitar que programas maliciosos modifiquen el registro del sistema.
- Deberá incluir control de URL maliciosas basado en reputación y análisis de descargas por reputación, con consulta a sistemas de reputación en la nube que recopilen información sobre amenazas a nivel mundial.
- Deberá incluir control de dispositivos extraíbles y periféricos, tales como USB, unidades de CD y Bluetooth; deberá permitir bloquear dispositivos, restringirlos a solo lectura, impedir la ejecución de aplicaciones desde ellos y definir qué dispositivos están autorizados.
- Deberá incluir HIPS/IPS/IDS, detección de tráfico malicioso (MTD), prevención anti-exploit y permitir al administrador crear firmas o reglas personalizadas de IDS/IPS.
- Deberá incluir prevención básica de fuga de datos (DLP), soportada por el mismo agente de protección de endpoint.
- Deberá permitir programar, por fecha y hora, reglas para el control de aplicaciones y dispositivos.
- Deberá permitir controlar aplicaciones, procesos, archivos, carpetas, registros, módulos y bibliotecas DLL; restringir actividades sospechosas o de alto riesgo y controlar la ejecución mediante hash o registro de la aplicación en la consola.
- Deberá permitir proteger archivos confidenciales mediante reglas de seguridad y crear conjuntos de sitios web accesibles únicamente para determinados grupos de usuarios.
- Deberá permitir bloquear servidores específicos o crear reglas según niveles de criticidad y reputación de URL.
- Deberá permitir monitorear cambios en archivos específicos de servidores y en llaves del registro.
- Deberá proteger los navegadores Internet Explorer, Firefox, Chrome, Opera y Safari, bloqueando sitios infectados conocidos y comprobando los datos descargados antes de su ejecución.
- Deberá incluir protección contra ransomware basada tanto en firmas como en comportamiento (Cryptoguard o funcionalidad equivalente), detectar e interrumpir automáticamente procesos de cifrado malicioso aunque no exista una firma conocida y bloquear procesos comúnmente asociados con ransomware.
- Deberá detectar y proteger contra amenazas de día cero y amenazas desconocidas mediante tecnologías basadas en comportamiento, machine learning o deep learning, incluyendo malware oculto en aplicaciones legítimas (code cave) y técnicas de explotación de DLL Injection.
- Deberá proteger o monitorear frente a programas sospechosos que intenten incrustar complementos en navegadores, instalar bibliotecas maliciosas o modificar archivos del sistema.
- Deberá contar con un módulo que proteja contra el cifrado no autorizado del sector de arranque (boot) del disco duro.
- Deberá permitir localizar brechas de seguridad y eliminarlas.
- Deberá integrarse con sistemas de correlación de eventos (SIEM).

ANEXO 1 - ANEXO TÉCNICO

Contratar la renovación de las licencias de la solución de endpoint de nueva generación actual de la Alcaldía Distrital de Santiago de Cali, requeridas para la protección de los equipos de cómputo, servidores y correo electrónico que conforman la infraestructura tecnológica a cargo del Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones (DATIC).

- Deberá disponer de un módulo de amenazas que permita consultar detalles del malware detectado en endpoints y marcar los incidentes como resueltos o no resueltos.
- Deberá permitir filtrar las máquinas por nombre y evitar duplicidad de equipos por ese campo.
- Deberá enviar periódicamente informes de seguridad por correo electrónico al administrador de la plataforma, independientemente del servicio de correo que se encuentre en uso.
- Deberá permitir un modo de coexistencia para evaluar el funcionamiento de la herramienta sin detener los procesos de la Entidad.

1.1. Sistemas operativos compatibles

La solución deberá soportar sistemas operativos de 32 o 64 bits, de acuerdo con el siguiente mínimo indicado en los estudios previos:

- Windows 8, Windows 8.1, Windows 10 y versiones posteriores, con sus últimas actualizaciones.
- Windows Server 2012, Windows Server 2016 y versiones posteriores.
- macOS 10.13 y versiones posteriores.
- Linux/Unix: Amazon Linux y Amazon Linux 2; CentOS 6/7/8; Debian 8, 9 y 10; Oracle Linux 6/7/8; Red Hat Enterprise Linux 6/7/8; SUSE/SUSE Enterprise Linux 11; Ubuntu 16.04 y versiones posteriores; Solaris.

La solución deberá soportar, para endpoints, puestos de trabajo fijos y móviles en plataformas Intel y AMD, los sistemas operativos señalados en este anexo; y para servidores, los sistemas Windows y Linux relacionados

1.2. Reportes y auditoria

- Deberá generar reportes gráficos desde la consola centralizada, sin requerir productos adicionales.
- Deberá permitir reportes sobre riesgos, cumplimiento de políticas, exploraciones, estado de los equipos, estado de licencias e historial de ataques de los últimos treinta (30) días, según se requiera.

1.3. Requisitos de EDR (Endpoint Detection and Response)

- La consola deberá incluir un módulo EDR para todas las máquinas contempladas por la Alcaldía Distrital de Santiago de Cali.
- La gestión EDR deberá realizarse desde la misma consola de antivirus en la nube, sin licencias adicionales ni un agente adicional en los equipos finales.
- La solución EDR deberá ser cien por ciento (100 %) cloud y permitir la elaboración de análisis de causa raíz.
- La herramienta de gestión de incidentes deberá presentar las alertas de amenazas organizadas en casos para facilitar su gestión.

ANEXO 1 - ANEXO TÉCNICO

Contratar la renovación de las licencias de la solución de endpoint de nueva generación actual de la Alcaldía Distrital de Santiago de Cali, requeridas para la protección de los equipos de cómputo, servidores y correo electrónico que conforman la infraestructura tecnológica a cargo del Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones (DATIC).

- Deberá permitir aislar máquinas que presenten posibles amenazas. Durante el aislamiento se deberán cortar automáticamente las comunicaciones hacia Internet, carpetas compartidas y conexiones SSH; la única comunicación permitida será con la consola de administración del endpoint.
- Deberá permitir buscar y detectar amenazas en endpoints mediante hash, nombre de archivo, direcciones IP, dominios completos o parciales y líneas de comandos.

1.4. Protección de correo electrónico y colaboración

- Deberá proteger las 6.600 cuentas de correo electrónico de la Entidad, con XDR y gestión centralizada cien por ciento (100 %) en la nube.
- Deberá integrarse directamente con el tenant de la solución de correo en la nube mediante API.
- Deberá bloquear URL maliciosas y archivos con malware detectados en los cuerpos y archivos adjuntos de los correos electrónicos.
- Deberá analizar malware en cuerpos y adjuntos de correo mediante técnicas de machine learning.
- Deberá bloquear URL maliciosas en cuerpos y adjuntos utilizando listas de reputación.
- Deberá detectar mensajes con intentos de robo de credenciales o phishing.
- Deberá detectar mensajes con intentos de fraude o técnicas BEC (Business Email Compromise).
- Deberá contar con análisis tipo sandbox para URL, archivos y MAC, según lo establecido en los estudios previos.

2. Servicios obligatorios asociados al licenciamiento

- El contratista deberá realizar la instalación y el despliegue de todas las licencias de protección de correo, endpoint (antivirus) y EDR adquiridas por la Entidad.
- El contratista deberá verificar y validar que la renovación del licenciamiento se haya ejecutado correctamente, de conformidad con las condiciones técnicas y el alcance del proceso.
- Deberá suministrar soporte técnico 5x8 para escalar incidentes o tickets relacionados con la solución. El tiempo de respuesta sobre el estado de la solicitud no podrá ser superior a cuatro (4) horas. El soporte podrá prestarse por web, correo electrónico, teléfono o de manera presencial.

3. Obligación de presentar fichas técnicas

OBLIGATORIEDAD: El proponente deberá adjuntar con su oferta las fichas técnicas oficiales de los bienes, licencias, productos y/o servicios que propone suministrar, expedidas o publicadas por el fabricante de la solución. Las fichas deberán permitir identificar claramente la marca, el producto, la versión o edición aplicable y las funcionalidades ofrecidas, y deberán aportar información suficiente para verificar el cumplimiento de cada uno de los requisitos técnicos mínimos establecidos en este Anexo.

ANEXO 1 - ANEXO TÉCNICO

Contratar la renovación de las licencias de la solución de endpoint de nueva generación actual de la Alcaldía Distrital de Santiago de Cali, requeridas para la protección de los equipos de cómputo, servidores y correo electrónico que conforman la infraestructura tecnológica a cargo del Departamento Administrativo de las Tecnologías de la Información y las Comunicaciones (DATIC).

- Las fichas técnicas deberán corresponder a los productos efectivamente ofertados y guardar consistencia con la propuesta técnica.
- El proponente deberá señalar en su propuesta, para cada requisito técnico, la ficha técnica, página, apartado o documento donde se evidencia su cumplimiento.
- La presentación de fichas técnicas no exime al proponente de cumplir la totalidad de los requisitos establecidos en este Anexo, ni reemplaza otros documentos exigidos en el pliego de condiciones.
- La Entidad podrá verificar la información aportada y solicitar las aclaraciones o verificaciones que resulten procedentes conforme a las reglas del proceso de selección.

4. Declaración de cumplimiento del proponente

Con la presentación de la oferta, el proponente deberá manifestar que conoce y acepta las especificaciones técnicas de este Anexo y que la solución ofertada cumple integralmente con todos los requisitos mínimos, cantidades, funcionalidades, compatibilidades y servicios exigidos. En caso de resultar adjudicatario, se obliga a suministrar y mantener durante la vigencia contractual el licenciamiento y las funcionalidades ofertadas, así como a ejecutar la instalación, el despliegue, la validación y el soporte en los términos aquí previstos.

Razón social del proponente:

Nombre del representante legal: _____

Firma: _____

Fecha: _____