Fecha (Mes y año):	Septiembre del 2026				
Proceso solicitante:	Gestión Informática				
DATOS DE LA SOLICITUD					
Tipo de Solicitud:	Bienes		Servicios	X	Obra

DESCRIPCIÓN

La Unidad Ejecutora de Saneamiento del Valle del Cauca – UESVALLE requiere contratar la renovación, por un término de dos (2) años, de las licencias de ESET PROTECT Complete para la protección del servidor y los equipos de cómputo de la Entidad, incluyendo los servicios de soporte técnico, configuración, capacitación y validación de su adecuado funcionamiento; así como la renovación, por el mismo término, de las licencias de ESET Secure Authentication para la implementación de mecanismos de doble autenticación en los servicios y sistemas institucionales que defina la Entidad.

JUSTIFICACIÓN

El artículo 43 de la Ley 715 de 2001 establece que corresponde a los departamentos dirigir, coordinar y vigilar el sector salud y el Sistema General de Seguridad Social en Salud en el territorio de su jurisdicción, atendiendo las disposiciones nacionales sobre la materia.

EL DEPARTAMENTO DEL VALLE DEL CAUCA conforme la ley 715 de 2001 debe desarrollar acciones de promoción, prevención, pedagogía, gestión, inspección, vigilancia y control, de los factores de riesgo ambientales, hábitat, del consumo, biológicos y del comportamiento, dentro de los cuales se encuentran la vigilancia de la calidad del agua de consumo humano, de los residuos sólidos incluidos los especiales y peligrosos, de los desechos líquidos, de las aguas de uso recreacional, de la calidad del aire, la vigilancia y control al uso y aplicaciones de plaguicidas, radiaciones ionizantes, saneamiento en edificaciones de establecimientos públicos, a los alimentos, bebidas alcohólicas, medicamentos, enfermedades zoonóticas y enfermedades de trasmisión vectorial. Varias de estas actividades son realizadas por la SECRETARIA DE SALUD DEPARTAMENTAL DE SALUD, a través de la Unidad Ejecutora de Saneamiento del Valle del Cauca - UESVALLE.

Con el Decreto 1798 de 2017, la Gobernadora del Valle del Cauca, aprobó el acuerdo No. 11 de noviembre 14 de 2017, expedido por el Consejo Directivo de la Unidad Ejecutora de Saneamiento del Valle del Cauca, el cual contiene los Estatutos internos de la Entidad; que hacen explicito, el facultar a la UESVALLE en el desarrollo de acciones a nivel departamental, mediante la asistencia y acompañamiento técnico que permite intervenir los problemas de salud ambiental identificados en las actividades de inspección, vigilancia y control, que regularmente se hacen como cuerpo de apoyo operativo de la Secretaría Departamental de Salud.

La Unidad Ejecutora de Saneamiento del Valle del Cauca – UESVALLE requiere mantener y fortalecer las medidas de seguridad informática implementadas para la protección de su infraestructura tecnológica y de la información institucional. En este contexto, resulta necesario renovar, por un término de dos (2) años, 170 licencias de la solución de seguridad ESET PROTECT Complete destinadas a la protección del servidor y de los equipos de cómputo de la Entidad, incluyendo los servicios técnicos asociados de soporte, configuración, actualización, capacitación, acompañamiento y validación de su adecuado funcionamiento.

La renovación de estas licencias resulta necesaria para garantizar la continuidad de los mecanismos de protección de los equipos y recursos tecnológicos institucionales frente a diferentes tipos de amenazas informáticas, contribuyendo a prevenir, detectar y mitigar eventos que puedan afectar la disponibilidad, integridad y confidencialidad de la información y el normal funcionamiento de los sistemas y servicios tecnológicos de la Entidad.

La solución de seguridad deberá proporcionar mecanismos de protección frente a amenazas que puedan ingresar o propagarse a través de la navegación web, aplicaciones, dispositivos externos, archivos y demás elementos asociados al uso de los equipos institucionales, así como capacidades de detección y prevención frente a código malicioso, malware, ransomware y otras amenazas que puedan comprometer los recursos tecnológicos de la Entidad, de acuerdo con las características y funcionalidades de la solución contratada.

La continuidad de esta protección permitirá reducir la exposición de la Entidad a incidentes de seguridad que puedan ocasionar pérdida, alteración, cifrado, secuestro o divulgación no autorizada de información, afectaciones sobre los sistemas y bases de datos institucionales, indisponibilidad de servicios tecnológicos o compromiso de los equipos de cómputo, situaciones que podrían afectar el desarrollo normal de las actividades misionales y administrativas de la UESVALLE.

De manera complementaria, la Entidad requiere renovar seis (6) licencias de ESET Secure Authentication, por un término de dos (2) años, como mecanismo adicional para fortalecer los controles de acceso a determinados servicios y recursos tecnológicos institucionales mediante mecanismos de doble autenticación, de acuerdo con las necesidades de seguridad definidas por la Entidad. La articulación de estos mecanismos de protección de los equipos y de control de acceso contribuye al fortalecimiento de la seguridad de la infraestructura tecnológica institucional y a la gestión de los riesgos asociados al uso de las tecnologías de información y comunicaciones.

En consecuencia, con el propósito de garantizar la continuidad de los controles de seguridad informática, fortalecer la protección de la infraestructura tecnológica y mitigar los riesgos asociados a las amenazas cibernéticas, se hace necesario adelantar la contratación correspondiente para la renovación de las licencias de seguridad Endpoint y de las licencias de doble autenticación, junto con los servicios técnicos asociados, de conformidad con las necesidades y especificaciones técnicas establecidas por la Entidad.

Conforme a lo anterior, y en aras de garantizar el cumplimiento de lo establecido en la descripción de la presente solicitud, se requiere adelantar la contratación de los bienes y servicios relacionados, de acuerdo con la siguiente Clasificación Central de Productos (CPC), cuando aplique:

ITEM	CPC*	NOMBRE (Según Tabla del Dane)	CANTIDAD
1	83152	ESET PROTECT Complete	170
2	83152	ESET Secure Authentication	6

ESET PROTECT Complete:

ITEM	Categoría	Característica / Especificación
01	Administración	Consola de gestión Cloud

02	Administración	Gestión de usuarios basada en RBAC
03	Administración	Gestión de sistemas operativos Windows, Linux y Mac
04	Administración	Organización de infraestructura por AD, grupos estáticos y dinámicos
05	Integración	Integración con herramientas SIEM y generación de registros en formato JSON o LEEF
06	Reportes	Informes personalizados sobre distintas categorías
07	Protección Endpoint	Defensa para sistemas heterogéneos: Windows, Mac y Linux
08	Protección Endpoint	Escudo contra ransomware en Endpoint / Servidor
09	Protección Endpoint	Bloqueo contra ataques dirigidos
10	Control	Control de dispositivos
11	Control	Filtrado de navegación web por URL / categorías
12	Protección avanzada	Machine Learning
13	Protección avanzada	Bloqueo de Exploits
14	Protección avanzada	Detección de comportamiento HIPS
15	Protección avanzada	Telemetría para comprobar la reputación de procesos en ejecución y archivos
16	Detección	Correlación de detecciones e incidentes
17	Protección avanzada	Detección y bloqueo de ataques automáticos o DDOS
18	Ransomware	Ransomware Remediation
19	Ransomware	Restauración automática de archivos cifrados cuando se detecta ransomware en una fase posterior del ataque
20	Compatibilidad	Soporte para extensiones: MP3, 7z, rar, zip, csv, dat, sql, xml, bat, bin, gif, jpeg, jpg, png, html, ppt, pptx, java, xls, xlsx, mp4, doc, docx, pdf y txt
21	Detección	Detección de amenazas Zero-Day
22	Protección avanzada	Sandboxing basado en la nube
23	Detección	Análisis profundo de comportamiento
24	Movilidad	Protección contra amenazas en celulares / tablets Android
25	Movilidad	Filtrado de llamadas y mensajería de texto
26	Movilidad	Control de aplicaciones para equipos móviles
27	Movilidad	Módulo Anti-Theft
28	Cifrado	Cifrado de disco Windows - Mac
29	Cifrado	Algoritmo de cifrado AES a 256 bits
30	Autenticación	Autenticación en el sistema a SSO para inicio del usuario en máquina
31	Correo y colaboración	Protección avanzada para aplicaciones de Microsoft 365 y Google Workspace ante malware, phishing y spam
32	Protección avanzada	Defensa avanzada contra amenazas
33	Correo y colaboración	Gestión en consola de correo a nivel Multi Tenant
34	Correo y colaboración	Exploración del tráfico de correos electrónicos y detección de correos maliciosos
35	Correo y colaboración	Protección contra suplantación de identidad (Spoofing)
36	Correo y colaboración	Protección a nivel de tenant, usuarios y grupos
37	Vulnerabilidades	Gestión de parches y vulnerabilidades
38	Vulnerabilidades	Análisis automatizado del sistema operativo y aplicaciones de terceros
39	Vulnerabilidades	Informes de vulnerabilidad del software y dispositivos más expuestos al riesgo
40	Vulnerabilidades	Métricas de explotabilidad CVSS V3 y descripción de impacto según CIA
41	Vulnerabilidades	Puntuación del riesgo considerando CVSSv2/CVSSv3, popularidad de CVE, ciclo de vida de CVE y tasa de riesgo comprometido
42	Vulnerabilidades	Priorización de parches y remediaciones basada en criticidad
43	Vulnerabilidades	Gestión del ciclo de vida de vulnerabilidades con mitigación automatizada
44	Vulnerabilidades	Parcheo de vulnerabilidades de forma automática y manual
45	Vulnerabilidades	Análisis de miles de aplicaciones y detección de más de 35.000 vulnerabilidades y exposiciones comunes (CVE)

ESET Secure Authentication:

	Característica técnica	Descripción
1	Autenticación multifactor	MFA/2FA para reforzar el acceso mediante un segundo factor.
2	Protección contra accesos no autorizados	Protección frente a accesos no autorizados y robo de credenciales.
3	Notificación Push	Autenticación mediante notificaciones Push.
4	Contraseñas de un solo uso (OTP)	Generación de contraseñas de un solo uso.
5	OTP basado en tiempo (TOTP)	Contraseñas de un solo uso basadas en tiempo.
6	OTP basado en eventos (HOTP)	Contraseñas de un solo uso basadas en eventos.
7	OTP mediante SMS	Entrega de códigos OTP mediante SMS.
8	OTP mediante correo electrónico	Entrega de códigos OTP mediante correo electrónico.
9	Tokens de hardware	Soporte para tokens físicos de autenticación.
10	FIDO y llaves de seguridad	Soporte para FIDO y llaves de seguridad.
11	Microsoft Authenticator y Google Authenticator	Compatibilidad con Microsoft Authenticator y Google Authenticator.
12	Aplicación móvil	Aplicación móvil para Android e iOS.
13	Inicio de sesión en Windows	Protección del inicio de sesión en Windows.
14	Remote Desktop Protocol (RDP)	Protección de accesos mediante RDP.
15	VPN	Protección de accesos mediante VPN.
16	Aplicaciones web	Protección de accesos a aplicaciones web.
17	Outlook Web Access (OWA)	Protección de accesos mediante OWA.
18	Microsoft Active Directory	Integración con Microsoft Active Directory.
19	Active Directory Federation Services (AD FS)	Integración con AD FS.
20	RADIUS	Integración mediante protocolo RADIUS.
21	SAML	Integración mediante SAML para aplicaciones y servicios en la nube.
22	Servicios y aplicaciones cloud	Protección de servicios y aplicaciones cloud compatibles.
23	Sistemas operativos	Protección para Windows, macOS y Linux.
24	Escalamiento de privilegios	Protección frente al escalamiento de privilegios.
25	Consola web de administración centralizada	Administración centralizada mediante consola web.
26	Gestión de usuarios	Gestión y administración de usuarios.
27	Autoinscripción (self-enrollment)	Permite la autoinscripción de usuarios.
28	Multitenancy	Administración de múltiples empresas o entornos.
29	Implementación Cloud	Implementación en la nube.
30	Implementación On-Premises	Implementación local (On-Premises).
31	Modo offline	Funcionamiento offline para determinados métodos de autenticación.
32	Biometría del dispositivo móvil	Uso de biometría del dispositivo móvil cuando está disponible.
33	PIN de la aplicación móvil	Protección de la aplicación móvil mediante PIN.
34	Registro e informes	Registro e informes de eventos de autenticación.
35	API REST	API REST para integrar aplicaciones personalizadas.
36	SDK	SDK para integrar MFA en sistemas y aplicaciones propietarias.
37	VPN y RADIUS	Compatibilidad con soluciones VPN y servicios basados en RADIUS.
38	Tokens HOTP / OATH	Soporte de tokens HOTP compatibles con OATH.
39	Métodos personalizados de OTP	Posibilidad de utilizar métodos personalizados de entrega de OTP.

Las obligaciones específicas del contratista serán las siguientes:

1. Suministrar, activar y mantener vigentes las ciento setenta (170) licencias de ESET Endpoint Security, por un término de dos (2) años, destinadas a la protección de los servidores y equipos de trabajo definidos por la Unidad Ejecutora de Saneamiento del Valle del Cauca – UESVALLE.
2. Suministrar, activar y mantener vigentes las seis (6) licencias de ESET Secure Authentication, por un término de dos (2) años, destinadas a fortalecer los mecanismos de control de acceso y autenticación de los servicios y recursos tecnológicos definidos por la Unidad Ejecutora de Saneamiento del Valle del Cauca – UESVALLE.
3. Garantizar que las licencias suministradas sean legítimas, originales, vigentes y funcionales, y que se encuentren debidamente asociadas a la plataforma de administración correspondiente durante todo el plazo de ejecución contractual.
4. Realizar la activación, instalación, configuración, parametrización y puesta en funcionamiento de las soluciones contratadas en los equipos, servidores y recursos tecnológicos que determine la Entidad, de acuerdo con el alcance de las respectivas licencias.
5. Implementar, configurar y mantener disponible la consola de administración centralizada de la solución Endpoint Security, permitiendo al personal autorizado por la Entidad realizar labores de administración, monitoreo, consulta del estado de protección, gestión de alertas y generación de reportes, de acuerdo con las funcionalidades disponibles en la solución contratada.
6. Mantener habilitados los mecanismos de protección de los equipos y servidores frente a virus, malware, spyware, ransomware y demás amenazas informáticas contempladas dentro del alcance y funcionalidades de la solución Endpoint Security contratada.
7. Configurar y mantener habilitadas las funcionalidades de protección frente a amenazas provenientes de archivos, aplicaciones, dispositivos externos, navegación web y demás vectores contemplados dentro del alcance de la solución contratada.
8. Configurar y mantener las políticas de seguridad y protección requeridas por la Entidad, de acuerdo con sus necesidades, lineamientos de seguridad informática y las funcionalidades disponibles en las soluciones contratadas. .
9. Realizar mensualmente la verificación del estado de protección de los equipos administrados mediante la solución, identificando, cuando corresponda, equipos sin protección, componentes desactualizados, amenazas detectadas, eventos de seguridad y demás alertas relevantes generadas por la plataforma, e informar los resultados al supervisor.
10. Brindar soporte técnico especializado durante toda la vigencia contractual para atender incidentes, errores de instalación, problemas de actualización, configuración, administración y funcionamiento de las soluciones contratadas.
11. Atender los requerimientos técnicos formulados por el supervisor o por el personal autorizado por la Entidad a través de los canales de atención dispuestos por el contratista, incluida su Mesa de Ayuda, de conformidad con los tiempos de respuesta y solución establecidos en los Acuerdos de Nivel de Servicio (ANS).
12. Brindar capacitación y transferencia de conocimiento al personal técnico designado por la Entidad sobre la administración de Endpoint Security, configuración de políticas, monitoreo, consulta de eventos, generación de reportes y gestión de alertas, así como sobre la administración de ESET Secure Authentication, en lo que resulte aplicable.
13. Informar oportunamente al supervisor sobre incidentes, vulnerabilidades, alertas críticas o situaciones identificadas durante la prestación del servicio que puedan comprometer la seguridad de los equipos, servidores, recursos tecnológicos o información institucional, indicando las acciones recomendadas o implementadas para su atención.
14. Realizar las actividades de actualización, reinstalación, configuración, parametrización o ajuste de los componentes de las soluciones contratadas que resulten necesarias para garantizar la

continuidad de su funcionamiento y protección, dentro del alcance de las licencias y servicios contratados.

15. Garantizar la continuidad y vigencia de las licencias durante los dos (2) años de ejecución contractual, evitando interrupciones atribuibles al proceso de activación, configuración o gestión de las licencias por parte del contratista.
16. Mantener la confidencialidad y reserva de la información a la que tenga acceso con ocasión de la ejecución del contrato y abstenerse de utilizarla, reproducirla, divulgarla o suministrarla a terceros para fines diferentes de los relacionados con el objeto contractual.

	Funcionario(a) que realiza la solicitud	**Visto bueno Subdirector(a)**	**Aprobación del (la) Director(a) General**
Nombre:	María Rosario Tasamá Jiménez	Julián Eduardo Montoya Ramírez	Constanza Ivette Hernández Rojas
Cargo:	Profesional Universitario	Subdirector Administrativo	Directora General
Firma:			