TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Fábrica de Licores del Tolima reconoce la información como un activo estratégico que soporta el cumplimiento de su misión institucional, la operación productiva, la gestión financiera, la comercialización de licores y el cumplimiento de obligaciones legales y de control fiscal.

En cumplimiento de la Política de Gobierno Digital, el Modelo Integrado de Planeación y Gestión (MIPG) y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), se adopta el presente Plan de Seguridad y Privacidad de la Información (PSPI) para la vigencia 2026.

2. OBJETIVOS

OBJETIVO GENERAL:

Establecer los lineamientos, responsabilidades, controles y mecanismos de seguimiento para la gestión de la seguridad y la privacidad de la información en la Fábrica de Licores del Tolima, con el fin de:

OBJETIVOS ESPECIFICOS:

- Proteger la confidencialidad, integridad y disponibilidad de la información.
- Garantizar el adecuado tratamiento de los datos personales.
- Identificar, analizar y tratar los riesgos de seguridad de la información.
- Prevenir, detectar y gestionar incidentes de seguridad informática.
- Dar cumplimiento a la normativa legal vigente y a los lineamientos MinTIC aplicables a 2026.

3. ALCANCE

Este plan tiene aplicación a:

- Todos los **procesos estratégicos, misionales y de apoyo** de la FLT.
- Toda la **información institucional**, en cualquier formato (digital, físico, verbal, audiovisual).

- Todos los sistemas de información, aplicaciones, bases de datos, redes, servidores y dispositivos tecnológicos.
- Infraestructura tecnológica local, virtualizada, tercerizada o en la nube.
- Todos los funcionarios, contratistas, proveedores y terceros que tengan acceso a información o sistemas de la entidad.

4. TERMINOS Y DEFINICIONES

Activo de información: todos aquellos datos, documentos, sistemas, software, hardware, redes, infraestructura física y recursos humanos que tienen valor para una organización y son cruciales para su funcionamiento. Incluyen cualquier elemento que permita la creación, procesamiento, almacenamiento o transmisión de información, requiriendo protección para garantizar su confidencialidad, integridad y disponibilidad.

Confidencialidad: Propiedad que garantiza que la información solo sea accesible a personas autorizadas.

Integridad: Propiedad que asegura que la información sea exacta, completa y no haya sido alterada sin autorización.

Disponibilidad: Propiedad que garantiza que la información y los servicios estén disponibles cuando se requieran.

Dato personal: cualquier información que identifique o haga identificable a una persona física, ya sea directamente (nombre, DNI) o indirectamente (dirección IP, datos de localización, historial de navegación). Incluyen datos comunes como tu edad, domicilio, teléfono y correo electrónico, así como información más sensible (salud, origen étnico, creencias) y digital (fotos, voz, huellas dactilares).

Dato sensible: Dato personal que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación, riesgo grave o vulneración de derechos.

Incidente de seguridad de la información: Evento que compromete o pone en riesgo la confidencialidad, integridad o disponibilidad de la información.

MSPI: Modelo de Seguridad y Privacidad de la Información definido por el MinTIC para entidades públicas.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

5. OBJETIVOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

- Gestionar los sucesos de la seguridad de la información de la Fábrica de Licores del Tolima.
- Robustecer la seguridad y disponibilidad de la información y de la plataforma tecnológica ajustados a la declaración de aplicabilidad aprobada.
- Atender los requerimientos legales aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.

6. MARCO LEGAL

6.1. Gobierno Digital y Seguridad de la Información

- Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC
- Decreto 1008 de 2018 – Política de Gobierno Digital
- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital
- Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC)
- Modelo Integrado de Planeación y Gestión – MIPG

6.2 Protección de Datos Personales

- Ley 1581 de 2012
- Decreto 1377 de 2013
- Decreto 1074 de 2015
- Ley 1266 de 2008

6.3 Transparencia

- Ley 1712 de 2014
- Decreto 103 de 2015

6.4 Estándares de referencia

- ISO/IEC 27001
- ISO/IEC 27002
- ITIL v4

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

7.1 Roles y Responsabilidades

La entidad define nuevamente los roles y responsabilidades al interior de la entidad con la seguridad de la información de la siguiente manera:

Alta Dirección: Será la responsable definir, implementar y actualizar la Política de Seguridad de la información de liderar su implementación. Conformada por la Gerencia General y líderes de procesos.

Comité de Seguridad de la Información: Proponer mecanismos, metodologías,

lineamientos y procesos específicos para dar cumplimiento a la normatividad y lineamientos relacionados con Gobierno digital, seguridad y privacidad de la información, esto una vez esté constituido en la entidad. Orientar y coordinar su implementación. A través del comité institucional de Gestión y Desempeño presentará los avances obtenidos.

Analista y Líder de seguridad de la información: Para el caso particular de esta entidad sería el profesional de apoyo a la gestión en Ingeniería de Sistemas quien realizará las labores propias tales como el apoyo a la coordinación de la implementación de este modelo.

La Oficina de Control Interno. Realizar seguimiento en el cumplimiento de las políticas y plan de seguridad y privacidad de la información; así mismo, de hacer seguimiento a la gestión de riesgos. Evaluar sus avances a través de evidencias, herramientas autodiagnósticos de la Función Pública.

7.2 Responsabilidades en la Gestión Táctica y operativa de Seguridad Digital

Los funcionarios que tengan a su cargo o sean responsables de archivos públicos deben velar por la integridad, autenticidad, veracidad y fidelidad de la información de los documentos de archivo, sean éstos físicos o electrónicos, y serán responsables de su organización y conservación, de acuerdo con lo dispuesto en la Ley general de archivos.

8. SEGURIDAD EN EL RECURSO HUMANO

Con un criterio de seguridad de la información ya definido, la Fábrica de Licores del Tolima para la vinculación de las personas, o en actas de entrega del cargo, donde los usuarios, propietarios y administradores asumen formalmente la información que se les confía, elaborará un acuerdo de buen uso, de confidencialidad y no divulgación de la información sensitiva y de la información de carácter personal del ciudadano en favor de proteger y manejar bien este activo. Con lo anterior, si algún trabajador, funcionario o contratista, deja de prestar servicios en la Entidad o, en su caso, va a depender de otra dependencia aseguran el retorno total de la información que gestionó durante el ejercicio de sus funciones, se comprometen a no utilizar, no comercializar, no divulgar los productos o la propia información generada durante su gestión en la Entidad, durante el tiempo establecido por la normatividad aprobada de retención documental por la Fábrica de Licores del Tolima.

9. GESTION DE ACTIVOS

Se tiene como actividad para la presente vigencia el proceso de actualización de los activos de información, su clasificación, la asignación de responsabilidades a los activos de información y su tratamiento conforme a su clasificación, todo aplicado a la metodología propuesta por MINTIC, y la ISO 27000.

10. GESTION Y TRATAMIENTO DE RIESGOS.

a. Mapa de Riesgos de Seguridad y Privacidad de la Información.

Para esta vigencia se actualizará el mapa de riesgos referentes a la seguridad y privacidad de la información para cada uno de los procesos del SIG.

La FLT implementa un proceso formal de **gestión de riesgos**, alineado con el MSPI y MIPG:

Etapas:

1. Identificación de activos de información
2. Identificación de amenazas y vulnerabilidades
3. Análisis y valoración del riesgo (impacto y probabilidad)
4. Definición de controles y plan de tratamiento
5. Aceptación, mitigación, transferencia o eliminación del riesgo
6. Seguimiento y revisión periódica

11. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política de alto nivel o política general de seguridad y privacidad de información de la Fábrica de Licores del Tolima, establece su compromiso hacia la Seguridad y Privacidad de la Información. El responsable de la revisión de la misma será la alta gerencia y contará con revisión de esta anualmente y se la actualizará en caso de considerarlo necesario creando un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades de operación, gestión y administración de la seguridad de la información, así como la creación del Comité y el Administrador de Seguridad de la Información. Estableciendo roles, funciones y responsabilidades de operación y administración de los sistemas de información de la entidad debidamente documentadas y divulgadas.

12. SEGUIMIENTO A RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

A cargo de la oficina de Control interno de manera periódica. Cada líder de proceso tendrá la responsabilidad de establecer los controles necesarios para evitar su materialización.

13. ACTIVIDADES DEFINIDAS EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA VIGENCIA DE 2026.

No.	ACTIVIDAD	FECHA
1.	Gobierno y Planeación de la Seguridad de la Información • Actualizar y aprobar el **Plan de Seguridad y Privacidad de la Información** • Formalizar los **roles y responsabilidades** en seguridad y privacidad de la información (líder MSPI, TI, responsables de procesos). • Socializar el PSPI a funcionarios, contratistas y terceros con acceso a información institucional.	Febrero 2026
2.	Gestión de Activos de Información • Identificar, actualizar y mantener el **Inventario de Activos de Información** • Clasificar los activos de información según su nivel de:	Marzo 2026

	Confidencialidad – Integridad - Disponibilidad	
3.	Gestión de Riesgos de Seguridad de la Información (MSPI) • Identificar amenazas y vulnerabilidades asociadas a los activos de información críticos. • Valorar los riesgos de seguridad de la información (impacto y probabilidad).	Abril 2026
4.	Gestión de Incidentes de Seguridad de la Información • Implementar y socializar el **Procedimiento de Gestión de Incidentes de Seguridad de la Información**.	Abril 2026

No.	ACTIVIDAD	FECHA
	Controles de Seguridad de la Información • Implementar controles de **control de accesos** a sistemas de información (usuarios, roles, perfiles). • Fortalecer los mecanismos de **respaldo y recuperación de la información** • Aplicar controles de seguridad en: Servidores – Redes - Aplicaciones - Equipos de usuario final	Mayo 2026
	Protección de Datos Personales y Privacidad • Actualizar y publicar la **Política de Tratamiento de Datos Personales**.	Mayo 2026
	Continuidad y Disponibilidad de la Información • . Definir y mantener el **Plan de Continuidad de los Servicios de TI**. • Realizar pruebas de restauración de respaldos de información crítica	Junio 2026
	Sensibilización y Cultura de Seguridad • Capacitar a funcionarios y contratistas en: Seguridad de la información - Protección de datos personales - Buenas prácticas digitales • Realizar campañas de sensibilización sobre riesgos tecnológicos (phishing, uso de contraseñas).	Permanente

CONTROL DE CAMBIOS				
Versión	**Fecha**	**Elaboró**	**Reviso/Aprobó**	**Comentarios**
00	29/01/2026	Subgerente Administrativa/Contratista Calidad	Comité de gestión y desempeño	Creación del documento