
	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 1 de 24

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ALCALDÍA DE SAN AGUSTÍN HUILA.

**HEBER NEL MUÑOZ YASNO
ALCALDE 2024 – 2027**

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 2 de 24

1 INFORME INDIVIDUAL DE LA ORGANIZACIÓN

1.1 ORGANIZACIÓN

ALCALDÍA MUNICIPAL DE SAN AGUSTÍN


1.2 ACTIVIDAD ECONÓMICA

ACTIVIDADES EJECUTIVAS DE LA ADMINISTRACIÓN PÚBLICA

1.3 RESEÑA ALCALDÍA

La misión de la Administración Municipal de San Agustín patrimonio histórico y cultural de la humanidad, con un ecosistema único de gran importancia para el país, es una entidad territorial que garantiza, organiza y controla la provisión de bienes y servicios de calidad a sus habitantes, preservando su medio ambiente y transformando social y productivamente nuestro entorno, con un talento humano responsable y capaz de orientar los procesos de desarrollo sostenible fundamentado en la planeación colectiva, ejerciendo prácticas de buen gobierno democrático apoyado en la gestión a nivel departamental, nacional y de cooperación internacional, enfocada a la transformación social y productiva con compromiso social para alcanzar los objetivos del desarrollo del milenio.

San Agustín es un municipio ubicada al sur del departamento del Huila. Referenciado a una altura de 1.730 metros sobre el nivel del mar en las estribaciones del Macizo Colombiano con un clima de 20 °C el cual es propicio para el turismo arqueológico y ecológico, ciclo-turismo, cabalgatas, deportes extremos, entre otros, se cuenta con una población de aproximadamente 34.152 habitantes, además de atractivos turísticos como lo son el parque Arqueológico que es uno de los más importantes espacios arqueológicos de Colombia y fue declarado Patrimonio de la humanidad por la Unesco en 1995, tenemos a unos cuanto kilómetros a la laguna de la Magdalena que da nacimiento al río de nombre Magdalena el cual es considerado uno de los más importantes de Colombia.

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 3 de 24

1.4 ORGANIGRAMA

Figura 1. Organigrama [DECRETO 165 DEL 30 DE DICIEMBRE DE 2019](#)



Fuente: <http://www.sanagustin-huila.gov.co/alcaldia/organigrama>


Decreto No. 159 del 30 de diciembre de 2019 "POR MEDIO DEL CUAL SE ADOPTA EL MANUAL ESPECÍFICO DE FUNCIONES Y COMPETENCIAS LABORALES DE LA ALCALDÍA MUNICIPAL DEL MUNICIPIO DE SAN AGUSTÍN

1.5 ESTRUCTURA ORGANIZACIONAL OFICINA DE SERVICIOS ADMINISTRATIVOS ENCARGADA DE TI


La Oficina de Servicios Administrativos de la Alcaldía de San Agustín, se encuentra integrada por un (1) funcionario de Planta, el cual desarrolla actividades de tecnología con el apoyo de un (1) contratista. Este grupo de servidores se encuentra dirigido por la Secretaria de Gobierno y Servicios Administrativos, la cual establece las funciones a desarrollar por cada uno de los integrantes.

1.5.1 Funciones del área de Servicios Administrativos

San Agustín, Huila Colombia
 Calle 3 Carrera 12 Esquina Teléfono 8373177 <http://www.sanagustin-huila.gov.co>
 NIT: 891180056-6 Código Postal: 41668000

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 4 de 24

1. Ejecutar todas las funciones propias del Almacenista del municipio tales como: responder por la organización y adecuado funcionamiento; atender los pedidos de equipos, elementos, materiales, formas impresas y papelería; mantener información actualizada sobre el estado de las solicitudes de elementos formuladas por las diferentes dependencias de la Administración Municipal.
2. Expedir los Certificados de Paz y Salvo, requeridos por los funcionarios con todos los requisitos necesarios.
3. Actualizar permanentemente el registro de proveedores y las estadísticas de precios, materiales, elementos y equipos necesarios para la Administración Municipal.
4. Responder por el cargue de la información contractual en el SECOP.
5. Coordinar las políticas de archivo para, indexarlo, expurgar para garantizar el archivo general del municipio.
6. Administrar en archivo central del Municipio de acuerdo a la Ley 594 de 2000.
7. Administrar todos los componentes de las Tecnologías y las comunicaciones para garantizar el correcto funcionamiento del hardware y software, así como su interacción con las políticas de gobierno en línea y facilitándole a la ciudadanía el acceso a la información pública.
8. Coordinar los diferentes comités municipales que se encuentran o están relacionados con el área de su desempeño.
9. Cumplir las demás funciones correspondientes de acuerdo con el nivel, la naturaleza y el área de desempeño.

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 5 de 24

1.6 DESCRIPCIÓN DE LOS RECURSOS INFORMÁTICOS DE LA ALCALDÍA DE SAN AGUSTÍN.

1.6.1 Activos Informáticos

- **Equipos Tecnológicos de Oficina: 151**
 - Tipo escritorio: **31** equipos.
 - Tipo todo en uno: **9** equipos.
 - Tipo portátil: **46** equipos.
 - Tipo impresora **39** equipos.
 - Tipo escáner **15** equipos.
 - Tipo Tableta **11** equipos.

Servidor: 1


Servidor HP ProLiant DL380p Gen8 (Rack 2U), Procesadores 2x Intel Xeon E5-2660v2 2.20GHz Up to 3.00GHz Turbo HT 20-Cores 40-Threads, Memorias RAM 64GB DDR3 RDIMM ECC (ampliable), Discos duros 3x 4TB 7.2K 6Gb/s 3.5" LFF RAID-5 (Max. 12 discos), Controladora RAID 1/0/5/10, Puertos de red 4x GbE, Fuentes de poder 2x 750w (redundante), iLO 4 Standard, Windows Server 2019 Standard 64-bit 16-Core OEM DVD COA English Edition (No CALs)

1.6.2 Procesos que se Realizan Dentro de la oficina de Servicios Administrativos sobre TI

Proyectos TIC: Gestionar los proyectos de innovación tecnológica TIC de la Alcaldía Municipal, mediante la identificación de iniciativas de innovación, elaboración y diseño de los estudios, aprobación y seguimiento de los mismos.

Implementación de la Estrategia Gobierno Digital: Implementar y adoptar la Estrategia de Gobierno Digital establecida por el Ministerio TIC, mediante la formulación del Plan de Acción e informes de avance de la Estrategia.

Administración de la Infraestructura Tecnológica y Sistemas de Información: Administrar, operar y garantizar el funcionamiento de la infraestructura Tecnológica y Sistemas de Información con que cuenta la Alcaldía de San Agustín.

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 6 de 24

Racionalización de Trámites: Racionalizar los trámites y procedimientos administrativos del Municipio.

Publicación en la página web: Dar cumplimiento a la Ley 1712 de 2014 realizando la publicación de la información generada por las dependencias de la Alcaldía de San Agustín, en el portal institucional <http://www.sanagustin-huila.gov.co/>.

2 INFORME INDIVIDUAL DE VULNERABILIDADES, AMENAZAS Y RIESGOS DE SEGURIDAD INFORMÁTICA.

2.1 VALORACIÓN DE ACTIVOS


Valoración de los activos de información, de acuerdo al inventario identificado, teniendo en cuenta los criterios de valoración aplicados a cada uno de los activos y a las dimensiones de seguridad de los mismos.

Tabla 1. Criterios de Valoración

CÓDIGO	VALOR	CRITERIO
10		DAÑO EXTREMADAMENTE GRAVE
09		DAÑO MUY GRAVE
6-8		DAÑO GRAVE
3-5		DAÑO IMPORTANTE
1-2		DAÑO MENOR
0	PRECIABLE	IRRELEVANTE A EFECTOS PRÁCTICOS

Tabla 2. Dimensiones de Seguridad de Activos

DIMENSIONES DE SEGURIDAD	
C	CONTABILIDAD
I	INTEGRIDAD
A	AUTENTICIDAD
D	DISPONIBILIDAD
T	TRAZABILIDAD

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 7 de 24

2.2 IDENTIFICACIÓN DE VULNERABILIDADES

2.2.1 Software y/o Aplicaciones del Municipio de San Agustín

En busca de agilizar y tener una mejor respuesta a la hora de realizar actualizaciones, verificaciones, recaudo, temas de almacén, entre otras, la Secretaría de Hacienda realiza la implementación del sistemas denominado HAS, que permita centralizar el análisis y procesamiento de la información de tipo financiero y tributario de los ciudadanos referente a impuestos, recaudo, entre otros.


Para el portal web institucional de la Alcaldía de San Agustín, fue otorgada por el Ministerio de las Tecnologías y la Información TI cumpliendo con un alto estándar de normatividad en cuanto a seguridad y acceso a la información se trata esta dada como portal territorial mediante el link: <http://www.sanagustin-huila.gov.co/>.

En el caso de las licencias de sistemas operativos, existe una cantidad importante de equipos de cómputo en la Administración Municipal, que utilizan sistemas operativos sin soporte técnico, lo cual permite que se vean expuestos a malware y otras debilidades de seguridad, debido a la falta de actualizaciones y parches de seguridad disponibles para su protección.

2.2.2 Hardware del Municipio de San Agustín

El servidor que se encuentra en la Alcaldía fue adquirido hace poco y se encuentra en buen estado, sin embargo se encuentra ubicado en una área de la Administración Municipal, donde las condiciones no son óptimas y presenta a futuro un alto riesgo para su funcionamiento, (aire acondicionado, aislamiento, acceso restringido, etc.), lo que no permite una administración y gestión eficiente sobre los servicios y aplicativos que éstos albergan, por parte de personal calificado y designado para tal fin.

De igual forma se encuentran muchos equipos de cómputo que funcionan con memorias RAM DDR1, discos duros con interfaz IDE de baja capacidad, procesadores de baja velocidad, entre otros aspectos, que dificultad las labores

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 8 de 24

de soporte técnico debido a la inexistencia de repuestos en el mercado.

En materia de equipos de red, se encuentran switches sin opción de administración, y cableado estructurado instalado en diferentes tipos de categoría, desde la categoría 5E hasta la categoría 6E, lo que no permite transmisión eficiente de datos a través de la red LAN. Afectando el direccionamiento, los servicios de red y el acceso a los diferentes aplicativos disponibles.

Además, la no existencia de un stock de repuestos, afecta la vida útil de algunos activos de información, como lo son equipos de cómputo, redes de comunicaciones, servicio de internet, equipos auxiliares como UPS, estabilizadores, etc., y no permite que se realicen planes de mantenimiento correctivo eficientemente.

Equipos Auxiliares de la alcaldía de San Agustín

Con relación a los equipos auxiliares, como las UPS y estabilizadores, aún existen dependencias en donde se requiere respaldo eléctrico por la naturaleza de sus funciones, como lo son gran parte de la Administración Municipal, que por estar ubicadas con un canal de energía diferente sufre alteraciones de energía.

En el edificio municipal, no se cuenta con una planta eléctrica que supla las necesidades cuando existen cortes de energía, los cuales generan múltiples problemas a los diferentes equipos de tecnología así como pérdida de información

2.2.3 Personal de la alcaldía de San Agustín


Con respecto al personal encargado de la administración de sistemas de información y la infraestructura tecnológica, existen inconvenientes debido a la corta planta de personal disponible en la Oficina TIC, ya que solo se cuenta con los siguientes funcionarios:

- Líder de Programa TIC: funcionario encargado, de la coordinación de proyectos TIC externos y de la estructuración de proyectos y requerimientos tecnológicos a nivel interno en la Administración

San Agustín, Huila Colombia

Calle 3 Carrera 12 Esquina Teléfono 8373177 <http://www.sanagustin-huila.gov.co>

NIT: 891180056-6 Código Postal: 41668000

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 9 de 24

Municipal.

Además del dato anterior, se cuenta con personal de prestación de servicios para apoyar la ejecución de programas, proyectos y normatividad establecidos a nivel nacional, y que son de obligatorio cumplimiento por parte de los entes territoriales, como lo son Gobierno Digital, Vive Digital para la gente, Ley de Transparencia, entre otros.


Adicionalmente y contratado por prestación de servicios que apoyan labores de soporte a servidor y aplicativos con información requerida para el cumplimiento de funciones misionales en la Administración, pero que no poseen en algunos casos los suficientes conocimientos técnicos respecto a las medidas que se deben tener en cuenta para salvaguardar los activos de información a cargo.

Como es notorio, la carga laboral asignada, es un factor importante al momento de enfrentar las funciones requeridas para la administración y gestión de la infraestructura tecnológica, y en caso de alguna emergencia, el personal existente resulta ser insuficiente para aplicar procedimientos establecidos, y/o no posee las suficientes herramientas o conocimientos técnicos necesarios para afrontar un evento de seguridad de la información.

2.2.4 Datos e Información de Procesos Internos

El manejo de la información y datos de la Administración Municipal presenta múltiples situaciones, dependiendo del tipo de información a tratar. En el caso de información generada y manejada por funcionarios que se dedican a procesos misionales, se presenta desconocimiento de procedimientos mínimos de protección y seguridad de la información, como el resguardo de la misma en dispositivos de respaldo, asignación y uso de contraseñas robustas de usuario en equipos de cómputo, aplicativos y demás servicios de red habilitados.

Referente a los backups o copias de respaldo de información, ésta es una práctica poco utilizada por los funcionarios para garantizar la disponibilidad de su información en caso de alguna eventualidad, como sucede en muchas ocasiones en las que los equipos de cómputo, estaciones de trabajo y/o instalaciones eléctricas presentan daños o alteraciones en sus condiciones normales. Estas situaciones afectan en algunas ocasiones los discos duros y/o repositorios conectados, por lo cual realizar recuperación de información,

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 10 de 24

cuando está comprometida la integridad de los mismos, es una labor casi imposible.

Situación similar se presenta en la gestión de contraseñas por parte de los funcionarios, ya que se manejan normalmente las mismas contraseñas asignadas por defecto, no tienen la complejidad necesaria, y/o no son modificadas periódicamente, a pesar de las recomendaciones emitidas, para evitar por ejemplo, ingeniería social para acceder a la información que protegen.


En los procesos de contratación relacionados con software y/o aplicativos se presenta una situación supremamente delicada, ya que no se está teniendo en cuenta la entrega a la Administración Municipal de la propiedad y los derechos de autor de los software, aplicativos y/o desarrollos contratados, en las obligaciones de los proveedores, lo cual genera que cualquier parametrización, modificación y/o actualización que se requiera sobre los mismos, genere una asignación presupuestal para tal fin, teniendo en cuenta que éstas no se pueden realizar sin autorización expresa del proveedor.

2.2.5 Soportes de Información

Entre los diferentes soportes de información que se encuentran en la Administración Municipal, los que más vulnerabilidad presentan son los materiales impresos, ya que en algunos casos, no se resguardan documentos e información sensible bajo llave y/o con las medidas que garanticen confidencialidad e integridad suficientes.

De igual forma, tampoco existen suficientes instalaciones para su correcta disposición y archivo, como lo estipula la Ley General de Archivo, ni existen repositorios de información disponibles para albergarlos digitalmente, lo cual genera un riesgo latente para la Administración Municipal.

En cuanto al manejo de dispositivos como CD, DVD, Discos Duros Externos y memorias flash (USB), para el almacenamiento de información sensible para el desarrollo de las actividades misionales de la Administración, requiere sensibilización a los funcionarios para la debida gestión y almacenamiento de los mismos como soporte y/o respaldo de información, ya que no existen procedimientos establecidos y aprobados por la alta dirección, y en la mayoría

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 11 de 24

de los casos, los funcionarios deben disponer de dispositivos personales para uso en actividades de la entidad.


2.2.6 Infraestructura Física de las Instalaciones de la Administración Municipal

Respecto a la infraestructura física, se presentan importantes deficiencias en la disposición de equipos y cableado estructurado, como se relaciona a continuación:

- Servidores: Mala disposición de servidor, ya que no existe suficiente espacio en el lugar donde se encuentra actualmente, ni existe uno adicional que lo albergue.
- No se cuenta con un Rack de comunicaciones, así como tampoco se cuenta con control de acceso a éste, por lo que cualquier persona que ingrese a esta área puede acceder a él.
- Cableado estructurado: el tablero eléctrico principal de la Oficina TIC permanece desprotegido, expuesto múltiples amenazas, ya sea por manipulación indebida, desastres naturales o incidentes que se puedan presentar accidentalmente. En las demás oficinas existen extensiones eléctricas y multitomas para habilitar puestos de trabajo, exponiendo los equipos a eventuales accidentes. Existen también conexiones de equipos de alta potencia a redes de energía regulada. De igual forma, se ubican switches y routers en diferentes oficinas del Edificio Municipal, sin la debida disposición del cableado, como lo indican las diferentes normas técnicas de cableado estructurado. Adicionalmente se presenta instalación de equipos de comunicación y de redes sin la debida autorización por parte de la Oficina TIC.

2.3 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

Una vez identificados y valorados los activos, se procede a la identificación de amenazas para cada uno de éstos, así como a la degradación y el impacto de éstas sobre los activos de acuerdo a su valoración.

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 12 de 24

También se realiza deducción de la probabilidad o frecuencia con las que se presentan las amenazas y/o vulnerabilidades identificadas en la entidad.

Tabla 11. Escala de Frecuencia de Amenazas

<u>VALOR</u>	<u>RANGO</u>	<u>PROBABILIDAD</u>
<u>5</u>	<u>1 VEZ CADA SEMANA</u>	<u>ALTA</u>
<u>4</u>	<u>1 VEZ CADA MES</u>	<u>MEDIA</u>
<u>3</u>	<u>1 VEZ CADA 6 MESES</u>	<u>BAJA</u>
<u>2</u>	<u>1 VEZ AL AÑO</u>	<u>MUY BAJA</u>
<u>1</u>	<u>1 VEZ CADA 2 AÑOS</u>	<u>RARO</u>

Tabla 12. Rango Porcentual de Impactos en Activos para Dimensiones de Seguridad


IMPACTO	VALOR CUALITATIVO
MUY ALTO	100%
ALTO	75%
MEDIO	50%
BAJO	20%
MUY BAJO	5%

Tabla 13. Rango de Impactos en Activos

IMPACTO	VALOR CUALITATIVO
DESASTROSO	8
MAYOR	5
MODERADO	3
MENOR	2
INSIGNIFICANTE	1

2.4 IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS

Una vez definida la frecuencia con la que se presentan las vulnerabilidades y amenazas en la Administración Municipal, se procede a calcular el riesgo de cada

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 13 de 24


amenaza para cada uno de los activos identificados y valorados. Posteriormente se calcula el nivel de riesgo total para cada activo, y definir el tratamiento a aplicar de acuerdo al tipo de activo y al nivel de riesgo identificado.

2.5 VALORACIÓN DE CONTROLES PARA TRATAMIENTO DE RIESGOS


Con base en la información referente al nivel de riesgo identificado y el tratamiento que se debe efectuar, se verifican los controles y/o procedimientos existentes en la Administración Municipal, estandarizados en el Anexo A de la norma NTC-ISO/IEC 27001:2013, el cual funciona como lista de chequeo para la implementación de controles y/o medidas de seguridad. Posteriormente se definen controles y/o procedimientos a implementar para seguir el tratamiento de riesgos indicado.

Tabla 34. Lista de Chequeo de Controles de Seguridad en Administración Municipal según ISO27001:2013


ISO 27001:2013 Controles de Seguridad			Controles actuales	Comentarios (justificación de exclusión)
5 Políticas de Seguridad	5,1	Dirección de la alta gerencia para la seguridad de la información		
	5.1.1	Políticas de seguridad de la información	Política general de SI publicada en el SIGC	
	5.1.2	Revisión de las políticas de seguridad de la información	Revisión anual de la Política general de SI	
6 Organización de la Seguridad de la Información	6,1	Organización interna		
	6.1.1	Roles y responsabilidad de seguridad de la información	Política general de SI publicada en el SIGC	
	6.1.2	Segregación de deberes	Asignación de responsabilidad sobre activos de información	
	6.1.3	Contacto con autoridades	Red de emergencias mediante empresa de seguridad	
	6.1.4	Contacto con grupos de interés especial	No existe asignación de responsabilidad para contactar grupos de interés	
	6.1.5	Seguridad de la información en la gestión de	No se han definido aplicación de políticas y/o procedimiento de SI	

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 14 de 24


		proyectos	en los proyectos	
	6,2	Dispositivos móviles y teletrabajo		
	6.2.1	Política de dispositivos móviles	No existe política para dispositivos móviles, pero existen directrices elevadas por talento humano	
	6.2.2	Teletrabajo	Se fomenta y aplican lineamientos de la política de teletrabajo pero no existe trazabilidad	
7 Seguridad en los Recursos Humanos	7,1	Previo al empleo		
	7.1.1	Verificación de antecedentes	Solicitud de antecedentes disciplinarios, fiscales, judiciales y profesionales	
	7.1.2	Términos y condiciones del empleo	Explícitamente no se definen obligaciones sobre la información a manejar	
	7,2	Durante el empleo		
	7.2.1	Responsabilidades de la Alta Gerencia	No existen procedimientos que garanticen responsabilidades de funcionarios sobre SI	
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	No existe conciencia de SI	
	7.2.3	Proceso disciplinario	No existen procesos disciplinarios para violaciones de SI	
	7,3	Terminación y cambio de empleo		
	7.3.1	Termino de responsabilidades o cambio de empleo	No se establecen acuerdos de confidencialidad con funcionarios	
	8 Gestión de Activos	8,1	Responsabilidad de los activos	
8.1.1		Inventario de activos	Inventario desactualizado, pendiente de revisión, asignación de responsabilidad y aprobación por la alta dirección	
8.1.2		Propiedad de activos	Se aplica formato de traslado de activos, pero se debe revisar clasificación y asignación final	
8.1.3		Uso aceptable de los activos	Es necesario sensibilización para el uso eficiente de los	

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 15 de 24


		activos	
8.1.4	Devolución de activos	Formato de traslado de activos y manual de almacén, pero es necesario socializar y divulgar	
8,2	Clasificación de la información		
8.2.1	Clasificación de la información	Procedimientos de clasificación de información por parte de Archivo Municipal	
8.2.2	Etiquetado de la información	Procedimiento de etiquetado para activos de información, que no se aplica a cabalidad	
8.2.3	Manejo de activos	Procedimientos establecidos en Manual de Almacén	
8,3	Manejo de medios		
8.3.1	Gestión de medios removibles	Procedimiento de gestión de medios, pendiente de divulgar	
8.3.2	Eliminación de medios	Procedimiento inexistente	
8.3.3	Transporte de medios físicos	Directrices formales por parte de la Alta Dirección	
9 Control de Acceso	9,1	Requerimientos de negocio para el control de acceso	
	9.1.1	Política de control de acceso	Procedimientos de control de acceso que no se cumplen en su totalidad
	9.1.2	Acceso a redes y servicios de red	No existe política de acceso a redes y servicios de red
	9,2	Gestión de accesos de usuario	
	9.2.1	Registro y baja del usuario	Manual de almacén, no se cumple el procedimiento en su totalidad
	9.2.2	Provisión de acceso a usuarios	Formato de solicitud de cuentas de usuario, pero no se realiza trazabilidad al acceso
	9.2.3	Gestión de derechos de acceso privilegiados	Formato de solicitud de cuentas de usuario, pero no se realiza trazabilidad al acceso
	9.2.4	Gestión de información de autenticación secreta de usuarios	No existe política de gestión de información de autenticación secreta de usuarios
	9.2.5	Revisión de derechos de acceso	No se realizan revisiones

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 16 de 24


		de usuarios	periódicas de derechos de acceso a usuarios	
	9.2.6	Eliminación o ajuste de derechos de acceso	Formato de solicitud de cuentas de usuario	
	9,3	Responsabilidades del usuario		
	9.3.1	Uso de información de autenticación secreta	No existe política de gestión de información de autenticación secreta de usuarios	
	9,4	Control de acceso de sistemas y aplicaciones		
	9.4.1	Restricción de acceso a la información	Formato de solicitud de cuentas de usuario, no existe políticas de control de acceso	
	9.4.2	Procedimientos de inicio de sesión seguro	No existe procedimiento de ingreso seguro a sistemas y aplicaciones	
	9.4.3	Sistema de gestión de contraseñas	No existe política de gestión de contraseñas, pero si se gestionan las contraseñas del correo institucional	
	9.4.4	Uso de programas y utilidades privilegiadas	Formato de solicitud de cuentas de usuario para aplicativos de la Administración, para otros programas y utilidades no existe procedimiento de control de software	
	9.4.5	Control de acceso al código fuente del programa	No existe procedimiento de gestión de código fuente de aplicativos	
10 Criptografía	10,1	Controles criptográficos		
	10.1.1	Política en el uso de controles criptográficos	SE EXCLUYE	No se aplican controles criptográficos en la entidad
	10.1.2	Gestión de llaves	SE EXCLUYE	No se gestionan llaves de criptografía en la entidad
11 Seguridad Física y del Entorno	11,1	Áreas seguras		
	11.1.1	Perímetro de seguridad físico	Restricciones mediante Vigilancia, cámaras y avisos de "Solo personal"	

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 17 de 24


		autorizado", sin definición general en la entidad	
11.1.2	Controles físicos de entrada	No existen controles robustos de ingreso a las instalaciones	
11.1.3	Seguridad de oficinas, habitaciones y facilidades	Restricciones mediante Vigilancia, cámaras y avisos de "Solo personal autorizado", sin definición general en la entidad	
11.1.4	Protección contra amenazas externas y del ambiente	Se encuentran definidos riesgos en el SGSST, mas no está implementada en áreas críticas de tecnología	
11.1.5	Trabajo en áreas seguras	No existe procedimiento de trabajo en áreas seguras	
11.1.6	Áreas de entrega y carga	Existen directrices asignadas a personal de vigilancia y bitácora de ingreso en entrada principal de cada sede, pero estas no están consolidadas en toda la entidad	
11.2	Equipo		
11.2.1	Instalación y protección de equipo	No existen directrices claras, por tanto no hay cumplimiento de las mismas por parte de funcionarios	
11.2.2	Servicios de soporte	No se cumple a cabalidad con los servicios de soporte requeridos en la entidad (electricidad, telecomunicaciones, aire acondicionado, etc.)	
11.2.3	Seguridad en el cableado	No existen medidas de protección y seguridad del cableado eléctrico y de telecomunicaciones, de acuerdo a estándares internacionales	
11.2.4	Mantenimiento de equipos	No existe plan de mantenimiento de equipos	
11.2.5	Retiro de activos	No existen directrices ni políticas definidas para retiro temporal de activos, aunque se aplica servicio de vigilancia y bitácora de ingreso en entrada	

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 18 de 24


		principal de cada sede	
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	No existen medidas de seguridad para activos que se encuentran fuera de las instalaciones
	11.2.7	Eliminación segura o reúso del equipo	No existen directrices para disposición segura o reúso de equipos
	11.2.8	Equipo de usuario desatendido	No existen directrices definidas ni procedimientos establecidos al respecto
	11.2.9	Política de escritorio limpio y pantalla limpia	No existen directrices ni políticas de escritorio y pantalla limpia
12 Seguridad en las Operaciones	12,1	Procedimientos Operacionales y Responsabilidades	
	12.1.1	Documentación de procedimientos operacionales	Manual de funciones. No existen procedimientos de operación detallados.
	12.1.2	Gestión de cambios	No existe procedimiento de control de cambios
	12.1.3	Gestión de la capacidad	No existen procedimientos de gestión de capacidad.
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	No existe procedimientos para la separación de ambientes
	12,2	Protección de Software Malicioso	
	12.2.1	Controles contra software malicioso	No existen políticas de prohibición de uso de software no autorizado, sin embargo se realizan sensibilizaciones al respecto.
	12,3	Respaldo	
	12.3.1	Respaldo de información	Se realizan backups de algunos sistemas de información, sin un procedimiento establecido para almacenamiento y pruebas de restauración
	12,4	Bitácoras y monitoreo	
	12.4.1	Bitácoras de eventos	No existe un registro de

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 19 de 24


		eventos u actividades de SI	
12.4.2	Protección de información en bitácoras	No existe procedimiento de control de la información de bitácoras	
12.4.3	Bitácoras de administrador y operador	No existe registros de actividades de administrador ni de operadores	
12.4.4	Sincronización de relojes	No se cuenta con fuente de referencia de tiempo único	
12,5	Control de software operacional		
12.5.1	Instalación de software en sistemas operacionales	No se realizan controles de actualizaciones de software	
12,6	Gestión de vulnerabilidades técnicas		
12.6.1	Gestión de vulnerabilidades técnicas	Solo existe el Mapa de Riesgos por Proceso en el SIG para gestión de riesgos, pero no abarca vulnerabilidades técnicas de los mismos	
12.6.2	Restricciones en la instalación de software	Se efectúan restricciones para la instalación de software pero no existe proceso documentado	
12,7	Consideraciones de auditoria de sistemas de información		
12.7.1	Controles de auditoría de sistemas de información	Procedimientos de Auditoría Interna y Planes de Mejora Continua	
13,1	Gestión de seguridad en red		
13 Seguridad en las Comunicaciones	13.1.1	Controles de red	En algunos casos se aplica el Formato de solicitud de cuentas de usuario, para aplicativos a los que se requiere acceso, perfil requerido, etc. Existen directrices de seguridad en redes pero no son cumplidas por los funcionarios
	13.1.2	Seguridad en los servicios en red	No se tienen identificados en todos los servicios de red directrices de seguridad en información
	13.1.3	Segregación en redes	Existen procedimientos básicos no documentados de

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 20 de 24


		segregación de redes en la entidad	
	13,2	Transferencia de información	
	13.2.1	Políticas y procedimientos para la transferencia de información	No existe seguimiento de flujo de comunicaciones en la red
	13.2.2	Acuerdos en la transferencia de información	No existen directrices u acuerdos de transferencia de información
	13.2.3	Mensajería electrónica	No existen directrices u definiciones de protección formal para mensajería electrónica
	13.2.4	Acuerdos de confidencialidad o no-revelación	No existen acuerdos ni políticas de confidencialidad de información transmitida
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14,1	Requerimientos de seguridad en sistemas de información	
	14.1.1	Análisis y especificación de requerimientos de seguridad	No existen directrices ni políticas de requerimientos de SI en Fichas Técnicas y Estudios Previos Contractuales
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	No existen directrices de seguridad formales de servicios en aplicaciones de redes públicas.
	14.1.3	Protección de transacciones en servicios de aplicación	No existen directrices de protección de transacciones en los servicios disponibles en la entidad
	14,2	Seguridad en el proceso de desarrollo y soporte	
	14.2.1	Política de desarrollo seguro	No existen políticas de desarrollo seguro de software
	14.2.2	Procedimientos de control de cambios del sistema	No existen directrices en el control de cambio de sistemas
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	No existen directrices de revisión técnica de aplicaciones
	14.2.4	Restricción de cambios en	No existen directrices de

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 21 de 24

		paquetes de software	restricción de cambios en paquetes de software	
	14.2.5	Principios de seguridad en la ingeniería de sistemas	No existe procedimiento de construcción de sistemas seguros	
	14.2.6	Entorno de desarrollo seguro	No existen políticas para ambientes de desarrollo seguro	
	14.2.7	Desarrollo tercerizado	No existen directrices para desarrollos contratados externamente	
	14.2.8	Pruebas de seguridad del sistema	No existen procedimientos de pruebas de seguridad	
	14.2.9	Pruebas de aceptación del sistema	No existen procedimientos de pruebas para aceptación de sistemas	
	14,3	Datos de prueba		
	14.3.1	Protección de datos de prueba	Se realizan backups de sistemas de información, pero no existen procedimientos para protección de datos de prueba	
15 Relaciones con Proveedores	15,1	Seguridad de la información en relaciones con el proveedor		
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	No existen políticas de SI para relaciones con proveedores	
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	No existen políticas de SI para relaciones con proveedores	
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	No existen políticas de SI para relaciones con proveedores	
	15,2	Gestión de entrega de servicios de proveedor		
	15.2.1	Monitoreo y revisión de servicios del proveedor	No existen políticas de SI para relaciones con proveedores	
	15.2.2	Gestión de cambios a los servicios del proveedor	No existen políticas de SI para relaciones con proveedores	
16 Gestión de	16,1	Gestión de incidentes de seguridad de la información y mejoras		

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 22 de 24


Incidentes de Seguridad de la Información	16.1.1	Responsabilidades y procedimientos	No existe asignación de responsabilidades y procedimientos de respuesta rápida a incidentes de seguridad	
	16.1.2	Reporte de eventos de seguridad de la información	No existen directrices ni procedimientos para aplicar en eventos de SI	
	16.1.3	Reporte de debilidades de seguridad de la información	No existe procedimiento de reporte de eventos de SI, pero se realizan reportes informales de los servidores por dependencia	
	16.1.4	Valoración y decisión de eventos de seguridad de la información	No existe reporte de eventos de SI	
	16.1.5	Respuesta a incidentes de seguridad de la información	No existen procedimientos de respuesta a incidentes de SI	
	16.1.6	Aprendizaje de incidentes de seguridad de la información	No existen procedimientos de respuesta a incidentes de SI, ni registro de incidentes	
	16.1.7	Colección de evidencia	Existen procedimientos de custodia de archivos como Tablas de retención documental, más no se aplican procedimientos para la identificación, recolección, adquisición y preservación de información	
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17,1	Continuidad de la seguridad de la información		
	17.1.1	Planeación de la continuidad de la seguridad de la información	No se tiene formalidad del BCP y no se tiene cumplimiento por parte de los funcionarios	
	17.1.2	Implementación de la continuidad de la seguridad de la información	Existen procedimientos para el mantenimiento de la información física de la entidad, pero no se tiene formalidad del BCP	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	No se han realizado pruebas de funcionalidad en SI	
	17,2	Redundancias		

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 23 de 24

	17.2.1	Disponibilidad de facilidades de procesamiento de información	No cuenta con elementos redundantes	
18 Cumplimiento	18,1	Cumplimiento con Requerimientos Legales y Contractuales		
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	Existen responsables para el cumplimiento de las leyes y tiene responsables en la identificación	
	18.1.2	Derechos de propiedad intelectual (IPR)	No se cuentan con procedimientos documentados y aprobados para tal fin, pero se entregan derechos contractuales de documentos realizados por contratistas	
	18.1.3	Protección de registros	Existen tablas de retención documental que especifican los registros y el periodo por el cual se deberían retener, además del almacenamiento, manejo y destrucción	
	18.1.4	Privacidad y protección de información personal identificable (PIR)	Existen algunas políticas de protección de información por aplicativo	
	18.1.5	Regulación de controles criptográficos	SE EXCLUYE	No se aplican controles criptográficos en la entidad
	18,2	Revisiones de seguridad de la información		
	18.2.1	Revisión independiente de seguridad de la información	Se cuentan con auditorias en SI	
	18.2.2	Cumplimiento con políticas y estándares de seguridad	No se realizan procedimientos de SI	
	18.2.3	Revisión del cumplimiento técnico	Se realiza revisión en algunos sistemas de información	

3 CONCLUSIONES DEL ANÁLISIS DE RIESGOS

Se efectúa una valoración efectiva a los activos de información de la Alcaldía, las amenazas y vulnerabilidades existentes, de modo que en el análisis y evaluación de

	SECRETARIA DE GOBIERNO Y SERVICIOS ADMINISTRATIVOS	Código: PLA-SG120-03
		Fecha aprobación: enero de 2021
	PLANES Y PROGRAMAS	Versión: 02
		Página 24 de 24

riesgos, se concluye que el mayor nivel de riesgo al que se enfrenta un activo, lo tienen los sistemas operativos de los servidores sobre los cuales operan los sistemas de información de la Administración Municipal, y que albergan gran cantidad de información de suma importancia para los procesos financieros y administrativos que se ejecutan al interior de la entidad territorial, y con los cuales se desarrollan las funciones y procesos misionales, dirigidos a la comunidad, Así mismo, de manera preliminar se puede concluir que el menor nivel de riesgo sobre un activo, lo tienen los servicios externos contratados (internet, ADSL, entre otros), puesto que no tienen mayor impacto sobre los procesos internos, y son de fácil tratamiento para la Administración.

Igualmente, se obtiene como resultado del mismo, que dentro de las actividades a desarrollar para la mitigación de riesgos en la Administración Municipal, uno de los propósitos fundamentales es la documentación de procedimientos de seguridad de información, la divulgación, sensibilización y la apropiación de los mismos entre los funcionarios, de modo que esto conlleve a mejorar todos los servicios que se ofrecen tanto a usuarios internos como a usuarios externos, siendo los primeros planes de mitigación a abarcar por la administración.

HEBER NEL MUÑOZ YASNO
Alcalde Municipal

Preparo: David Camilo Yunda
Apoyo a la gestión T.I.
Reviso: Eyder Julio Paz.
Profesional Universitario