AGENCIA PARA LA INFRAESTRUCTURA DEL META

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 102-TIC-PL-003 VERSIÓN 01

ELABORO	REVISÓ	APROBÓ
FRANCIS MOSQUERA NOVOA	FRANCIS MOSQUERA NOVOA	OSCAR DANIEL SALAMANCA
Cargo: Jefe Oficina Asesora de Planeación	Cargo: Jefe Oficina Asesora de Planeación	Cargo: Gerente

TABLA DE CONTENIDO

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

1. INTRODUCCIÓN

Este documento se elaboró con la recopilación de las mejores prácticas, nacionales e internacionales, para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del plan de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, es la entidad encargada de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

La estrategia de Gobierno en Línea, liderada por el Ministerio TIC, tiene como objetivo, garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones, con el fin de contribuir con la construcción de un Estado más participativo, más eficiente y más transparente.

La planificación e implementación del plan de Seguridad y Privacidad de la Información en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad.

El plan de Seguridad y Privacidad de la Información, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

2. OBJETIVO

Establecer las actividades encaminadas a la protección de la tecnología de la información que posee la Agencia para la Infraestructura de Meta AIM, para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

3. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Seguridad y Privacidad de la Información, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la estrategia de Gobierno en Línea.

Todas las referencias a las políticas, definiciones o contenido relacionado, publicadas en el compendio de las normas técnicas colombianas NTC ISO/IEC 27000 vigentes, así como a los anexos con derechos reservados por parte de ISO/ICONTEC.

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

4. ALCANCE

Este procedimiento tiene alcance para todos servidores públicos vinculados a la Agencia para la Infraestructura del Meta -AIM-, inicia desde la producción de información, continua y termina salvaguardando la información.

5. DEFINICIONES

ADMINISTRADOR: Es la persona encargada de mantener y administrar redes informáticas y entornos informáticos relacionados incluyendo hardware informático, software de sistemas, aplicaciones de software y todo tipo de configuraciones. Planificar, coordinar e implementar medidas de seguridad de red para proteger información, software y hardware.

BACKUP: Es una palabra inglesa que en ámbito de la tecnología y de la información, es una copia de seguridad o el proceso de copia de seguridad. Backup se refiere a la copia y archivo de datos de la computadora de modo que se puede utilizar para restaurar la información original después de una eventual pérdida de datos.

CONFIDENCIALIDAD: Propiedad de la información que determina que esté disponible a personas autorizadas. (https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html)

DISPONIBILIDAD: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera. (https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html)

HARDWARE: La palabra hardware en informática se refiere a las partes físicas tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos. Cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado componen el hardware.

INTEGRIDAD: Propiedad de salvaguardar la exactitud de la información y sus métodos de procesamiento deben ser exactos. (https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html)

REDES SOCIALES: Son sitios en Internet conformados por comunidades de individuos para compartir intereses o actividades y permiten intercambio de información.

SERVIDOR PÚBLICO: Son servidores públicos los miembros de las corporaciones públicas, los empleados y trabajadores del Estado y de sus entidades descentralizadas territorialmente y por servicios. Los servidores públicos están al servicio del Estado y de la comunidad; ejercerán sus funciones en la forma prevista por la Constitución, la ley y el reglamento. La ley determinará el régimen aplicable a los particulares que temporalmente desempeñen funciones públicas y regulará su ejercicio (artículo 123. Constitución Política de Colombia)

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

SEGURIDAD: Protección de los activos de información, contra amenazas que garanticen la continuidad de la entidad, minimizando el riesgo y maximizando las oportunidades de la unidad. Además la seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

SISTEMA DE INFORMACIÓN: Un sistema de información (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

SOFTWARE: Se conoce como software al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas

TECNOLOGÍA DE LA INFORMACIÓN: Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia. (https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html)

ACCESO A LA INFORMACIÓN PÚBLICA: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

ACTIVO DE INFORMACIÓN: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

ARCHIVO: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

AMENAZAS: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

ANÁLISIS DE RIESGO: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

AUDITORÍA: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

BASES DE DATOS PERSONALES: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

CIBERSEGURIDAD: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

CIBERESPACIO: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

CONTROL: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

DATOS ABIERTOS: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan ser reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

DATOS PERSONALES: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

DATOS PERSONALES PÚBLICOS: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

DATOS PERSONALES PRIVADOS: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

DEPARTAMENTO DEL META
Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

DATOS PERSONALES MIXTOS: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

DATOS PERSONALES SENSIBLES: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

DECLARACIÓN DE APLICABILIDAD: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

DERECHO A LA INTIMIDAD: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

ENCARGADO DEL TRATAMIENTO DE DATOS: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

INFORMACIÓN PÚBLICA CLASIFICADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

INFORMACIÓN PÚBLICA RESERVADA: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

LEY DE HABEAS DATA: Se refiere a la Ley Estatutaria 1266 de 2008.

LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA: Se refiere a la Ley Estatutaria 1712 de 2014.

MECANISMOS DE PROTECCIÓN DE DATOS PERSONALES: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

PLAN DE CONTINUIDAD DEL NEGOCIO: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

PLAN DE TRATAMIENTO DE RIESGOS: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

PRIVACIDAD: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

REGISTRO NACIONAL DE BASES DE DATOS: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

RESPONSABILIDAD DEMOSTRADA: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

RESPONSABLE DEL TRATAMIENTO DE DATOS: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

TITULARES DE LA INFORMACIÓN: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

TRATAMIENTO DE DATOS PERSONALES: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

TRAZABILIDAD: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

PARTES INTERESADAS (STAKEHOLDER): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

6. POLITICAS DE OPERACIÓN

6.1 GENERALIDADES

La Agencia determina las siguientes políticas de operación para el adecuado control de la seguridad y privacidad de la información:

a. Los servidores públicos que estén vinculados con la Agencia para la Infraestructura del Meta, serán responsables de la información que se generen en los procesos de la entidad.
b. El Servidor público del área de sistemas quien se denominará como ADMINISTRADOR, será el encargado de realizar BACKUP a los equipos de la Agencia y al Sistema de Información para la Gestión de Archivos de la Agencia - SIGA.
c. La información es un activo de mucho valor para la Agencia de Infraestructura del Meta AIM y como tal debe ser protegido. Es por ello que en la implementación de la seguridad de la información se debe procurar tener: 1. Integridad de la información. 2. Confidencialidad de la información. 3 Disponibilidad de la información. Por consiguiente de recomienda sobre seguridad de la información:

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

POLÍTICA DE ESCRITORIOS Y PANTALLAS LIMPIOS:

- Se debe guardar bajo llave la información crítica.
- Si utiliza una notebook, manténgala en un lugar seguro para evitar hurtos o robos.
- No deje pendrives, CD's u otro elemento removible con información en lugares visibles y accesibles.
- No dejar accesibles documentos impresos que contengan datos confidenciales.
- Se debe dejar su lugar de trabajo en orden, apagar los equipos y guardar los documentos al finalizar la jornada laboral.
- Cerrar la sesión al ausentarse o dejar de utilizar un sistema informático.
- Si debe abandonar, aunque sea momentáneamente, su puesto de trabajo, bloquee su terminal con un protector de pantalla que solicite el ingreso de una clave.

CARPETAS COMPARTIDAS:

- Se debe establecer contraseñas robustas en las carpetas compartidas a través de la red y cámbielas periódicamente.
- No se debe compartir todo el disco de la computadora.
- Distribuir la información a compartir en distintas carpetas.

TRASLADO DE INFORMACIÓN:

Todo traslado de informacion critica debe realizarse de manera que garantice la preservacion y la seguridad de la informacion

- Uso de sobres cerrados y firmados.
- Entrega en mano al personal autorizado.
- En caso de ser medios digitales, proteger los archivos con contraseña.

RESGUARDO DE INFORMACIÓN:

El resguardo de informacion permite tener disponible e integra la informacion ante una contingencia. Para ello se debe tener en cuenta:

- Realizar copias de seguridad periódicas de la información crítica y de trabajo diario.
- Guardar las copias en lugar seguro.
- Verificar la integridad física y lógica de los respaldos.
- Garantizar la confidencialidad de los datos respaldados.
- Reutilización segura de los medios.

NAVEGACIÓN EN INTERNET:

- Utilizar un navegador seguro y con la configuración recomendada por la Agencia.

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

- Evitar acceder a sitios desconocidos o no confiables.
- No aceptar la instalación automática de software.
- No descargar archivos de sitios web no confiables.
- Descargar los archivos en una carpeta y analizarlos con un antivirus actualizado antes de abrirlos.
- No ingresar información crítica o personal en formularios, páginas o foros.
- Si un sitio requiere información crítica o personal sólo hacerlos en sitios seguros (la dirección debe comenzar por https).
- Utilizar un antivirus reconocido, con la configuración recomendada por la Agencia, sino tiene uno, se debe solicitar al líder el proceso de Tecnología de la Información y la Comunicación. Verificar que siempre esté activo y actualizado a la fecha.
- Analizar siempre los medios removibles (discos, disquettes, pen-drives, mp3, celulares, cámaras digitales) que se conecten a la computadora.
- Ejecutar un analisis completo (analisis en profundidad) del equipo al menos una vez por semana.

6.2 NORMATIVIDAD

Ley 1437 de 2011," Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo "Capítulo IV, "utilización de medios electrónicos en el procedimiento administrativo".

Ley Estatutaria 1581 DE 2012, g) Principio de seguridad: "La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."

Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones":

Decreto 2573 de 2014 "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea..." donde se encuentra como componente el modelo de Seguridad y Privacidad de la Información.

Decreto 1413 de 2017, Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

Decreto 612 de 2018, Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

DEPARTAMENTO DEL META
Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

Conpes 3854 de 2016 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL.

7. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tabla 9. Plan de seguridad y privacidad de la información

Objetivo	Actividades	Cronograma				Presupuesto	Responsable
		2022	2023	2024	2025		
Ejecutar las actividades encaminadas a la protección de la tecnología de la información que posee la Agencia para la Infraestructura de Meta AIM, para salvaguardar la confidencialidad, integridad y disponibilidad de la información	Elaborar documento con la estrategia de planificación y control operacional.					No requiere recursos	Jefe oficina asesora planeación
	Revisar periódicamente el tratamiento de riesgos tecnológicos establecidos en la entidad					Se gestionaran los recursos necesarios para el cumplimiento de la actividad	Jefe oficina asesora planeación
	Fortalecer en hardware y software la Agencia					Se gestionaran los recursos necesarios para el cumplimiento de la actividad	Gerente Jefe oficina asesora planeación
	Realizar la medición periódica de los indicadores.					No requiere recursos	Jefe oficina asesora planeación
	Fortalecer en hardware y software la Agencia y Fortalecer redes internas de la entidad.					Se gestionaran los recursos necesarios para el cumplimiento de la actividad	Gerente Jefe oficina asesora planeación

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

8. DESCRIPCIÓN DE LA ACTIVIDAD

8.1 BACKUP DE LA INFORMACIÓN

FLUJOGRAMA	DESCRIPCIÓN DE LA ACTIVIDAD	RESPONSABLE
INICIO		
	Realizar el respaldo de información, producida de las diferentes actividades, que realizan los procesos de la Agencia. Se debe velar por el cumplimiento de los tres principios básicos de la seguridad de la información: integridad, confidencialidad y disponibilidad.	Servidores Públicos
	Salvaguardar la información en los equipos de la Agencia. Guardar la información de los contratos en el Sistema de Información para la Gestión de Archivos SIGA -, se usará el procedimiento Cargue de Información de Contratos en el Sistema de Información para la Gestión de Archivos – SIGA 102-TIC-PR-001 para tener en cuenta los parámetro de los archivos, que se almacenan en el SIGA	Servidores Públicos
	• Realizar BACKUP de la información contenida en los equipos de cada servidor público de la Agencia. • Hacer un respaldo de la información que se encuentra en el Sistema de Información para la Gestión de Archivos – SIGA. • Realizar, los BACKUP del software de correspondencia y carpetas compartidas de la red física de la Agencia.	Servidor Público (ADMINISTRADOR)
FIN		

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co

9. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN
		DOCUMENTO INICIAL

DEPARTAMENTO DEL META

Carrera 15 No.40-01 Primavera Urbana
Lobby 1 – Piso 8. Villavicencio - Meta
contactenos@aim-meta.gov.co