

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 1 de 20

1. INFORMACIÓN GENERAL DEL CONTRATO

Contratista	<i>Oscar Giovanni Henao Cárdenas</i>
Informe de Actividades N°.	<i>01</i>
Período	<i>10 de octubre al 09 de noviembre 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>\$ 3.700.000</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 20

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

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 3 de 20

3. DESARROLLO DEL CONTRATO

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.	Evidencia punto 1	
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 (5 de octubre de 2025 al 03 de noviembre de 2025)	Evidencia punto 2	

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 4 de 20

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 borrador de la Resolución “POR MEDIO DE LA CUAL SE ADOPTA LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LA ALCALDÍA DE SANTA ROSA DE CABAL”, actualmente en revisión técnica y jurídica para su posterior firma y publicación. Este documento contiene los lineamientos institucionales para asegurar la confidencialidad, integridad, disponibilidad y no repudio de la información, en cumplimiento de la normativa vigente sobre seguridad digital, protección de datos personales y el Modelo de Seguridad y Privacidad de la Información (MSPI).	Evidencia punto 3	

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 5 de 20

OBJETIVOS O ALCANCES DEL CONTRATO	ACTIVIDAD DESARROLLADA	REGISTRO	OBSERVACIONES
4. Realizar revisiones y análisis periódicos de la infraestructura tecnológica, identificando vulnerabilidades, realizando correctivos y asegurando la privacidad y seguridad de la información.	Se realizó el análisis y seguimiento oportuno de la detección de una URL maliciosa identificada por el antivirus WatchGuard como potencial amenaza de phishing. La revisión incluyó la verificación del enlace sospechoso, su clasificación como riesgo y la documentación correspondiente en el informe de "Seguimiento detecciones Antivirus Phishing". Con esto, se asegura la mitigación de vulnerabilidades y la protección de la información institucional. Se realizó el análisis e informe de una alerta recurrente del antivirus WatchGuard en el equipo sg-SSTcomparendos, identificándose como un falso positivo relacionado con el módulo legítimo Cisco Posture. Se validó que no existía riesgo real para la infraestructura, y se recomendó la exclusión del archivo en el antivirus para evitar nuevas alertas. Se realiza revisión y análisis del contenido de un correo para verificar su autenticidad y determinar si corresponde a un intento de suplantación o fraude electrónico, en el que se observa una posible tentativa de phishing, identificado por el asunto 'Fwd: Te han delegado una solicitud'. El mensaje presenta características sospechosas que sugieren un intento de obtener información de manera fraudulenta.	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 realizó segunda versión de la Matriz de Inventario y Clasificación de Activos de Información actualizando las dependencias de la Administración Municipal, consolidada en el archivo maestro con base en los lineamientos del MinTIC, disponible en el drive institucional.	Evidencia punto 5	

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 6 de 20

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 creó pieza gráfica para campañas de concientización de los funcionarios de la alcaldía de Santa Rosa de nombre: Protección para la conexión en Redes WiFi públicas. Se realizó difusión de pieza gráfica a través del carrusel del aplicativo SAIA de nombre: Protección para la conexión en Redes WiFi públicas. Se creó pieza gráfica para campañas de concientización de los funcionarios de la alcaldía de Santa Rosa a través de grupo de WhatsApp Institucional Se realizó comunicado SAIA tema: Tips de seguridad digital para proteger tu información: Zonas Wi-Fi Públicas, como campaña de concientización de los funcionarios de la alcaldía de Santa Rosa	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 actualizó documento borrador de la POLÍTICA DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN segunda versión	Evidencia punto 7	

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 7 de 20

OBJETIVOS O ALCANCES DEL CONTRATO	ACTIVIDAD DESARROLLADA	REGISTRO	OBSERVACIONES
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.	Esta actividad no se realizó en el presente informe, se realizará para el segundo informe dado que el informe es bimestral		
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 TERCER 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 fue diligenciado en el Drive institucional dispuesto para este fin, en cumplimiento de los lineamientos establecidos.	Evidencia punto 9	

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 8 de 20

OBJETIVOS O ALCANCES DEL CONTRATO	ACTIVIDAD DESARROLLADA	REGISTRO	OBSERVACIONES
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 el 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 realizó soporte técnico para instalación y configuración de nueva impresora en la Secretaría de Planeación	Evidencia punto 11	

Giovanny Henao Cárdenas

Contratista: Oscar Giovanny Henao Cárdenas

Fecha de entrega: 14 de noviembre de 2025

Vo. Bo

Martha Jeny Agudelo Romero
Supervisora: Martha Jeny Agudelo Romero



Fecha: 02/03/2022

Versión: 2.0

Página 9 de 20

EVIDENCIA 1

[illegible]



Fecha: 02/03/2022

Versión: 2.0

Página **10** de **20**

EVIDENCIA 2

Archivo Inicio Insertar Dibujar Disposición de página Fórmulas Datos Revisar Vista Automatizar Ayuda

Pegar Fuente Alineación Número Estilos Celdas Edición Confidencialidad Complementos Copilot

A1 Cliente

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Cliente	Tipo de equi	Equipo	Nombre ma	Tipo de ame	Tipo de malv	Número de c	Acción	Detectado p	Ruta de dete	Excluido	Fecha	Grupo	Dirección IP	Dominio	Descripción	
2	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		6 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
3	Alcaldia de	Estación	SC-SECJEFC	URLs con m	a URL con mal		8 Bloqueado	Protección V	https://gwbk	FALSO	#####	Todos\Bloq	10.18.5.21		starosa.local		
4	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		6 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
5	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		6 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
6	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		6 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
7	Alcaldia de	Portátil	DESKTOP-L72VBVM	URLs con m	a URL con mal		2 Bloqueado	Protección V	https://unde	FALSO	#####	Todos\Servic	10.18.0.36				
8	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		10 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
9	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		8 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
10	Alcaldia de	Estación	SP-PROFUNIVSITARIO	URLs con m	a URL con mal		2 Bloqueado	Protección V	https://eechi	FALSO	#####	Todos\Bloq	10.18.5.125		starosa.local		
11	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		2 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
12	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		6 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
13	Alcaldia de	Estación	SG-TECADMINSYCDH	URLs con m	a URL con mal		14 Bloqueado	Protección V	https://sour	FALSO	#####	Todos\Bloq	10.18.5.240		starosa.local		
14	Alcaldia de	Estación	SG-TECADMINSYCDH	URLs con m	a URL con mal		4 Bloqueado	Protección V	https://sour	FALSO	#####	Todos\Bloq	10.18.5.240		starosa.local		
15	Alcaldia de	Estación	SG-TECADMINSYCDH	URLs con m	a URL con mal		4 Bloqueado	Protección V	https://kettle	FALSO	#####	Todos\Bloq	10.18.5.240		starosa.local		
16	Alcaldia de	Estación	SG-TECADMINSYCDH	URLs con m	a URL con mal		4 Bloqueado	Protección V	https://kettle	FALSO	#####	Todos\Bloq	10.18.5.240		starosa.local		
17	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		6 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
18	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		6 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
19	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		6 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				
20	Alcaldia de	Estación	DESKTOP-BMFTA5P	URLs con m	a URL con mal		6 Bloqueado	Protección V	https://hol-	FALSO	#####	Todos\Servic	192.168.1.2				



Versión: 2.0

Página **11** de **20**

EVIDENCIA 3

[illegible]

EVIDENCIA 4

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Cliente	Tipo de equipo	Equipo	Nombre mal	Tipo de amenaza	Tipo de malware	Número de	Acción	Detectado por	Ruta de detección	Excluido	Fecha	Grupo	Dirección IP	Dominio	Descripción
2	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			3	Movido a Cui:Protección d C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
3	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			2	Movido a Cui:Protección d C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
4	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			1	Movido a Cui:Protección d C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
5	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			2	Movido a Cui:Protección d C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
6	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			1	Movido a Cui:Análisis baj C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
7	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			1	Movido a Cui:Protección d C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
8	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			1	Movido a Cui:Análisis baj C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
9	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			3	Movido a Cui:Protección d C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
10	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			1	Movido a Cui:Protección d C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
11	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			1	Movido a Cui:Análisis baj C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
12	Alcaldía de	Estación	sg-SSTcomp; Generic Mal Virus y ransc	Troyano			2	Movido a Cui:Protección d C:\Users\Equ			FALSO	#####	Todos\Bloqu	10.18.1.242		
13																
14																
15																
16																
17																



SECRETARÍA DE
TECNOLOGÍA DE
LA INFORMACIÓN Y
LA COMUNICACIÓN TIC

ALCALDÍA DE
SANTA ROSA DE CABAL

INFORME TÉCNICO PREVENTIVO DE SEGURIDAD DIGITAL

Entidad: Alcaldía de Santa Rosa de Cabal
Fecha del Informe: 03 de noviembre de 2025
Responsable del análisis: Ing. Giovanni Henao Cárdenas
Clasificación del evento: Alerta de falso positivo del antivirus

1. Descripción del evento

Durante las revisiones periódicas de seguridad digital, se detectaron múltiples alertas generadas automáticamente por el antivirus corporativo **WatchGuard** en la estación de trabajo identificada como **sg-SSTcomp**. Estas alertas señalaban la presencia de una posible amenaza catalogada como **"Generic Malware"** de tipo Troyano.

2. Análisis técnico

- Las detecciones ocurrían de forma repetitiva sobre el mismo archivo o proceso contenido dentro de la ruta:
C:\Users\Equipo\Pictures\CiscoPosture\
- Este directorio corresponde al software legítimo de verificación de cumplimiento de políticas de acceso de red de Cisco (**Cisco Posture**).
- El archivo detectado fue revisado y catalogado como **falso positivo**, basado en:
 - Registro automático marcado como "Falso" en **WatchGuard**.
 - No se encontraron comportamientos maliciosos ni alteraciones sistémicas.
 - Confirmación de que forma parte de un componente seguro del ecosistema Cisco.

3. Acciones realizadas

Acción	Responsable	Estado
Revisión técnica del archivo detectado	Responsable Seguridad Digital	Completado
Verificación de reputación del archivo y del proceso	Responsable Seguridad Digital	Completado
Markado como falso positivo en el antivirus	WatchGuard	Completado
Recomendación de exclusión en el antivirus	Área de TI	Pendiente según validación

4. Impacto en la operación

- Impacto a la disponibilidad del servicio:** Nulo
- Impacto en la integridad o confidencialidad de los datos:** Ninguno
- Interrupción de actividades:** No se registraron afectaciones

5. Recomendaciones de mejora

- Agregar exclusión del directorio **CiscoPosture**, en la configuración del antivirus para evitar nuevas alertas.
- Actualizar las firmas del antivirus corporativo.
- Registrar este evento en la bitácora de **alertas preventivas**.

6. Registro de evidencia

Se adjunta archivo CSV exportado desde el sistema **WatchGuard**, correspondiente a las detecciones realizadas entre el 21 y 29 de octubre de 2025.

Giovanny Henao Cárdenas

OSCAR GIOVANNY HENAO CARDENAS
Ing. de Sistemas
Especialista en Seguridad **Informática**

Alcaldía Municipal de Santa Rosa de Cabal
Carrera 14, Calle 12 Esquina C.A.M
Bello, PSE 300-3000
Código postal 900229

www.santarosadecabal-riacabala.gov.co

Alcaldía Municipal de Santa Rosa de Cabal
Carrera 14, Calle 12 Esquina C.A.M
Bello, PSE 300-3000
Código postal 900229

www.santarosadecabal-riacabala.gov.co

Alcaldía Municipal de Santa Rosa de Cabal
Carrera 14, Calle 12 Esquina C.A.M
Bello, PSE 300-3000
Código postal 900229

www.santarosadecabal-riacabala.gov.co

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 13 de 20


<https://camiloromero.com.co/>




 8/98 security vendors flagged this URL as malicious

[Reanalyze](#)
[Search](#)
[More](#)

<https://camiloromero.com.co/>
camiloromero.com.co

Status	Content type	Last Analysis Date
200	text/html; charset=utf-8	19 days ago

[text/html](#)
[trackers](#)
[iframes](#)
[external-resources](#)

[DETECTION](#)
[DETAILS](#)
[COMMUNITY](#)

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	 Phishing
BitDefender	 Phishing
CRDF	 Malicious
Forcepoint ThreatSeeker	 Phishing
Fortinet	 Phishing
G-Data	 Phishing
Lionic	 Phishing
Sophos	 Phishing
Abusix	 Clean
Acronis	 Clean
ADMINUSLabs	 Clean
ALLabs (MONITORAPP)	 Clean
AlienVault	 Clean
Antiy-AVL	 Clean
Artists Against 419	 Clean
benkow.cc	 Clean
BlockList	 Clean
Blueliv	 Clean
Certego	 Clean
Chong Lua Dao	 Clean
CINS Army	 Clean

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 14 de 20



Gio Henao <giovannyh@gmail.com>

Fwd: Te han delegado una solicitud

Gio Henao <giovannyh@gmail.com>

6 de noviembre de 2025, 19:52

Para: Gobierno Digital Santa Rosa de Cabal <gobiernoentinea@santarosadecabal-risaralda.gov.co>, Subsecretaría TIC <tic@santarosadecabal-risaralda.gov.co>, Sistemas Alcaldía Santa Rosa Santa Rosa de Cabal <sistemas@santarosadecabal-risaralda.gov.co>

Cordial saludo

De acuerdo a su solicitud se realizó análisis del sitio Web solicitado, encontrando lo siguiente:

<http://www.santarosa-cauca.gov.co/pqrs/ebd2b96e0e8196bf2289db16bd1e165e607bc090>

ANÁLISIS:

Aunque el dominio base aparentemente pertenece a una entidad pública, se identifican las siguientes posibles amenazas:

- El enlace hace referencia a otra entidad denominada "Santa Rosa – Cauca", que no corresponde a nuestra jurisdicción ni sistemas institucionales.
- Uso de HTTP no seguro: el enlace utiliza protocolo no cifrado, lo cual podría facilitar ataques de phishing, robo de información o redireccionamientos maliciosos.
- Contenido relacionado con números de solicitud inespecíficos ("81645493702"): forma parte de la ingeniería social utilizada para generar confianza y provocar la apertura del enlace.
- Esquema coincidente con amenazas tipo phishing: el mensaje que acompaña el enlace busca que se haga clic para "ver una solicitud", generando posible riesgo de robo de datos o instalación de malware.

Por lo anterior, se recomienda:

No deben acceder al enlace desde ningún dispositivo institucional.

Conclusión operativa

Toda plataforma de PQRS institucional, así como cualquier envío de enlaces a ciudadanos para seguimiento de trámites, debe obligatoriamente operar sobre **HTTPS** con certificado válido. De lo contrario, la integridad, confidencialidad y autenticidad de la información están en riesgo.

Por tanto, este enlace debe ser tratado como **potencialmente inseguro, incluso si pertenece a un dominio gubernamental válido**, y no debe utilizarse para ingresar datos ni descargar archivos hasta que se verifique formalmente su finalidad y se garantice su seguridad.

Saludos

GIOVANNY HENAO CARDENAS
Ingeniero de Sistemas

[El texto citado está oculto]

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022 Versión: 2.0 Página 15 de 20
--	---------------------------------	---

EVIDENCIA 5

4	MATRIZ DE IN												
5													
6													
7													
8	IDENTIFICACIÓN DEL ACTIVO DE INFORMACIÓN (LEY 594 DE 2000 - LEY 1712 DE 2014- DECRETO 103 DE 2015 - DECRETO 1080 DE 2015 - ISO 27001)												
9	Manejadores	Procesos	Código sistema de gestión documental	Identificador	Tipo	Oficina	Sede documental	Subsede documental	Nombre	Descripción	Nombre del responsable de la producción de la información (Propietario activo)	Fecha de actualización de la información	Nombre de la información (Codi
10	APOYO	Gestión de la información		1	Dispositivos de Tecnologías de Infor				Servidor Aplicación ARIES	soporte a usuarios	TIC		
11	APOYO	Gestión de la información		2	Servicios				Publicaciones en sitio WEB	del sitio Web de la entidad	TIC		
12	APOYO	Gestión de la información		3	Sistemas de Información y Aplicacion				Sistema unico de informacion de Tramites SUIT	integrados de las Hojas de vida de tramites y servicios de la entidad.	TIC		
13	APOYO	Gestión de la información		4	Sistemas de Información y Aplicacion				Administración Licenciamiento Microsoft Office	Asignación de licencias a usuarios de la administración Municipal.	TIC		Alexande
14	APOYO	Gestión de la información		5	Información y datos de la Entidad				Matriz de Riesgos	peligros o amenazas que podrían afectar el cumplimiento de los	TIC		Giovanny
15	APOYO	Gestión de la información		6	Información y datos de la Entidad				Plan de Mejoramiento	mejoramiento perteneciente a la oficina TIC	TIC		
16	APOYO	Gestión de la información		7	Información y datos de la Entidad				Encuestas de Satisfacción	análisis de la calificación por cada una de las preguntas.	TIC		
17	APOYO	Adquisición y gestión de recursos físicos y tecnológicos		8	Dispositivos de Tecnologías de Infor				Switch	la red Local	TIC		Alexande
18	APOYO	Adquisición y gestión de recursos físicos y tecnológicos		9	Dispositivos de Tecnologías de Infor				Access Point	Dispositivo electrónico para establecer conexiones inalámbricas	TIC		Alexande
19	APOYO	Adquisición y gestión de recursos físicos y tecnológicos		10	Dispositivos de Tecnologías de Infor				Firewall	permitiendo solo las comunicaciones seguras y autorizadas.	TIC		Alexande
20	APOYO	Adquisición y gestión de recursos físicos y tecnológicos		11	Dispositivos de Tecnologías de Infor				Equipos críticos de Financiera	Procesamiento de datos financieros	TIC		Alexande
21	APOYO	Adquisición y gestión de recursos físicos y tecnológicos		12	Dispositivos de Tecnologías de Infor				Equipos para navegación y Ofimaticos	únicamente a navegación web y aplicaciones de productividad de oficina	TIC		Alexande
22	APOYO	Gestión de la información		13	Sistemas de Información y Aplicacion				Sistemas Operativos para servidores	como el hardware y los servicios, para que puedan ser utilizados por	TIC		Alexande
23	APOYO	Gestión de la información		14	Sistemas de Información y Aplicacion				Sistemas Operativos para equipos no críticos (funcio	una computadora y los usuarios, facilitando la ejecución de programas y	TIC		Alexande
24	APOYO	Adquisición y gestión de recursos físicos y tecnológicos		15	Servicios				Impresoras área de nomina, área financiera	impresiones de nómina y pagos contratista y proveedores	TIC		Alexande
25	APOYO	Adquisición y gestión de recursos físicos y tecnológicos		16	Servicios				Impresoras funcionarios y contratistas	funcionarios y contratista de la entidad	TIC		Alexande
26	APOYO	Adquisición y gestión de recursos físicos y tecnológicos		17	Servicios				Scanner de Nomina y financiera y archivo	documentos con información sensible (contratos, datos personales,	TIC		Alexande
27	APOYO	Adquisición y gestión de recursos físicos y tecnológicos		18	Servicios				Scanner funcionarios y contratistas	imágenes físicas en archivos digitales	TIC		Alexande
28	APOYO	Adquisición y gestión de recursos físicos y tecnológicos		19	Soporte para Almacenamiento de Info				Cuarto de telecomunicaciones	cuanto a servidores, comunicaciones y componentes de redes	TIC		Alexande
< > Inventario Activos													

EVIDENCIA 6

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 16 de 20

https://municipio-santa-rosa.net/saa.com
SAA - SODEA



¿Sabías que conectarte a un Wi-Fi pública puede poner en riesgo tu información personal?

Cuando usas estas redes, tus contraseñas, fotos y mensajes pueden ser vistos o robados por personas malintencionadas.

Para protegerte, evita conectarte a redes abiertas y, si necesitas internet, usa los datos de tu celular o pregunta por una red privada y segura.

Si no te queda más remedio y tienes que conectarte...

- Verifica el nombre de la red con el establecimiento.
- Evita transacciones sensibles (banco, compras).



INICIO DE SESIÓN

USUARIO
oscar.henao

CONTRASEÑA

[Iniciar](#)

Necesita ayuda para ingresar



SI NO ESTÁS CONECTADO A LA RED WI-FI DE TU HOGAR O DEL TRABAJO, OJO CON LAS REDES WI-FI GRATIS EN SITIOS PÚBLICOS.

© 2022 SODEA. Todos los derechos reservados.



¿Sabías que conectarte a un Wi-Fi pública puede poner en riesgo tu información personal?

Cuando usas estas redes, tus contraseñas, fotos y mensajes pueden ser vistos o robados por personas malintencionadas.

Para protegerte, evita conectarte a redes abiertas y, si necesitas internet, usa los datos de tu celular o pregunta por una red privada y segura.

Si no te queda más remedio y tienes que conectarte...

- Verifica el nombre de la red con el establecimiento.
- Evita transacciones sensibles (banco, compras).



SI NO ESTÁS CONECTADO A LA RED WI-FI DE TU HOGAR O DEL TRABAJO, OJO CON LAS REDES WI-FI GRATIS EN SITIOS PÚBLICOS.



INFORME DE ACTIVIDADES

Fecha: 02/03/2022

Versión: 2.0

Página **17** de **20**

**SI NO ESTÁS CONECTADO
A LA RED WI-FI DE TU
HOGAR O DEL TRABAJO,
OJO CON LAS REDES
WI-FI GRATIS
EN SITIOS PÚBLICOS.**

**Riesgos a los que te
expones**

La información que transmitas por la red
puede ser capturada y usada en tu contra

¿Por qué?

- 1 No sabes quién esta
conectado a la red ni
sus intenciones.
- 2 Desconoces cuáles son
las configuraciones y el nivel
de seguridad de la conexión.

**Si no te queda más remedio
y tienes que conectarte...**

- ✓ Verifica el nombre de la red
con el establecimiento.
- ✗ Evita transacciones
sensibles (banco, compras).
- ✗ Desactiva compartir
archivos y olvida la red
al salir

**RED
FALSA**

EVIDENCIA 7

 ADMINISTRACIÓN MUNICIPAL SANTA ROSA DE CABAL SECRETARÍA DE PLANEACIÓN SUBSECRETARÍA DE TIC POLÍTICA DE RESPALDO, CUSTODIA Y RECUPERACIÓN DE LA INFORMACIÓN 1. INTRODUCCIÓN Esta política tiene como propósito garantizar la disponibilidad, integridad y recuperación de la información crítica institucional de la Alcaldía de Santa Rosa de Cabal, mediante la implementación de procedimientos de respaldo, custodia y restauración alineados con las mejores prácticas y la normativa vigente. 2. MARCO NORMATIVO - Ley 1581 de 2012 - Protección de datos personales. - Ley 1273 de 2009 - Delitos informáticos. - Decreto 1008 de 2018 - Gobierno Digital. - Modelo de Seguridad y Privacidad de la Información – MSPi (MinTIC). - Estándares internacionales ISO/IEC 27001 y 27002. - Archivo General de la Nación – Acuerdo 060 de 2001. 3. GLOSARIO - Backup: copia de seguridad que permite recuperar datos ante pérdida o corrupción. - Custodia: almacenamiento y resguardo seguro de los medios de respaldo. - RTO/RPO: tiempos máximos aceptables para restaurar servicios y datos. - Off-site: almacenamiento externo o remoto de respaldos. - Restauración: proceso de recuperación de información desde un respaldo. 4. OBJETIVOS 4.1 OBJETIVO GENERAL: Asegurar que la información institucional pueda ser recuperada de forma oportuna ante incidentes que afecten la operación normal.	 ADMINISTRACIÓN MUNICIPAL SANTA ROSA DE CABAL SECRETARÍA DE PLANEACIÓN SUBSECRETARÍA DE TIC 4.2 ALCANCE: Esta política aplica a todos los activos de información digitales, sistemas, servidores, bases de datos y servicios en la nube utilizados por la entidad. 5. ORGANIZACIÓN - Subsecretaría TIC: diseño y ejecución de la política. - Coordinación de Infraestructura y Soporte: administración de respaldos. - Responsables de proceso: validación y definición de activos críticos. - Comité Institucional: aprobación y seguimiento de cumplimiento. La Subsecretaría identificará a los responsables de realizar los backups y de definir el procedimiento para hacer las copias de seguridad y restaurarlas que incluirán como mínimo: • De qué hacer copia, • El tipo de copia, • La plataforma tecnológica necesaria • Los soportes, • La periodicidad, • La vigencia, • Su ubicación, • Pruebas de restauración. Así mismo se llevará un control de los soportes utilizados, se vigilará que sólo tiene acceso personal autorizado y que se destruyen los soportes de forma segura, en caso de tener que desecharlos. Los mismos criterios de seguridad serán aplicables en caso de hacer copias en la nube o en proveedores externos. 6. VIGENCIA, RESPONSABILIDADES Y ACTUALIZACIÓN DE LA POLÍTICA	 ADMINISTRACIÓN MUNICIPAL SANTA ROSA DE CABAL SECRETARÍA DE PLANEACIÓN SUBSECRETARÍA DE TIC 6.1 Responsabilidades La Subsecretaría de Tecnologías de la Información y las Comunicaciones (TIC) de la Alcaldía de Santa Rosa de Cabal será la dependencia responsable de liderar la implementación, mantenimiento, actualización y supervisión de la presente Política de Respaldo, Custodia y Recuperación de la Información. Esta dependencia será también la encargada de brindar soporte técnico y estratégico en materia TIC a todas las áreas de la entidad, con el fin de garantizar la disponibilidad, integridad y continuidad de los servicios de información. 6.2 Gestión de excepciones a la política Cualquier excepción o desvío a lo establecido en la presente Política de Respaldo, Custodia y Recuperación de la Información deberá ser solicitada de manera formal y justificada por el área o dependencia interesada. La solicitud deberá especificar: • El motivo de la excepción. • Su alcance y duración estimada. • Los posibles impactos asociados. • Los controles compensatorios o medidas alternativas que mitigarán el riesgo. La evaluación y aprobación de excepciones será responsabilidad del Comité Institucional de Gestión y Desempeño, con el apoyo técnico de la Subsecretaría TIC. Toda excepción aprobada deberá registrarse en el "Registro de Excepciones del SGSPi" y será revisada periódicamente o cuando se modifiquen las condiciones que originaron dicha excepción. En caso de no ser aprobada la solicitud, la dependencia solicitante deberá ajustarse a lo dispuesto en la presente política sin modificación alguna. 6.3 Cumplimiento El cumplimiento de esta política es obligatorio. Su incumplimiento será considerado un incidente de seguridad de la información y podrá dar lugar a acciones disciplinarias conforme al régimen aplicable a los servidores públicos, o a la terminación del vínculo contractual con terceros, sin perjuicio de las acciones legales o administrativas a que haya lugar.
---	--	---

Página 18 de 21 2031 palabras Español (España) Predicciones de texto: activado

Concentración 50%

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 19 de 20

EVIDENCIA 9



ALCALDÍA DE
SANTA ROSA
DE CABAL

SUBSECRETARÍA DE TECNOLOGÍAS DE LA
INFORMACIÓN Y LA COMUNICACIÓN

24 de octubre de 2025

DE: Oscar Giovanni Henao Cardenas - CONTRATISTA - SUBSECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

PARA: Johan Sebastian Villalba Hernandez - SUBSECRETARIO (A) - SUBSECRETARIA DE PLANIFICACIÓN SOCIOECONÓMICA



No. 20251024-3919-I

ASUNTO: RESPUESTA: DILIGENCIAMIENTO SEGUIMIENTO PLANES DECRETO 612 DE 2018

Cordial saludo:

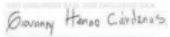
En atención a su solicitud, me permito informar que se realizó la labor correspondiente al reporte de las acciones ejecutadas en el TERCER PERIODO, en los siguientes planes a cargo:

- Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI)
- 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 fue diligenciado en el Drive institucional dispuesto para este fin, en cumplimiento de los lineamientos establecidos.

Quedo atento a cualquier observación o información adicional que se requiera.

Cordialmente



Oscar Giovanni Henao Cardenas
CONTRATISTA

Proyectó: Oscar Giovanni Henao Cardenas - CONTRATISTA - SUBSECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Copia: MARÍA ZOBEIDA TOBON CASTAÑO - PROFESIONAL UNIVERSITARIO - SUBSECRETARÍA DE TECNOLOGÍAS

	INFORME DE ACTIVIDADES	Fecha: 02/03/2022
		Versión: 2.0
		Página 20 de 20

EVIDENCIA 10

