

Plan de Seguridad y Privacidad de la Información



Subgerencia de Tecnologías de la Información y las Comunicaciones

2023
Versión 1

Contenido

INTRODUCCIÓN.....	3
OBJETIVO.....	4
ALCANCE.....	4
METODOLOGIA APLICABLE.....	4
Fase 1- Diagnóstico	4
Fase 2- Planificación	4
Fase 3- Operación	5
Fase 4 – Evaluación de desempeño	5
Fase 5 – Mejoramiento Continuo.....	5
ESTRATEGIA DE IMPLEMENTACIÓN	5

INTRODUCCIÓN

La evolución del gobierno electrónico ha llevado a que el Estado Colombiano establezca la Política de Gobierno Digital en donde se define: (i) la gobernanza basado en el relacionamiento entre el orden nacional y territorial, y el nivel central y descentralizado, que involucre a los grupos de interés; (ii) cuatro (4) habilitadores que permiten ejecutar las líneas de acción en donde se encuentran relacionados los siguientes: arquitectura, seguridad y privacidad de la información, cultura y apropiación y servicios ciudadanos digitales; (iii) líneas de acción e (iv) iniciativas dinamizadoras



Ilustración 1: Esquema de estructura y habilitadores de la política de gobierno digital, fuente MinTic.

Teniendo en cuenta que, la seguridad y privacidad de la información se encuentra definida como uno de los habilitadores y en cumplimiento con lo establecido en la Resolución 500 del 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital” expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, la Agencia-ATENA define el plan descrito en el documento como parte integral para el fortalecimiento de procesos, trámites, servicios e infraestructura de TI más seguros; permitiendo así preservar la confidencialidad, integridad y disponibilidad de los activos de información los cuales apoyan el cumplimiento de objetivos institucionales y la relación de confianza con las partes interesadas.

OBJETIVO

Definir las actividades que permitan establecer, implementar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información – MSPI, alineadas con las buenas prácticas establecidas en la NTC/IEC 27001:2013 y la política de gobierno digital.

ALCANCE

Este documento es aplicable a todos funcionarios, contratistas, proveedores y terceros que, en cumplimiento de sus funciones utilicen, recolecten, procesen, intercambien, consulten y en general participen en el ciclo de vida de la información institucional.

METODOLOGÍA APLICABLE

De acuerdo con el contexto institucional y la metodología definida en el Modelo de Seguridad y Privacidad de la Información – MSPI, se contempla la operación del Subsistema de Gestión de Seguridad de la Información y seguridad digital basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten gestionar y mantener adecuadamente la seguridad y privacidad de los activos de información.



Ilustración 2. Ciclo de operación del modelo de seguridad y privacidad de la información, Fuente: MinTic.

Fase 1- Diagnóstico

Su objetivo es identificar el estado actual de la Entidad respecto a la adopción del MSPI basado en un análisis GAP.

Fase 2- Planificación

Se determinan las necesidades y objetivos de seguridad y privacidad de la información teniendo en cuenta el mapa de procesos y en general el contexto interno y externo. Esta fase define el plan de valoración y tratamiento de riesgos, siendo ésta la parte más importante del ciclo.

Fase 3- Operación

En esta fase se implementan los controles que van a permitir disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.

Fase 4 – Evaluación de desempeño

Determina el sistema y forma de evaluación de la adopción del modelo.

Fase 5 – Mejoramiento Continuo

Establece procedimientos para identificar desviaciones en las reglas definidas en el modelo y las acciones necesarias para su solución y no repetición

ESTRATEGIA DE IMPLEMENTACIÓN

A continuación, se relacionan las actividades a realizar en cada una de las fases metodológicas definidas, las cuales serán ejecutadas durante la vigencia 2023.

Cada una de las fases se dará por completada, cuando se cumplan todos los requisitos definidos

FASE	ACTIVIDADES	SALIDAS	RESPONSABLE	FINALIZACIÓN
Diagnóstico	Identificar el nivel de madurez de seguridad y privacidad de la información en que se encuentra la Entidad, como punto de partida para la implementación del MSPI	Herramienta de autodiagnóstico o (Análisis GAP)	Subgerencia TIC	30-Jun-2023
Planificación	Determinar las partes interesadas	Contexto institucional.	Subgerencia TIC	31-Mar-2023
	Establecer las funciones de seguridad y privacidad de la información a través de acto	Acto administrativo	Subgerencia TIC	30-Jun-2023

FASE	ACTIVIDADES	SALIDAS	RESPONSABLE	FINALIZACIÓN
	administrativo.			
	Revisar y determinar actualización de la política de seguridad y privacidad de la información	Política actualizada, aprobada, publicada y socializada.	Subgerencia TIC	30-Sep-2023
	Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información	Procedimiento de gestión de riesgos de seguridad	Subgerencia TIC	30-Jul-2023
	Estructurar una metodología que permita definir las acciones que debe seguir la Entidad para gestionar los riesgos de seguridad y privacidad de la información	Guía gestión de riesgos de seguridad.	Subgerencia TIC	31-Mar-2023
		Declaración de aplicabilidad	Subgerencia TIC	30-Jul-2023
		Plan de tratamiento de riesgos	Subgerencia TIC	31-Ene-2023
	Definir un plan de comunicación, capacitación, sensibilización y concientización	Plan de sensibilización y comunicación de seguridad de la información.	Subgerencia TIC	17-Feb-2023
	Definir plan de gestión de vulnerabilidades	Plan de análisis de vulnerabilidades	Subgerencia TIC	20-Mar-2023
Operación	Implementar los planes y controles para lograr los objetivos del MSPI	Plan de implementación de controles de seguridad y privacidad de la información que contenga como mínimo: controles, actividades,	Subgerencia TIC	15-Feb-2023

FASE	ACTIVIDADES	SALIDAS	RESPONSABLE	FINALIZACIÓN
		fechas, responsable de implementación y presupuesto		
		Evidencia de la implementación de los controles de seguridad y privacidad de la información.	Subgerencia TIC	31-Mar-2023 30-Jun-2023 31-Oct-2023 31-Dic-2023
	Gestionar vulnerabilidades	Informe de vulnerabilidades.	Subgerencia TIC	31-Oct-2023
		Plan de remediación.	Subgerencia TIC	31-Oct-2023
	Establecer contacto con los grupos de interés	Registro en CCOC, Csirt PONAL y Csirt Gobierno	Subgerencia TIC	30-Jun-2023 31-Dic-2023
	Socializar con el equipo TI los boletines informativos y de gestión para la prevención de incidentes de seguridad	Correo electrónico	Subgerencia TIC	A demanda
	Definir, implementar y probar las estrategias de continuidad de TI	Plan de pruebas de continuidad Informe ejecución de pruebas	Subgerencia TIC	31-Ago-2023
Evaluación de desempeño	Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.	Seguimiento de indicadores	Subgerencia TIC	31-Mar-2023 30-Jun-2023 31-Oct-2023 31-Dic-2023
	Apoyar las auditorías que se realicen al modelo de seguridad y privacidad de la información	Resultados de las auditorías internas	Subgerencia TIC	31-Oct-2023
		No conformidades de las auditorías internas.	Subgerencia TIC	31-Oct-2023
		Plan de auditorías que	Subgerencia TIC	31-Oct-2023

FASE	ACTIVIDADES	SALIDAS	RESPONSABLE	FINALIZACIÓN
		evidencia la programación de las auditorias de seguridad y privacidad de la información		
	Revisar seguimiento sobre la implementación del MSPI en la Entidad, por parte de la alta dirección (comité de gestión institucional), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia	Acta y documento de Revisión por la Dirección.	Subgerencia TIC	Fechas de comités
		Compromisos de la Revisión por la Dirección.	Subgerencia TIC	Fechas de comités
Mejoramiento Continuo	Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.	Plan de mejora	Subgerencia TIC	31-Oct-2023
	Revisar el cumplimiento de los procedimientos y políticas implementadas en materia de seguridad.	Plan de mejora	Subgerencia TIC	31-Oct-2023