

	PLAN	<b>Código: PL-TIC-01</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 03
		Fecha: 31/01/2022
		<b>Página 1 de 10</b>

## PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



**Secretaría de Tecnologías  
de la Información y la Comunicación**  
*Gobernación del Quindío*



**GOBERNACION DEL QUINDIO**

**2022**

	<b>PLAN</b>	<b>Código: PL-TIC-01</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 03
		Fecha: 31/01/2022
		<b>Página 2 de 10</b>

## 1. INTRODUCCIÓN

La gobernación del Quindío reconoce la importancia y el valor que tiene la información que maneja los sistemas de información estratégicos, misionales y de apoyo en el desarrollo de las funciones propias de la administración central departamental. Dicha información debe de ser protegida contra accesos no autorizados, o contra daños intencionados o no intencionados que puedan comprometer la integridad, la disponibilidad y la confidencialidad de esta.

Por otra parte, el decreto 1008 de 2018, en el artículo 2.2.9.1.1.3 Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales (Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales) los cuales son los elementos fundamentales para la implementación de la estrategia y el logro de los propósitos de la Política de Gobierno Digital.

Teniendo en cuenta lo anterior, el habilitador transversal de seguridad y privacidad de la información, se debe implementar bajo el modelo de seguridad y privacidad de la información MSPI, en el que a través de un correcto diagnóstico, unaplanificación, la implementación del mismo, una evaluación de desempeño acompañado siempre de mejora continua garantizará que la confidencialidad, la integridad y la disponibilidad de la información en la administración central departamental.

	<b>PLAN</b>	<b>Código: PL-TIC-01</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 03
		Fecha: 31/01/2022
		<b>Página 3 de 10</b>

## 2. OBJETIVO GENERAL

Establecer el Plan de Seguridad y Privacidad de la Información, el cual está dirigido a la implementación del modelo de seguridad y privacidad de la información MSPI y a todas las etapas que lo componen. Lo anterior en atención al contexto organizacional de la entidad, las capacidades técnicas y recursos disponibles.

### 2.1. OBJETIVOS ESPECÍFICOS

- Comunicar e implementar la estrategia de seguridad de la información.
- Identificar infraestructuras críticas en las entidades a través de la implementación de mejores prácticas de seguridad de la información.
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MSPI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

	<b>PLAN</b>	<b>Código: PL-TIC-01</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 03
		Fecha: 31/01/2022
		<b>Página 4 de 10</b>

### 3. MARCO LEGAL

Legislación	Tema	Referencia
Ley 527 de 1999	“Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos”	El mensaje de datos es “La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el télex o el telefax”.
Ley 1226 del 2008	“Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países”	Se regula el manejo de la información para “todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades de naturaleza pública o privada”.
Ley 1273 del 2009	“Por medio de la cual 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”.	“De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos”.
CONPES 3701 de 2011	Lineamientos de política para ciberseguridad y Ciberdefensa	Busca generar lineamientos de política en ciberseguridad y ciberdefensa encaminados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país.
Ley 1581 de 2012	Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales	Hace referencia, en particular, al artículo 15 de la Constitución Nacional, según el cual “todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
Ley 1712 de 2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública	Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que “Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley”. El objeto de la ley es “regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y

	<b>PLAN</b>	<b>Código: PL-TIC-01</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 03
		Fecha: 31/01/2022
		<b>Página 5 de 10</b>

		garantía del derecho y las excepciones a la publicidad de información”.
Decreto 2573 del 2014	Estrategia de Gobierno en Línea de la República de Colombia	El Decreto establece los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto 113 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones	El decreto tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.
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"	Permite lograr una mejor competitividad, proactividad e innovación en la ciudadanía y el Estado, por lo que la gobernación del Quindío desempeña un papel importante con la implementación de recursos tecnológicos que le permita alcanzar los propósitos que dispone esta ley, gestionando los riesgos y amenazas que traigan consigo la implementación de nuevas tecnologías de la información o avances tecnológicos que puedan beneficiar tanto a la entidad como a los municipios del departamento y sus comunidades.
Resolución número 00500 de marzo 10 de 2022	"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"	La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.
Directiva presidencial No. 03 del 15 de marzo de 2022	Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.	Con el fin de dar cumplimiento al artículo 147 de la Ley 1955 de 2019, "Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad", disminuir los costos de funcionamiento, acelerar la innovación, brindar entornos confiables digitales para las entidades públicas y mejorar sus procedimientos y servicios, se imparten las siguientes directrices

	<b>PLAN</b>	<b>Código: PL-TIC-01</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 03
		Fecha: 31/01/2022
		<b>Página 6 de 10</b>

<b>4. CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>					
<b>FASE MSPI</b>	<b>ACTIVIDADES</b>	<b>META</b>	<b>PRODUCTO</b>	<b>RESPONSABLE(S)</b>	<b>FECHA</b>
Diagnóstico	Realizar el Diagnóstico del modelo seguridad privacidad de la Información de la Gobernación del Quindío	Establecer las fortalezas y debilidades que tiene la entidad en cuanto a la seguridad y privacidad de la información	Diagnóstico MSPI	Director de Gobierno Digital	15/04/2022
Planificación	Realizar Cronograma de actividades de todas las fases del modelo de seguridad y privacidad de la información MSPI	Establecer el cronograma de actividades correspondiente a la implementación del modelo de seguridad y privacidad de la información	Plan de seguridad y privacidad de la información	Director de Gobierno Digital	29/04/2022
	Procedimientos de seguridad de la información.	Diseñar y/o actualizar las políticas de seguridad y privacidad de la información de la gobernación del Quindío	Políticas de seguridad y privacidad de la información	Director de Gobierno Digital	13/05/2022
	Diseñar y/o actualizar los Procedimientos de seguridad de la información.	Actualizar los procedimientos de seguridad y privacidad de la información, con el fin de que sean normalizados, por la secretaría de Planeación	Procedimientos de seguridad de la información.	Director de Gobierno Digital	03/06/2022
	Definir los Roles y responsabilidades de seguridad y privacidad de la información.	Lograr establecer los roles y responsabilidades en seguridad y privacidad de la información que incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Roles y responsabilidades de seguridad y privacidad de la información.	Director de Gobierno Digital	24/06/2022

	<b>PLAN</b>	<b>Código: PL-TIC-01</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 03
		Fecha: 31/01/2022
		<b>Página 7 de 10</b>

	Realizar el levantamiento de matriz de activos de información	Crear un documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección.	Matriz de Inventario de activos de información.	Director de Gobierno Digital	13/05/2022
	Con base a la matriz de inventario de activos de información, se identifican los riesgos de seguridad y privacidad de la información y seguridad digital	Identificación, Valoración y tratamiento de riesgo.	Plan de tratamiento de riesgos de seguridad y privacidad de la información y matriz de riesgos de seguridad y privacidad de la información y seguridad digital	Director de Sistemas y Director de Gobierno Digital	20/05/2022
	Realizar piezas gráficas y material de promoción y sensibilización en seguridad de la información en la gobernación del Quindío	Crear un plan y/o Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Plan de sensibilización y comunicación de seguridad y privacidad de la información	Director de Gobierno Digital	01/06/2022
	Realizar todas las actividades de identificación y planificación de la infraestructura compatible con el protocolo IPV6	Establecer el estado actual de la entidad en cuando a la implementación del protocolo IPV6 en la entidad.	Plan de diagnóstico de IPV4 a IPV6.	Director de Gobierno Digital	30/06/2022

	<b>PLAN</b>	<b>Código: PL-TIC-01</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 03
		Fecha: 31/01/2022
		<b>Página 8 de 10</b>

Implementación	Actualizar la declaración de aplicabilidad y el plan de control operacional	Establecer un Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Declaración de aplicabilidad y plan de control operacional	Director de Gobierno Digital	02/08/2022
	Realizar las actividades necesarias con el fin de dar seguimiento a el plan de tratamiento de riesgos	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Implementación del plan de tratamiento de riesgos.	Director de Gobierno Digital	30/6/2022
	Definir y medir los indicadores de gestión de la implementación del modelo de seguridad y privacidad de la información	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Indicadores De Gestión.	Director de Gobierno Digital	30/06/2022
	Definir las actividades de transición hacia el protocolo IPV6 en la administración central departamental	Realizar un plan de transición del protocolo de IPV6 de la gobernación del Quindío.	Plan de Transición de IPv4 a IPv6	Director de Sistemas y Director de Gobierno Digital	01/08/2022
Evaluación de Desempeño	Con los datos obtenidos en la implementación, se debe realizar plan donde se evalué el desempeño de la planificación e implementación del modelo MSPI	Crear documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	Plan seguimiento MSPI	Director de Gobierno Digital	15/09/2022
	Definir las actividades que debe realizar la persona y/o organización que realice la auditoria del modelo MSPI	Realizar una auditoría independiente sobre la efectividad de la implementación del modelo de seguridad y privacidad de la información	Plan de Ejecución de Auditorias	Director de Gobierno Digital	15/10/2022

	<b>PLAN</b>	<b>Código: PL-TIC-01</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 03
		Fecha: 31/01/2022
		<b>Página 9 de 10</b>

<b>Mejora Continua</b>	Con base a los resultados de la evaluación de desempeño se debe plantear el plan de mejoramiento.	Realizar un Plan de mejoramiento, con el fin de comenzar de nuevo el ciclo del modelo MSPI y corregir lo que haya lugar	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Director de Gobierno Digital	30/11/2022
------------------------	---	---	--	------------------------------	------------

	<b>PLAN</b>	<b>Código: PL-TIC-01</b>
	<b>PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	Versión: 03
		Fecha: 31/01/2022
		<b>Página 10 de 10</b>

## 5. DOCUMENTOS DE REFERENCIA

Guías Modelo de Seguridad y Privacidad:

- Guía 1 - Metodología de pruebas de efectividad
- Guía 2 - Política General MSPI v1
- Guía 3 - Procedimiento de Seguridad de la Información
- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 6 - Gestión Documental
- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 9 - Indicadores Gestión de Seguridad de la Información
- Guía 10 - Continuidad de Negocio
- Guía 11 - Análisis de Impacto de Negocio
- Guía 12 - Seguridad en la Nube
- Guía 13 - Evidencia Digital (En actualización)
- Guía 14 - Plan de comunicación, sensibilización, capacitación
- Guía 15 - Auditoria
- Guía 16 - Evaluación de Desempeño
- Guía 17 - Mejora continua
- Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
- Guía 19 - Aseguramiento de protocolo IPv4\_IPv6
- Guía 20 - Transición IPv4\_IPv6
- Guía 21 - Gestión de Incidentes

ELABORACION	REVISION	APROBACIÓN
Elaborado por:	Revisado por:	Aprobado por:
Cesar Augusto Jaramillo Patiño	Bryan Johann Aranzazu Medina	Jhon Mario Lievano
Cargo: Profesional Universitario	Cargo: Director Gobierno Digital	Cargo: Secretario TIC