

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 1 de 8

1. INFORMACIÓN GENERAL DEL CONTRATO

Contratista	<i>Oscar Giovanni Henao Cárdenas</i>
Informe de Actividades N°.	<i>Final</i>
Período	<i>9 de noviembre al 31 de diciembre de 2025</i>
Número del Contrato	<i>845-2025</i>
Objeto:	<i>PRESTACIÓN DE SERVICIOS PROFESIONALES PARA DISEÑAR E IMPLEMENTAR ACCIONES ESTRATÉGICAS PARA FORTALECER LA GESTIÓN DE TECNOLOGÍA Y LAS CONDICIONES DE SEGURIDAD DIGITAL AL INTERIOR DE LA ADMINISTRACIÓN MUNICIPAL SECTOR CENTRAL.</i>
Plazo	<i>Dos (2) meses y (22) días</i>
Valor Total del Contrato	<i>DIEZ MILLONES CIENTO TRECE MIL TRECIENTOS TREINTA Y TRES PESOS M/CTE. (\$10.113.333).</i>
Valor del Periodo del Informe	<i>\$ 2.713.333</i>
Fecha de Inicio	<i>10 de octubre de 2025</i>
Fecha de Terminación	<i>31 de diciembre de 2025</i>
Plan, Programa o Proyecto	<i>FORTALECIMIENTO DEL ECOSISTEMA DIGITAL EN EL MUNICIPIO DE SANTA ROSA DE CABAL</i>
Supervisora Encargada	<i>Martha Jeny Agudelo Romero</i>
Secretaría	<i>Secretaria de Planeación – Subsecretaria TIC.</i>

ADICION	N.A
PRORROGA	N.A
TERMINACION FINAL	<i>31 de diciembre de 2025</i>
DISPONIBILIDAD	1400 del 01/10/2025
REGISTRO PRESUPUESTAL	1737 del 08/10/2025

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 2 de 8

RUBRO	2.3.2.02.02.008 SERVICIOS PRESTADOS A LAS EMPRESAS Y SERVICIOS DE PRODUCCIÓN
--------------	--

2. INFORMACIÓN TÉCNICA – DATOS GENERALES DE INTERVENCIÓN

CATEGORIA/GRUPO POBLACIONAL	RANGOS EDADES	N° PARTICIPANTES	GÉNERO	
			F	M
HOMBRES	0-60 AÑOS EN ADELANTE	40.229		X
MUJERES	0-60 AÑOS EN ADELANTE	42.240	X	

Rangos de Edades: 0 – 5 años (), 6 – 12 años (), 13 – 17 años (), 18 – 26 años (), 27 – 60 años () y Mayores de 60 ().

PERTENENCIA ÉTNICA						VULNERABILIDAD							
Afro		Indígenas		Mestizos		Discapacitados		Desplazados		Red Unidos		Damnificados	
F	M	F	M	F	M	F	M	F	M	F	M	F	M
SIN DATOS						SIN DATOS							

BENEFICIARIOS POR ZONA	
URBANA	RURAL
69.857	12.612

INSTITUCIONES INTERVENIDAS		
URBANA	RURAL	TOTAL
NO APLICA	NO APLICA	NO APLICA

3. DESARROLLO DEL CONTRATO

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 3 de 8

OBJETIVOS O ALCANCES DEL CONTRATO	ACTIVIDAD DESARROLLADA	REGISTRO	OBSERVACIONES
1. Implementar y gestionar soluciones avanzadas de ciberseguridad, incluyendo la configuración de firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), y software antivirus, garantizando la protección de la infraestructura tecnológica de la Alcaldía.	Se realizó mantenimiento y revisión técnica de la solución antivirus institucional, verificando el funcionamiento óptimo de las consolas de administración y la actualización de firmas. Se mantuvo la operación estable del sistema WatchGuard Cloud, garantizando protección activa en estaciones y servidores críticos. Se realizó la creación y aprovisionamiento de dos servidores virtuales en el entorno VMware ESXi, los cuales estarán destinados a la instalación y configuración de la plataforma de monitoreo y gestión de seguridad Wazuh para la detección y prevención de intrusiones (IDS/IPS) 1. Creación de máquinas virtuales: Se han generado dos instancias denominadas WAZUH y WAZUH 2, considerando la disponibilidad de recursos del host y los requerimientos del sistema para garantizar un óptimo rendimiento durante las operaciones de análisis, monitoreo y correlación de eventos de seguridad. Se verificó la correcta asignación de los recursos y la conexión de red de cada máquina virtual, asegurando que ambas se encuentren accesibles y listas para el proceso de instalación. 4. Validación de estado inicial: Las máquinas virtuales fueron dejadas en estado de apagado, con la imagen ISO correspondiente ya montada, para proceder con la instalación y configuración de Wazuh, de acuerdo con las políticas de seguridad y lineamientos técnicos establecidos por la entidad.	Evidencia punto 1	

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 4 de 8

OBJETIVOS O ALCANCES DEL CONTRATO	ACTIVIDAD DESARROLLADA	REGISTRO	OBSERVACIONES
	2. Asignación y configuración de recursos de hardware: WAZUH: 8 vCPUs, 8 GB de memoria RAM, 200 GB de disco duro provisionado, adaptador de red configurado en VM Network, e inclusión de la imagen ISO Ubuntu 24.04.2 Desktop para su instalación. WAZUH 2: 4 vCPUs, 8 GB de memoria RAM, 60 GB de disco duro provisionado, adaptador de red configurado en VM Network, e inclusión de la imagen ISO Ubuntu 24.04.2 Desktop. 3. Configuración de conectividad y disponibilidad:		
2. Monitorear proactivamente las plataformas de seguridad, como la consola web del antivirus, para detectar intrusiones y amenazas, y ejecutar acciones correctivas rápidas en caso de incidentes de seguridad.	Se realizó el monitoreo constante de la consola web del antivirus WatchGuard. Como resultado, se detectaron múltiples intentos de acceso a URLs maliciosas (clasificadas como "URL con malware") en estaciones de trabajo, los cuales fueron bloqueados oportunamente por el sistema de Protección Web. Se adjunta el informe de amenazas como respaldo de esta actividad. Se realizó el monitoreo constante de la consola web del antivirus WatchGuard. Como resultado, se detectaron múltiples intentos de acceso a páginas de Phishing en estaciones de trabajo, los cuales fueron bloqueados oportunamente por el sistema de Protección Web. Se adjunta el informe de amenazas como respaldo de esta actividad. Se realizó revisión y seguimiento a los informes ejecutivos generados por la consola de administración del antivirus WATCHGUARD CLOUD. desde (diciembre de 2025)	Evidencia punto 2	

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 5 de 8

OBJETIVOS O ALCANCES DEL CONTRATO	ACTIVIDAD DESARROLLADA	REGISTRO	OBSERVACIONES
3. Aplicar y asegurar el cumplimiento de las políticas de seguridad y privacidad de la información, alineadas con las leyes y regulaciones de protección de datos y seguridad informática.	Se está monitoreando y aplicando activamente el cumplimiento de las políticas de seguridad y privacidad de la información, alineadas con la normativa vigente. Como evidencia de ello, el antivirus WatchGuard está bloqueando de forma automática los intentos de conexión de dispositivos USB en los equipos de la Alcaldía de Santa Rosa de Cabal, lo cual contribuye a prevenir accesos no autorizados y protege la integridad de los sistemas institucionales. Se elaboró ajuste final a la POLÍTICA DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN	Evidencia punto 3	
4. Realizar revisiones y análisis periódicos de la infraestructura tecnológica, identificando vulnerabilidades, realizando correctivos y asegurando la privacidad y seguridad de la información.	Durante el periodo evaluado se realizaron revisiones periódicas de la infraestructura tecnológica mediante herramientas de seguridad endpoint, permitiendo identificar el estado de vulnerabilidades de servidores y estaciones de trabajo. Como resultado, se efectuó seguimiento a los activos evaluados y se aplicaron medidas preventivas para reducir riesgos que puedan afectar la disponibilidad, integridad y privacidad de la información.	Evidencia punto 4	
5. Actualizar la matriz de activos de la información de todas las dependencias de la Administración Municipal, teniendo en cuenta las recomendaciones dadas por el Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC y la Gobernación de Risaralda.	Se entregó Matriz de Inventario y Clasificación de Activos de Información actualizando las dependencias de la Administración Municipal, alineada con las últimas tablas de retención documental, aprobadas y publicadas.	Evidencia punto 5	

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 6 de 8

OBJETIVOS O ALCANCES DEL CONTRATO	ACTIVIDAD DESARROLLADA	REGISTRO	OBSERVACIONES
6. Capacitar a funcionarios y contratistas en seguridad de la información, mediante charlas, manuales y comunicados internos, con el objetivo de promover buenas prácticas y sensibilización sobre la protección de datos y políticas de gobierno digital.	Se realizó versión final del PLAN DE GESTIÓN DE CULTURA ORGANIZACIONAL EN LA APROPIACIÓN DEL SGSI	Evidencia punto 6	
7. Actualizar, optimizar y realizar seguimiento a las políticas de respaldo de información y planes de contingencia, garantizando la ejecución automática y segura de copias de seguridad.	Se entrega versión final de la POLÍTICA DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN	Evidencia punto 7	
8. Elaborar diagnósticos bimestrales de la seguridad informática de la Alcaldía, presentando informes detallados sobre el estado de la seguridad, identificando riesgos, vulnerabilidades, eventos de seguridad y proponiendo un plan de acción para mitigar posibles amenazas, socializándolo con todo el equipo de la Subsecretaría de TIC.	Se realizó consolidación de evidencias del autodiagnóstico de seguridad y privacidad de la información, conforme a los lineamientos del MSPI, registrando los resultados en el Drive institucional dispuesto para el seguimiento de planes.	Evidencia punto 8	

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 7 de 8

OBJETIVOS O ALCANCES DEL CONTRATO	ACTIVIDAD DESARROLLADA	REGISTRO	OBSERVACIONES
9. Realizar las acciones del plan de acción y seguimiento de la matriz de riesgos informáticos, asegurando que esté alineada con las amenazas actuales, tanto internas como externas, y realizando mediciones periódicas para garantizar la precisión y efectividad en la gestión de riesgos. Sugiriendo actualización a la matriz según nuevos riesgos identificados o riesgos ya neutralizados por no representar ya amenaza.	Se realizó la labor correspondiente al reporte de las acciones ejecutadas en el CUARTO PERIODO, en los siguientes planes a cargo: - Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - Plan de Seguridad y Privacidad de la Información El registro y actualización de la información se diligenció en el Drive institucional dispuesto para este fin, en cumplimiento de los lineamientos establecidos.	Evidencia punto 9	
10. Realizar seguimiento al plan de acción para la implementación de la política Seguridad Digital, consolidando las respectivas evidencias de cumplimiento y ejecutando acciones enmarcadas en el objeto contractual. Recomendando acciones nuevas a incluir luego de elaborar el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información en los instrumentos dispuestos por el MINTIC para tal fin.	Se realizó consolidación de evidencias del autodiagnóstico de seguridad y privacidad de la información, conforme a los lineamientos del MSPI, registrando los resultados en el Drive institucional dispuesto para el seguimiento de planes.	Evidencia punto 10	
11. Asistir en reuniones y actividades de la Subsecretaría TIC, brindando soporte técnico y participando en propuestas de mejora e innovación tecnológica.	Se entrega versión ajustada del PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Evidencia punto 11	

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 8 de 8

El presente informe se entrega en cumplimiento a la carta de compromisos suscrita el día 26 de noviembre con la entrega total y definitiva de las evidencias correspondiente al acta final con fecha de corte al día 31 de diciembre de 2025.

Giovanny Henao Cárdenas

Contratista: Oscar Giovanny Henao Cárdenas

Fecha de entrega: 31 de diciembre de 2025

Vo. Bo

Martha Jeny Agudelo Romero

Supervisora: Martha Jeny Agudelo Romero