CODIGO Y VERSION

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

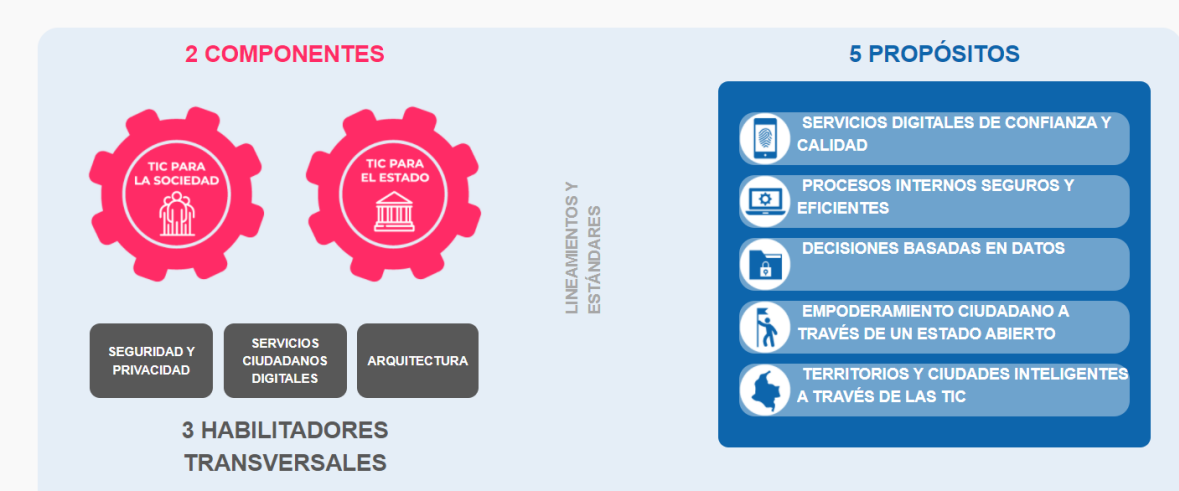
2022

La movilidad es de todos

Mintransporte

PRESENTACIÓN

La constante evolución del gobierno electrónico ha llevado a que el Estado Colombiano establezca la Política de Gobierno Digital en donde se definen 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:



En tal sentido la Superintendencia de Transporte establece y adopta el plan descrito en el documento como parte integral para el fortalecimiento de la confianza con el ciudadano, usuarios y grupos de interés a través de procesos interno seguros y eficientes; esto con la incorporación de la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información institucionales, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en la Entidad

TABLA DE CONTENIDO

1. OBJETIVO GENERAL

Establecer el Plan de Seguridad y Privacidad de la información a través de actividades que permitan establecer, implementar, operar, monitorear, revisar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información – MSPI y la estrategia de Seguridad Digital.

1.1 Objetivos Específicos

- Avanzar en la implementación del modelo de seguridad y privacidad de la información, con el propósito de mantener y mejorar el nivel de madurez de la entidad en materia de seguridad y privacidad de la información.
- Fortalecer el uso y apropiación en materia de Seguridad Digital en la Superintendencia de Transporte.

2. MARCO LEGAL

- 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 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)
- 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 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.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012
- 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”CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.
- 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 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

3. DEFINICIONES

- Activos de información: es: “algo que una organización valora y por lo tanto debe proteger”. Se puede considerar como un activo de información a: los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios. Es importante precisar que el concepto de activos de información definido en la ley 1712 de 2014 es diferente al concepto que maneja el MSPI – ISO 27001.
- Análisis de Vulnerabilidades: Identificación del nivel de exposición existentes en los sistemas, haciendo pruebas de intrusión, que sirven para verificar y evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos y servidores
- CSIRT: Equipos de respuesta a incidentes de seguridad.
- COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
- MSPI: Modelo de Seguridad y Privacidad de la Información

4. DESARROLLO DEL PLAN

A través del contexto institucional, estratégico y la metodología definida del Modelo de Seguridad y Privacidad de la Información – MSPI, la oficina TIC define una serie de actividades que permiten ejecutar las estrategias de gobierno digital establecidas 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”

4.1. Contexto Institucional

La Superintendencia de Transporte tiene como objetivo principal la vigilancia, inspección, y control que le corresponden al Presidente de la República como suprema autoridad administrativa en materia de tránsito, transporte y su infraestructura de conformidad con la ley y la delegación establecida en este decreto acceso, seguridad y legalidad, en aras de contribuir a una logística eficiente del sector.

Misión

Somos la Superintendencia que supervisa el servicio público de transporte, la actividad portuaria y la infraestructura, por una Colombia conectada, incluyente y competitiva.

Visión

En 2022 seremos reconocidos en el País, como la Superintendencia que de manera efectiva y transparente ejerce sus funciones de supervisión, protege a los usuarios y contribuye al fortalecimiento del sector transporte.

4.2. Contexto Estratégico

CONTEXTO ESTRATÉGICO ARTICULADO	
Objetivo Estratégico al que Contribuye	OE02 Fortalecer las Tecnologías de la Información y las Telecomunicaciones

CONTEXTO ESTRATÉGICO ARTICULADO	
Modelo Integrado de Planeación y Gestión - MIPG	Política Gobierno Digital Política de Seguridad Digital Política de Gestión Documental Política de Transparencia, acceso a la información pública y lucha contra la corrupción

4.3. Metodología

Es gestión propia del Modelo de Seguridad y Privacidad de la Información:

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

4.4. Actividades de Implementación

Planificación – Gestión de activos de información

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Publicación y actualización activos de información	Generar matriz con activos de información a publicar en el portal de datos abiertos	Matriz con activos de información anonimizados
	Generar matriz con índice de información clasificada y reservada a publicar en el portal de datos abiertos	Matriz con índice de información clasificada y reservada
	Publicar de activos de información en la página web institucional.	Correo electrónico de solicitud cargue de matrices
	Socializar sobre actualización de inventario de activos de información 2021	Correo electrónico/pieza gráfica
Actualización activos de información 2022	Actualizar manual de activos de información TIC-MA-004. Incluye parámetros para identificar infraestructuras críticas.	Documento publicado y aprobado en cadena de valor
	Actualizar formato para el registro, clasificación y actualización de activos de información TIC-FR-010	Documento publicado y aprobado en cadena de valor
	Generar pieza gráfica para sensibilización	Pieza gráfica
	Charla de sensibilización de conceptos sobre activos de información – socialización manual en su nueva versión TIC-MA-004	Actas de sesiones de sensibilización y capacitación
	Enviar correo electrónico solicitando la actualización de activos de información a los líderes de proceso.	Correo electrónico
	Revisar los activos de información reportados en el formato TIC-FR-010	Correo electrónico
	Retroalimentar y corregir de los activos reportados.	Correo electrónico / actas de mesa de trabajo
	Recibir de formato final y oficio de entrega por parte de los líderes de proceso.	Oficio de aceptación y entrega de activos

Planificación – Gestión de riesgos de seguridad de la información

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Actualización de documentación de riesgos de seguridad de la información	Evaluar la estrategia de seguridad digital para integrar en el manual de gestión de riesgo institucional y la política de riesgo de la entidad	Política gestión del riesgo actualizada en cadena valor Manual TIC-MAC-007 actualizado en cadena de valor
	Socializar documentos actualizados	Correo electrónico y pieza gráfica
Identificación, consolidación de riesgos de	Identificar, analizar y evaluar los riesgos de todos los procesos.	Matriz de riesgos

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
seguridad de la información y seguridad digital	Aceptación y aprobación de los riesgos identificados en cada uno de los procesos	Matriz de riesgos publicada en cadena de valor.
	Elaborar planes de tratamiento de riesgos	Matriz de riesgos publicada en cadena de valor.
Seguimiento planes de tratamiento	Realizar Seguimiento a los planes de manejo de riesgo de seguridad de la información establecidos por cada uno de los procesos y subprocesos, con sus respectivas evidencias.	Formato de seguimiento de planes de riesgos.
Evaluación de riesgos residuales	Evaluar el riesgo residual de los riesgos identificados	Matriz de riesgo / actas sesiones.

Planificación – Toma de conciencia y comunicación

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Conciencia y comunicación	Elaborar matriz de cultura y apropiación con los temas relacionados a seguridad de la información	Documento con actividades de cultura y apropiación
Ejecución de la estrategia de cultura y apropiación en seguridad de la información	Llevar a cabo las acciones que fomenten la cultura organizacional en materia de seguridad de la información	Correo electrónico, piezas gráficas
Medición de apropiación en seguridad de la información	Ejecutar acción programada que permita medir la apropiación de los conceptos/procedimientos de seguridad en la Entidad, a través de eventos controlados de phishing e ingeniería social	Correo electrónico, actas mesa de trabajo, reportes

Operación - Implementación

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Gobierno Digital	Comando Conjunto Cibernético - CCOC	Participar en las reuniones convocadas por CCOC	Correo electrónico / actas
		Cumplir los requerimientos de infraestructuras críticas del gobierno	Correo electrónico / actas
	Actualización datos de contacto con partes interesadas	Registrar enlace de seguridad con los equipos de CSIRT Gobierno, COLCERT, CSIRT Policía	Correo electrónico de registro y actualización
	Autodiagnóstico MSPI	Actualizar autodiagnóstico del MSPI	Autodiagnóstico

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Controles NTC/IEC ISO 27001:2013	Creación Declaración de aplicabilidad de controles de seguridad de la información	Definir y actualizar de controles aplicados en la Entidad.	Declaración de Aplicabilidad
	Implementación de controles de seguridad de la información	Implementar las políticas de seguridad definidas.	Reportes
Gestión de Vulnerabilidades	Aprovechamiento de seguridad plataforma office 365	Validar la implementación de controles de seguridad en las herramientas colaborativas.	
	Estructuración y ejecución del plan de análisis de vulnerabilidades	Elaborar el plan de análisis de vulnerabilidades, alcance y coordinar ejecución pruebas.	Plan de análisis de vulnerabilidades Informe d ejecución del plan
	Plan remediación de vulnerabilidades	Establecer plan de remediación de vulnerabilidades	Correo electrónico / actas
		Ejecutar plan de remediación.	Correo electrónico / actas

Operación - Gestión de incidentes

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Validar necesidad de documentos relacionados con incidentes de seguridad	Actualizar el ciclo de gestión de incidentes de seguridad (prevención, detección, análisis, clasificación, valoración, priorización, tiempos de respuesta, contención, recuperación, comunicación y aprendizaje)	Actualización y mejora del Manual de mesa de servicios de TI TIC-MA-008
Sensibilización sobre incidentes de seguridad.	Socializar la documentación creada/actualizada.	Actas sesiones Pieza gráfica
CSIRT PONAL / CSIRT / Comando Conjunto Cibernético - CCOC	Socializar con el equipo TI los boletines informativos y de gestión para la prevención de incidentes de seguridad.	Correo electrónico
Eventos/vulnerabilidades	Realizar seguimiento a las herramientas de seguridad informática validando comportamientos sospechosos sobre la infraestructura TI	Correo electrónico / actas sesiones

Operación - Continuidad de seguridad de la información

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Analizar impacto de la operación de TI	Documentar el análisis de impacto	BIA

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Determinar estrategias de continuidad de TI	Documentar las estrategias que permitan continuar con la operación de los servicios TI de acuerdo con la criticidad	Documento continuidad de servicios de TI aprobado y publicado en cadena de valor
Respuesta a la contingencia	Implementar las estrategias de continuidad de TI	Plan de crisis o incidentes Plan operativo de recuperación de entorno TI. Procedimiento de crisis o incidentes
Prueba, mantenimiento y revisión de continuidad	Ejecutar pruebas sobre las estrategias definidas	Plan de pruebas de continuidad Informe ejecución de pruebas
Consultoría continuidad de negocio	Establecer el alcance y criterio para el proceso de consultoría en continuidad del negocio	Documento técnico

Evaluación de desempeño

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Indicadores MSPI	Actualización de Indicadores	Revisar y actualizar de acuerdo con los objetivos del MSPI.	Hoja de vida de indicadores
	Gestión de indicadores	Reportar seguimiento de los indicadores	Reportes
Auditorías Internas y Externas	Apoyo en las auditorias que se realicen.	Participar en las auditorias que se realicen correspondientes a seguridad de la información	Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información

Mejoramiento continuo

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Mejora	Validación en sitio y sobre la infraestructura tecnológica la	Revisar el cumplimiento de los procedimientos y políticas	Informe

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
	implementación de la política y los controles de seguridad	implementadas en materia de seguridad.	
	Reporte de oportunidades de mejora	Generar oportunidades de mejora que se requieran, derivadas de las visitas de inspección y revisión de la documentación del MSPI	Oportunidades de mejora

4. SEGUIMIENTO

La dependencia encargada de realizar el monitoreo, seguimiento y control del plan de acuerdo con la competencia y la normatividad vigente es Oficina de Tecnologías de la información y las comunicaciones.

5. CONTROL DE CAMBIOS DEL DOCUMENTO

Control de cambios		
Versión	**Fecha**	**Descripción del cambio**
1	30-Nov-2020	Creación del documento
2	20-Ene-2022	Actualización del plan de seguridad digital y desagregación de actividades por componente que se desarrollaran durante el año y de acuerdo con el anexo 1 de 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”

6. APROBACIÓN DEL DOCUMENTO

Aprobación del documento		
Etapa	**Nombres y apellidos**	**Cargo**
Elaboró	Maria Alejandra Suarez	Contratista oficina TIC
Revisó:	Claudia Milena Rodríguez Alvarez	Asesora despacho del superintendente
Aprobó	Jorge Guillermo Neira	Jefe de Oficina TIC