Plan de Seguridad y Privacidad de la Información
2022 – 2024

Versión preliminar

Subgerencia de Tecnologías de la Información y las Comunicaciones

Bogotá D.C., enero 2022

Av. Eldorado No. 66 – 63
PBX: 324 10 00 Fax: 315 34 48
Código postal: 111321
www.educacionbogota.edu.co
Información: Línea 195

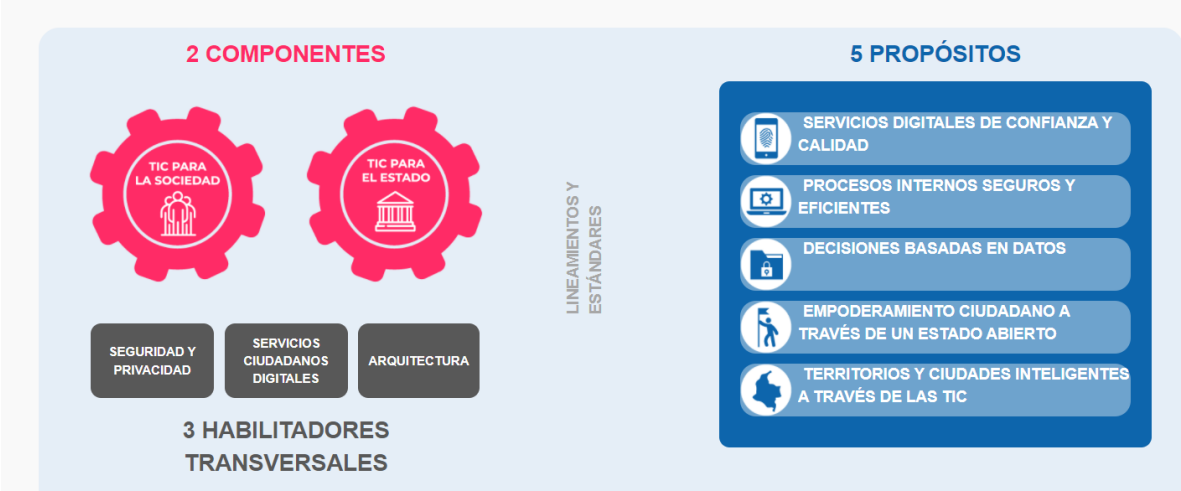
Contenido

INTRODUCCIÓN 3
OBJETIVO 4
ALCANCE 4
METODOLOGIA APLICABLE 4
ESTRATEGIA DE IMPLEMENTACIÓN 6
MARCO NORMATIVO 8

INTRODUCCIÓN

La Política de Gobierno Digital define dos (2) componentes: TIC para el Estado y TIC para la Sociedad, y tres (3) habilitadores transversales: Seguridad y privacidad de la información, servicios ciudadanos digitales y Arquitectura, como se evidencia a continuación:

Tabla 1: Esquema de componentes y habilitadores transversales 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 transversales y en cumplimiento con lo establecido en el Decreto 612 de 2018, 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.

METODOLOGIA 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.

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.

Ilustración 1. Ciclo de operación del modelo de seguridad y privacidad de la información, Fuente: MinTic.

ESTRATEGIA DE IMPLEMENTACIÓN

A continuación se relacionan las actividades a realizar en cada una de las fases metodológicas definidas, las cuales serán ejecutadas durante las vigencias 2022-2024.

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

Tabla 1: Estrategias de implementación

FASE	ACTIVIDADES	SALIDAS
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 (Análisis GAP)
Planificación	Determinar el alcance del MSPI y las partes interesadas	Política aprobada, publicada y socializada. Contexto institucional.
	Establecer las funciones de seguridad y privacidad de la información a través de acto administrativo.	Acto administrativo
	Definir y adoptar la política de seguridad y privacidad de la información	Política aprobada, publicada y socializada a través de acto administrativo.
	Establecer roles y responsabilidades asociadas a la seguridad y privacidad de la información	Conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.
	Estructurar una metodología que permita identificar y clasificar los activos de información	Procedimiento gestión de activos de información
		Guía gestión de activos de información
	Estructurar una metodología que permita gestionar los riesgos de seguridad y privacidad de la información	Procedimiento de gestión de riesgos de seguridad
		Guía gestión de riesgos de seguridad.
	Estructurar una metodología que permita definir las acciones que debe seguir la Entidad para poder	Declaración de aplicabilidad
		Plan de tratamiento de riesgos

FASE	ACTIVIDADES	SALIDAS
	gestionar los riesgos de seguridad y privacidad de la información	
	Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del MSPI	Incluir dentro de los proyectos de inversión de la Agencia -ATENEA aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido.
	Establecer y documentar las declaraciones especificas sobre la implementación de controles.	Manual de políticas de seguridad y privacidad de la información
	Definir un plan de comunicación, capacitación, sensibilización y concientización	Plan de capacitación, sensibilización y comunicación de seguridad de la información.
	Definir plan de análisis de vulnerabilidades	plan de análisis de vulnerabilidades
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, fechas, responsable de implementación y presupuesto
		Evidencia de la implementación de los controles de seguridad y privacidad de la información.
	Gestionar vulnerabilidades	Informe de vulnerabilidades.
		Plan de remediación.
	Establecer contacto con los grupos de interés	Registro en CCOC, Csirt PONAL y Csirt Gobierno
Evaluación de desempeño	Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.	Hoja de vida de indicadores
	Realizar auditorías con el fin de obtener información sobre el cumplimiento del MSPI	Resultados de las auditorías internas
		No conformidades de las auditorías internas.
		Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información
	Revisar el MSPI de 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.
		Compromisos de la Revisión por la Dirección.

FASE	ACTIVIDADES	SALIDAS
Mejoramiento Continuo	Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.	Plan de mejora documento

MARCO NORMATIVO

- 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”
- Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- 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”
- Ley 1273 de 2009. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado: de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, (“11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital)

- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política de Seguridad Digital del Estado Colombiano
- Guía para la administración de los riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo para la Función Pública - DAFP
- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.
- 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.

FIRMAS

	NOMBRE	CARGO	FECHA	FIRMA
APROBADO POR:				
REVISADO POR:	Lira Jazmín Pineda Moreno	Subgerente TIC	28/01/ 2022	
ELABORADO POR:	Maria Alejandra Suarez	Contratista TIC	24/01/ 2022	