

AGENCIA PARA LA INFRAESTRUCTURA DEL META

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

102-TIC-PL-02 VERSIÓN 02




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

1. OBJETIVO	4
2. ALCANCE	4
3. DEFINICIONES	4
4. GENERALIDADES	6
4.1 NORMATIVIDAD	6
4.2 FORMULACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.....	6
4.2.1 Organización de la seguridad de la información.....	6
4.2.2 Política de la seguridad y privacidad de la información	7
4.2.3 Procedimientos, instructivos y otros.	7
4.3 FASE DIAGNOSTICO DEL MODELO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA AGENCIA.....	7
4.3.1 Situación actual.....	7
4.4 FASE PLANIFICACION DEL MODELO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA AGENCIA.....	10
4.4.1 Planificación.....	10
4.5 FASE IMPLEMENTACIÓN DEL MODELO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA AGENCIA.....	11
4.5.1 Implementación.....	11
4.6 FASE EVALUACIÓN DEL MODELO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA AGENCIA.....	12
4.6.1 Evaluación de desempeño.....	12



AGENCIA PARA LA
INFRAESTRUCTURA DEL META
NIT. 900 220 547-5

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

102-TIC-PL-02-V01
27/01/2023

4.7 FASE MEJORA CONTINUA DEL MODELO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA AGENCIA.....	12
4.7.1 Mejora continúa	12
4.8 MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.....	12
4.9 RECURSOS ECONÓMICOS	14
4.10PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 14	
5. CONTROL DE CAMBIOS	16

COPIA CONTROLADA





AGENCIA PARA LA
INFRAESTRUCTURA DEL META
NIT. 900 220 547-5

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

102-TIC-PL-02-V01
27/01/2023

1. OBJETIVO

Ejecutar las actividades de planeación y control de los activos de la información y comunicación que posee la Agencia para la Infraestructura de Meta AIM, salvaguardando la confidencialidad, integridad y disponibilidad

2. ALCANCE

Este documento aplica para todos los procesos de la Agencia para Infraestructura del Meta AIM.

3. DEFINICIONES

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.

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>)

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>)

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 gestión la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

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





AGENCIA PARA LA
INFRAESTRUCTURA DEL META
NIT. 900 220 547-5

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

102-TIC-PL-02-V01
27/01/2023

a los particulares que temporalmente desempeñen funciones públicas y regulará su ejercicio (artículo 123. Constitución Política de Colombia)

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.

CONFIDENCIALIDAD: Es la propiedad de la información, por la que se garantiza que no está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad se entiende en el ámbito de la seguridad informática, como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros. Esto debe hacerse independientemente de la seguridad del sistema de comunicación utilizado: de hecho, un asunto de gran interés es el problema de garantizar la confidencialidad de la comunicación utilizada cuando el sistema es inherentemente inseguro (como Internet).

DISPONIBILIDAD: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La definiremos también como la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. Pensemos, por ejemplo, en la importancia que tiene este objetivo para una empresa encargada de impartir ciclos formativos a distancia. Constantemente está recibiendo consultas, descargas a su sitio web, etc., por lo que siempre deberá estar disponible para sus usuarios.

INTEGRIDAD: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento. Diremos igualmente que es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. Este objetivo es muy importante cuando estamos realizando trámites bancarios por Internet. Se deberá garantizar que ningún intruso pueda capturar y modificar los datos en tránsito

SEGURIDAD: Protección de los activos de información, contra amenazas que garanticen la continuidad del negocio, minimizando el riesgo y maximizando las oportunidades de la unidad. Adema 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





AGENCIA PARA LA
INFRAESTRUCTURA DEL META
NIT. 900 220 547-5

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

102-TIC-PL-02-V01
27/01/2023

4. GENERALIDADES

4.1 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

Conpes 3854 de 2016 POLÍTICA NACIONAL DE SEGURIDAD DIGITAL

4.2 FORMULACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

La Agencia para la Infraestructura del Meta AIM, para formulación del plan de seguridad y privacidad de la información, seguirá los pasos establecidos en la Guía de la seguridad y privacidad de la información emitida por el Ministerio de la Tecnología de la Información y Comunicación.

4.2.1 Organización de la seguridad de la información

La alta dirección deberá apoyar la seguridad de la información dentro de la Agencia para la Infraestructura del Meta AIM; adquiriendo un compromiso a través de la definición de roles





AGENCIA PARA LA
INFRAESTRUCTURA DEL META
NIT. 900 220 547-5

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

102-TIC-PL-02-V01
27/01/2023

y responsabilidades dentro de la organización, propuesto a garantizar la seguridad de la información. Inicialmente se implementará en los procesos misionales.

4.2.2 Política de la seguridad y privacidad de la información

La Agencia para la Infraestructura del Meta AIM, entendiendo la importancia de una adecuada gestión de la información, se compromete a mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, generando un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

4.2.3 Procedimientos, instructivos y otros.

El proceso de la tecnología de la información y comunicación de la Agencia para la Infraestructura del Meta AIM, diseñara, implementara y socializara a todos los procesos de la agencia los procedimientos, instructivos y otros, que garanticen la seguridad y privacidad de la información

La Agencia de la Infraestructura del Meta AIM, usó la metodología planteada en el **Modelo de la Seguridad y Privacidad de la Información, emitido por el Ministerio de la Tecnología de la Información y Comunicación**. Donde contempla las siguientes fases:

4.3 FASE DIAGNOSTICO DEL MODELO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA AGENCIA

4.3.1 Situación actual

Se identificó el estado actual de la seguridad y privacidad de la información de la Agencia para la Infraestructura del Meta AIM, por medio de la **guía de la seguridad de la información emitida por el Ministerio de la Tecnología de la Información y comunicación**, donde se pretende con el diagnóstico alcanzar las siguientes metas

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.

En la actualidad la agencia realizo el siguiente diagnóstico (Tabla 1. Evaluación de efectividad de controles), usando la **herramienta Instrumento de identificación de la línea base de seguridad del Ministerio de la Tecnología de la Información y Comunicación**.





Tabla 1. Evaluación de efectividad de controles

Evaluación de Efectividad de controles			Evaluación de efectividad de control
Dominio	Calificación Actual	Calificación Objetivo	
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	18	100	INICIAL
SEGURIDAD DE LOS RECURSOS HUMANOS	17	100	INICIAL
GESTIÓN DE ACTIVOS	20	100	INICIAL
CONTROL DE ACCESO	20	100	INICIAL
CRIPTOGRAFÍA	20	100	INICIAL
SEGURIDAD FÍSICA Y DEL ENTORNO	20	100	INICIAL
SEGURIDAD DE LAS OPERACIONES	20	100	INICIAL
SEGURIDAD DE LAS COMUNICACIONES	20	100	INICIAL
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	7	100	INICIAL
RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	20	100	INICIAL
CUMPLIMIENTO	31,5	100	REPETIBLE
20	100	INICIAL	

Fuente: Instrumento de identificación de la línea base de seguridad del Ministerio de la Tecnología de la Información y Comunicación.

Grafico 1. Estado actual

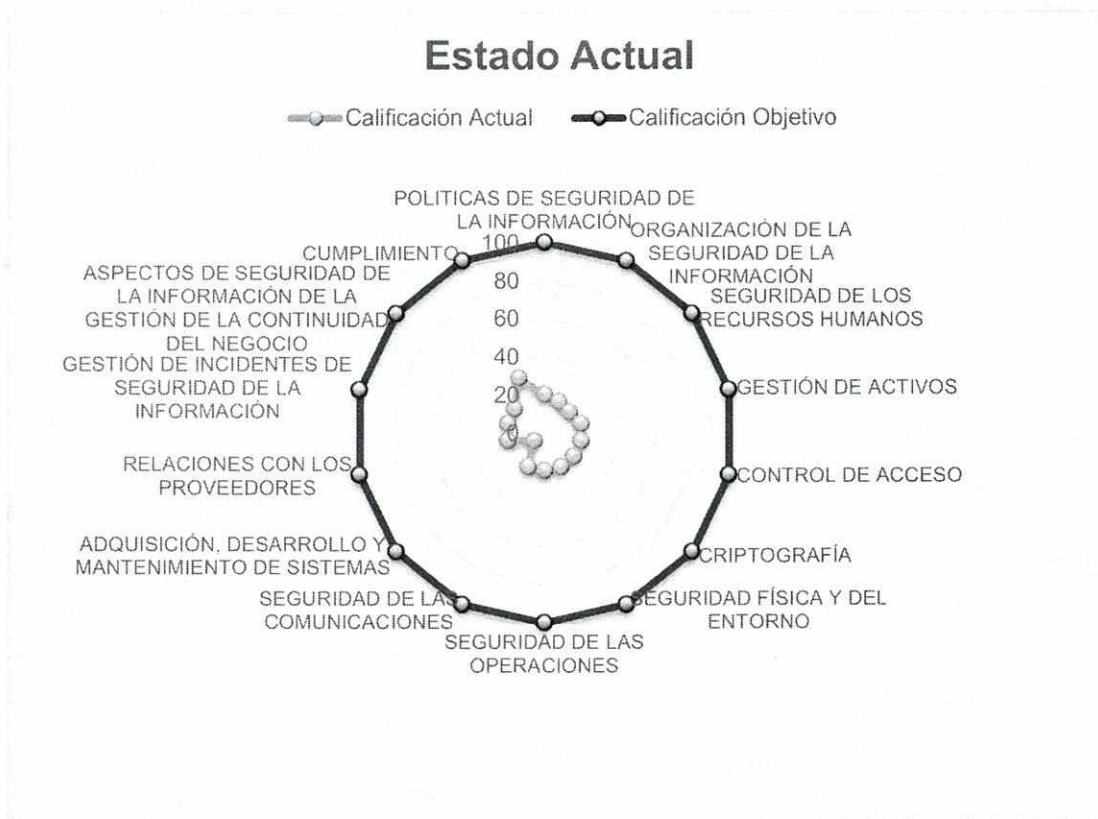


AGENCIA PARA LA
INFRAESTRUCTURA DEL META
NIT. 900 220 547-5

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

102-TIC-PL-02-V01
27/01/2023

Estado Actual



Con la **herramienta Instrumento de identificación de la línea base de seguridad del Ministerio de la Tecnología de la Información y Comunicación**, se realizó el diagnóstico para determinar el avance ciclo Planificar, hacer, Ajustar y Verificar (PHVA) de funcionamiento del modelo de operación. Obteniendo los siguientes resultados:

Tabla 2. Avance en el ciclo Planificar, hacer, Ajustar y Verificar

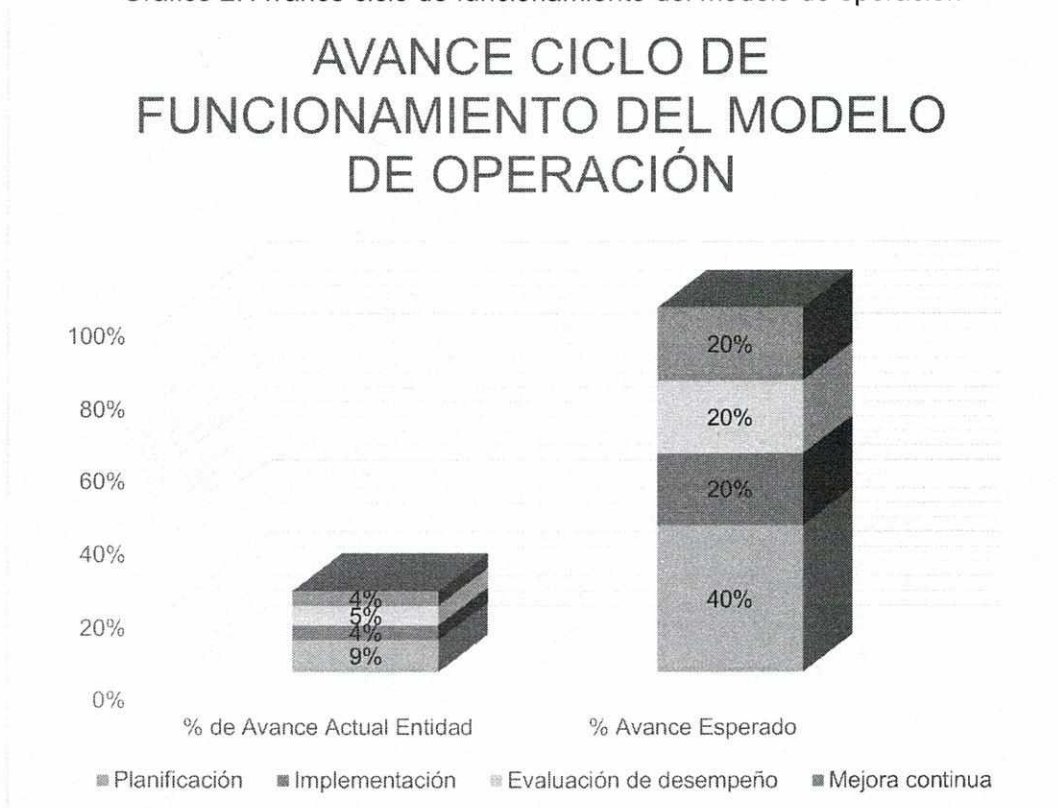
Año	Avance PHVA		
	Componente del Ciclo	% de Avance Actual Entidad	% Avance Esperado
2022	Planificación	9%	40%
	Implementación	4%	20%
	Evaluación de desempeño	5%	20%
	Mejora continua	4%	20%
TOTAL		22%	100%

Fuente: Instrumento de identificación de la línea base de seguridad del Ministerio de la Tecnología de la Información y Comunicación.





Grafico 2. Avance ciclo de funcionamiento del modelo de operación



4.4 FASE PLANIFICACION DEL MODELO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA AGENCIA

4.4.1 Planificación

Con los resultados obtenidos con el diagnóstico, la entidad seguirá lo planteado en la **Guía de la Seguridad de la Información emitida por el Ministerio de la Tecnología de la Información y Comunicación** para realizar la planificación (Tabla 3. Metas y resultados de planificación).

Tabla 3. Metas y resultados de planificación

Metas	Resultados
Política de Seguridad y Privacidad de la Información	Realizar documento con la política de seguridad de la información, debidamente aprobado y socializado al interior de la Entidad.



Metas	Resultados
Procedimientos de seguridad de la información.	Definir Procedimientos debidamente documentados, aprobados y socializados.
Roles y responsabilidades de seguridad y privacidad de la información.	Asignar a servidor público de la Agencia, a través de acto administrativo, las funciones donde será encargado de la seguridad de la información dentro de la entidad.
Inventario de activos de información.	Elaborar documento para la identificación, clasificación y valoración de activos de información.
Integración del plan de seguridad y privacidad de la información con el proceso de gestión documental	Aplicar la seguridad y la privacidad de la información en el proceso de gestión documental.
Identificación, Valoración y tratamiento de riesgo.	Definir los riesgos tecnológicos que se puedan presentar en la entidad, los cuales se deben identificar, valorar y dar tratamiento.
Manual de Comunicaciones.	Realizar documento donde se defina los medios de comunicación interna y externa que tiene la Agencia, garantizando el buen manejo de la información y esta se proporcione de una forma segura, clara y oportuna a los usuarios, clientes, servidores públicos y grupos de interés.

Fuente: Guía de la Seguridad de la Información emitida por el Ministerio de la Tecnología de la Información y Comunicación

4.5 FASE IMPLEMENTACIÓN DEL MODELO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA AGENCIA

4.5.1 Implementación

Para la implementación, la entidad seguirá lo planteado en la **Guía de la Seguridad de la Información emitida por el Ministerio de la Tecnología de la Información y Comunicación**, por consiguiente, se establecieron las siguientes metas, de acuerdo a la capacidad de recursos que cuenta la entidad, para el cumplimiento del Plan (Tabla 4. Metas y resultados de implementación).

Tabla 4. Metas y resultados de implementación

Metas	Resultados
Planificación y Control Operacional.	Elaborar documento con la estrategia de planificación y control operacional, revisado y aprobado.
Implementación del plan de tratamiento de riesgos.	Revisar periódicamente el tratamiento de riesgos tecnológicos establecidos en la entidad.
Indicadores De Gestión.	Realizar la medición periódica de los indicadores de gestión de seguridad y privacidad de la información.

Fuente: Guía de la Seguridad de la Información emitida por el Ministerio de la Tecnología de la Información y Comunicación

4.6 FASE EVALUACIÓN DEL MODELO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA AGENCIA

4.6.1 Evaluación de desempeño

Para la evaluación de desempeño, la entidad seguirá lo planteado en la **Guía de la Seguridad de la Información emitida por el Ministerio de la Tecnología de la Información y Comunicación**, donde establece las siguientes metas para su debida evaluación (Tabla 5. Metas y resultados de evaluación de desempeño)

Tabla 5. Metas y resultados de evaluación de desempeño

Metas	Resultados
Revisión y seguimiento, a la implementación del plan de seguridad y privacidad de la información.	Realizar revisiones periódicas a la implementación del plan de seguridad y privacidad de la información.
Plan de Auditorias	Incluir en las actividades de auditoria al proceso de tecnología la implementación del plan de seguridad y privacidad de la información.

Fuente: Guía de la Seguridad de la Información emitida por el Ministerio de la Tecnología de la Información y Comunicación

4.7 FASE MEJORA CONTINUA DEL MODELO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA AGENCIA

4.7.1 Mejora continúa

Para la mejora continúa, la entidad seguirá lo planteado en la **Guía de la Seguridad de la Información emitida por el Ministerio de la Tecnología de la Información y Comunicación**, por tal estableció la siguiente meta, para su cumplimiento (Tabla 6. Metas y resultados de mejora continúa)

Tabla 6. Metas y resultados de mejora continúa

Metas	Resultados
Mejora continua	Realizar los planes de mejoramiento, que se generen de los resultados de auditorías.

Fuente: Guía de la Seguridad de la Información emitida por el Ministerio de la Tecnología de la Información y Comunicación

4.8 MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Se establece en la tabla 7 el nivel de madurez del modelo de seguridad y privacidad de la información de la Agencia, de acuerdo al diagnóstico realizado con el **Instrumento de identificación de la línea base de seguridad del Ministerio de la Tecnología de la Información y Comunicación.**



Tabla 7. Nivel de madurez del Modelo de seguridad y privacidad de la Información de la Agencia

NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Nivel de cumplimiento	
	Inicial	SUFICIENTE
	Repetible	CRÍTICO
	Definido	CRÍTICO
	Administrado	CRÍTICO
	Optimizado	CRÍTICO

Fuente: Instrumento de identificación de la línea base de seguridad del Ministerio de la Tecnología de la Información y Comunicación.

Tabla 8. Descripción del nivel de madurez

Nivel	Descripción
Inexistente	Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo no están alineados a un Modelo de Seguridad.
	No se reconoce la información como un activo importante para su misión y objetivos estratégicos.
	No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
Inicial	Se han identificado las debilidades en la seguridad de la información.
	Los incidentes de seguridad de la información se tratan de forma reactiva.
	Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
Repetible	Se identifican en forma general los activos de información.
	Se clasifican los activos de información.
	Los servidores públicos de la entidad tienen conciencia sobre la seguridad de la información.
	Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.
	La entidad cuenta con un plan de diagnóstico para IPv6.



Nivel	Descripción
Definido	La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.
	La Entidad ha determinado los objetivos, alcance y límites de la seguridad de la información.
	La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.
	La Entidad tiene procedimientos formales de seguridad de la Información
	La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.
	La Entidad ha realizado un inventario de activos de información aplicando una metodología.
	La Entidad trata riesgos de seguridad de la información a través de una metodología.
	Se implementa el plan de tratamiento de riesgos.
	La entidad cuenta con un plan de transición de IPv4 a IPv6.
Administrado	Se revisa y monitorea periódicamente los activos de información de la Entidad.
	Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.
	Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.
	La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
Optimizado	En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización.
	Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.
	La entidad genera tráfico en IPv6.

Fuente: Guía de la Seguridad de la Información emitida por el Ministerio de la Tecnología de la Información y Comunicación

4.9 RECURSOS ECONÓMICOS

Para garantizar el cumplimiento de las actividades de planeación, implementación, evaluación y mejora del plan de seguridad y privacidad de la información de la Agencia, es necesario que se gestionen los recursos y que se han incluidos en el presupuesto de funcionamiento de la entidad.

4.10 PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tabla 9. Plan de seguridad y privacidad de la información



AGENCIA PARA LA
INFRAESTRUCTURA DEL META
NIT. 900 220 547-5

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

102-TIC-PL-02-V01
27/01/2023

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	Realizar el diagnóstico del Modelo de Seguridad y Privacidad de la Información de la Agencia					No requiere recursos	Jefe oficina asesora planeación
	Planificación: <ul style="list-style-type: none"> Realizar documento con la política de seguridad de la información. Definir Procedimientos. Asignar a servidor público responsable de la seguridad y privacidad de la información. Inventario de activos de información. Definir riesgos tecnológicos. 					No requiere recursos	Jefe oficina asesora planeación
	Implementación: <ul style="list-style-type: none"> Elaborar documento con la estrategia de planificación y control operacional. Revisar periódicamente el tratamiento de riesgos tecnológicos establecidos en la entidad Fortalecer en hardware y software la Agencia Realizar la medición periódica de los indicadores. Fortalecer redes internas de la entidad. 					Se gestionaran los recursos necesarios para el cumplimiento de la actividad	Gerente Jefe oficina asesora planeación
	Evaluación: <ul style="list-style-type: none"> Realizar revisiones periódicas a la implementación. Auditorías internas. 					No requiere recursos	Jefe oficina asesora planeación
	Mejora Continua: <ul style="list-style-type: none"> Realizar los planes de mejoramiento. 					No requiere recursos	Jefe oficina asesora planeación





AGENCIA PARA LA
INFRAESTRUCTURA DEL META
NIT. 900 220 547-5

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

102-TIC-PL-02-V01
27/01/2023

5. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN
1	01/10/19	DOCUMENTO INICIAL
2	28/01/23	DOCUMENTO ACTUALIZADO

COPIA CONTROLADA

