TABLA DE CONTENIDO

1. OBJETIVO.

Definir, priorizar e implementar las acciones de tratamiento necesarias para mitigar, controlar, aceptar o transferir los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información de la Fábrica de Licores del Tolima, garantizando el cumplimiento de los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) vigentes a 2026, la normativa legal aplicable y las políticas institucionales, con el fin de proteger los activos de información, asegurar la continuidad de los procesos misionales y fortalecer la confianza de ciudadanos, funcionarios, contratistas y terceros.

2. ALCANCE

Este Plan aplica a: Todos los activos de información de la Fábrica de Licores del Tolima, incluyendo información física y digital, bases de datos, aplicaciones, infraestructura tecnológica, servicios en la nube y activos asociados. - Todos los procesos institucionales: misionales, estratégicos, de apoyo y de evaluación. - Todos los funcionarios, contratistas y terceros que tengan acceso, gestionen o administren información institucional. - Sistemas de información, redes, equipos de cómputo, dispositivos de almacenamiento y servicios tecnológicos utilizados para el tratamiento de la información. - Los riesgos de seguridad de la información y de protección de datos personales identificados en el marco del Modelo de Seguridad y Privacidad de la Información (MSPI), alineados con la Política de Gobierno Digital.

3. POLITICA DE GOBIERNO DIGITAL

La Política de Gobierno Digital, en estrecha colaboración con la de Seguridad Digital, constituye la estrategia del Gobierno Nacional para la transformación digital del sector público, buscando fortalecer la relación Ciudadano - Estado mediante la mejora y la generación de confianza a través del uso y aprovechamiento seguro de las TIC,

integrándose al Modelo Integrado de Planeación y Gestión (MIPG) y a las políticas de Gestión y Desempeño Institucional para impulsar una administración pública eficiente, transparente, participativa y enfocada en la creación de valor público dentro de un entorno digital confiable.

La salvaguarda de los activos digitales y la integridad de la información de la Fábrica de Licores del Tolima constituyen un pilar fundamental para asegurar la continuidad de sus operaciones y el cumplimiento efectivo de su misión institucional.
En este sentido, la presente Política de Seguridad Digital establece que todos los empleados que, en el ejercicio de sus funciones, hagan uso de los recursos tecnológicos proporcionados por la entidad, asumen la ineludible responsabilidad de adherirse y cumplir cabalmente con las directrices y normativas para su uso aceptable.

Esta obligación se fundamenta en la comprensión de que cualquier utilización inapropiada, negligente o malintencionada de los sistemas informáticos, la infraestructura de red, el software, los datos y demás recursos tecnológicos, puede generar vulnerabilidades significativas que pongan en grave riesgo la operatividad ininterrumpida de los servicios esenciales para la producción, distribución y comercialización de nuestros productos.

En consecuencia, el incumplimiento de esta política no solo podría derivar en interrupciones en la cadena de valor y afectar la eficiencia de la gestión, sino que también podría comprometer la confidencialidad, integridad y disponibilidad de la información crítica, exponiendo a la Fábrica a potenciales pérdidas económicas, daños reputacionales y el incumplimiento de las regulaciones vigentes.

Por lo tanto, la observancia estricta de esta política es un deber inherente a la labor de cada individuo vinculado a la entidad, contribuyendo de manera activa a la creación y mantenimiento de un entorno digital seguro y confiable que respalde los objetivos estratégicos de la Fábrica de Licores del Tolima.

4. ALINEACIONES INSTITUCIONALES Y NORMATIVAS

Este Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se construye bajo un enfoque integral de alineación institucional y normativa, garantizando coherencia entre la estrategia, la operación y el control. En este sentido, el plan se articula con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), especialmente el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de Gobierno Digital, con el Modelo Integrado de Planeación y Gestión (MIPG), el Sistema de Control Interno y el Plan Estratégico de Tecnologías de la Información (PETI). Esta alineación permite que la gestión de los riesgos de seguridad y privacidad de la información no sea un ejercicio aislado, sino

un componente transversal que apoya el cumplimiento de los objetivos institucionales, fortalece la administración del riesgo, optimiza la toma de decisiones, prioriza inversiones en seguridad digital y contribuye a la mejora continua, la transparencia y la continuidad de los servicios tecnológicos y misionales de la Fábrica de Licores del Tolima.

4.1. Alineación con los directrices de MINTIC

El plan se fundamenta en:

- Política de Gobierno Digital.
- Modelo de Seguridad y Privacidad de la Información (MSPI).
- Guías de Gestión del Riesgo de Seguridad Digital emitidas por MinTIC.

El tratamiento de riesgos se orienta a la implementación progresiva de controles administrativos, técnicos y físicos, priorizados de acuerdo con el nivel de riesgo y el impacto institucional.

4.2. Alineación con MIPG

El Plan de Tratamiento de Riesgos contribuye directamente a:

- **Dimensión 7 – Control Interno:** fortaleciendo la gestión del riesgo y las actividades de control.

- **Dimensión 6 – Gestión del Conocimiento y la Innovación:** promoviendo buenas prácticas en seguridad de la información.

4.3. Articulación con el Sistema de Control Interno

El tratamiento de riesgos de seguridad y privacidad de la información fortalece los siguientes componentes del Sistema de Control Interno:

- Identificación, análisis y valoración de riesgos.
- Definición e implementación de actividades de control.
- Generación de información confiable para la toma de decisiones.
- Seguimiento y evaluación permanente de la eficacia de los controles.

Este plan se constituye en un insumo para los ejercicios de autoevaluación, auditoría interna y mejora continua.

4.4 Articulación con el PETI

El presente plan se integra al PETI como un instrumento operativo que:

- Prioriza inversiones en seguridad de la información y ciberseguridad.
- Orienta la adquisición de soluciones tecnológicas seguras.
- Reduce riesgos tecnológicos que puedan afectar la continuidad de los servicios digitales.

5. TERMINOS Y DEFINICIONES

Activo de Información: Elemento que tiene valor para la Fábrica de Licores del Tolima y que contiene, procesa o soporta información, tales como datos, documentos, aplicaciones, infraestructura tecnológica, servicios y personas.

Riesgo de Seguridad de la Información: Posibilidad de que una amenaza explote una vulnerabilidad y genere un impacto negativo sobre la confidencialidad, integridad o disponibilidad de la información institucional.

Riesgo de Privacidad de la Información: Probabilidad de que se afecten los derechos de los titulares de los datos personales como consecuencia de un tratamiento inadecuado, no autorizado o inseguro de la información personal.

Tratamiento del Riesgo: Proceso de selección e implementación de medidas para modificar el nivel de riesgo, incluyendo acciones de mitigación, aceptación, transferencia o eliminación del riesgo.

Amenaza: Causa potencial de un incidente no deseado que puede generar daño a un activo de información.

Vulnerabilidad: Debilidad en un activo, proceso o control que puede ser explotada por una amenaza.

Control de Seguridad: Medida administrativa, técnica o física implementada para reducir la probabilidad o el impacto de un riesgo de seguridad o privacidad de la información.

Datos Personales: Cualquier información vinculada o que pueda asociarse a una persona natural determinada o determinable, de conformidad con la Ley 1581 de 2012.

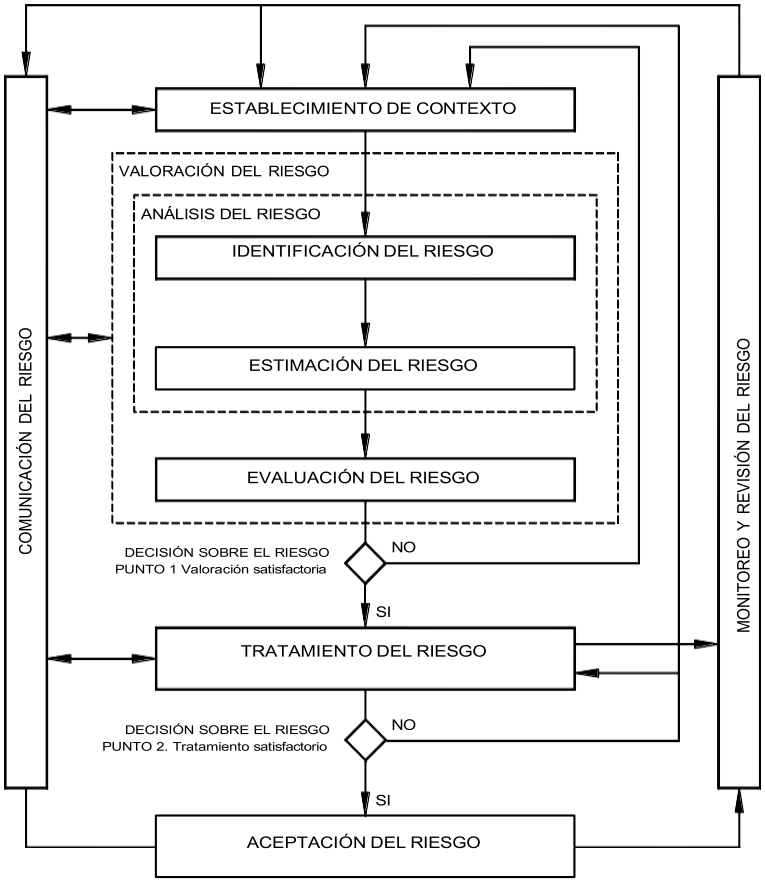
Incidente de Seguridad de la Información: Evento que compromete o puede

comprometer la confidencialidad, integridad, disponibilidad o privacidad de la información institucional.

Modelo de Seguridad y Privacidad de la Información (MSPI): Marco definido por MinTIC que establece los lineamientos para gestionar la seguridad y privacidad de la información en las entidades públicas, como parte de la Política de Gobierno Digital.

6. VISION GENERAL DEL PROCESO DE GESTION DE RIESGO EN LA SEGURIDAD DE LA INFORMACION

A continuación, se presenta el modelo de gestión de riesgos de seguridad de la información diseñada basada en la norma ISO/IEC 31000 y la metodología del Departamento Administrativo de la Función Pública, para la adecuada administración de riesgos en la seguridad de la información; los elementos que lo componen son:



La gestión de riesgos de seguridad de la información deberá ser iterativa para las actividades de valoración de riesgos y/o tratamiento de estos.

ROLES Y RESPONSABILIDADES.

GERENCIA: Definir, revisar la política de administración del riesgo e incluir los riesgos de seguridad y privacidad de la información.

LIDERES DE PROCESO: Apoyar y aportar de manera permanente en la implementación y consolidación de los riesgos de seguridad y privacidad de la entidad.

JEFE OFICIA DE CONTROL INTERNO: Realizar seguimiento al mapa de riesgo institucional

7. DEFINICION DEL CONTEXTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Se toma como referencia para definir los riesgos de seguridad y privacidad de la información de esta entidad, tomando como referencia el Modelo de Seguridad y Privacidad de la información de MINTIC, la gestión de riesgos de seguridad y privacidad de la información, la Norma Técnica Colombiana ISO/EC 31000, ISO 27005, Metodología Propuesta por el Departamento Administrativo de la Función Pública y el procedimiento interno de administración del riesgo definido en la entidad.

Como criterios para la gestión de riesgos de seguridad de la información se establecen:

i. Criterios de evaluación del riesgo de seguridad de la información:

La evaluación de los riesgos de seguridad de la información se enfocará en:

a. El valor estratégico del proceso de información.
b. La criticidad de los activos de información involucrados.
c. Los requisitos legales y reglamentarios, así como la obligaciones contractuales.

ii. Criterios de Impacto

Los criterios de impacto se especificarán en términos del grado, daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando aspectos tales como:

d. Nivel de clasificación de los activos de información impactados
e. Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
f. Operaciones deterioradas (afectación a partes internas o terceras partes)
g. Pérdida del negocio y del valor financiero
h. Alteración de planes o fechas límites
i. Daños en la reputación
j. Incumplimiento de los requisitos legales, reglamentarios o contractuales

NIVEL	CONCEPTO	DESCRIPCIÓN	SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
1	**Muy Bajo**	Si el hecho llegara a presentarse tendría consecuencias o efectos mínimos sobre la organización	Afecta a una actividad del proceso.
2	**Bajo**	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la organización.	Afecta a un grupo de trabajo, a una persona, grupo de personas o algunas actividades del proceso.
3	**Moderado**	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la organización.	Afecta un conjunto de datos personales o el proceso.
4	**Alto**	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la organización.	Afecta varios conjuntos de datos personales o procesos de la organización.
5	**Muy Alto**	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la organización.	Afecta toda la organización. Multas por incumplimiento de la Legislación. Suspensión de las actividades misionales de la organización.

iii. Criterios de Aceptación

Los criterios de aceptación dependerán con frecuencia de las políticas, metas, objetivos de la entidad y de las partes interesadas, por tanto, las escalas de aceptación de riesgos de seguridad de información se podrán tomar del

procedimiento de administración del riesgo.

8. VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACION

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Valor Asignado	Acción Requerida
Riesgo Extremo	**Mayor o igual a 16**	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad, reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa o compartir y/o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	**Mayor que 12 y menor a 16**	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado o compartir y/o transferir el riesgo.
Riesgo Moderado	**Mayor que 4 y menor o igual 11**	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor o compartir el riesgo.
Riesgo Bajo	**Menor o igual a 3**	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectadas y preventivas.

Los riesgos se deberán identificar, describir cuantitativamente o cualitativamente y priorizarse frente a los criterios de evaluación del riesgo y los objetivos relevantes, esta fase consta de las siguientes etapas:

La valoración del Riesgo de seguridad de la información consta de las siguientes actividades:

- Análisis del riesgo
- Identificación de los riesgos
- Estimación del riesgo
- Evaluación del riesgo

i. Identificación del riesgo

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación.

Los **activos de información** se clasifican en dos tipos:

a) **Primarios**:

a. Procesos o subprocesos y actividades del Negocio: procesos cuya

pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

b. **Información**: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

c. **Actividades y procesos de negocio**: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b) **De Soporte**

a. **Hardware**: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).

b. **Software**: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)

c. **Redes**: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información (conmutadores, cableado, puntos de acceso, etc.)

d. **Personal**: Consiste en todos los grupos de personas involucradas en el sistema de información (usuarios, desarrolladores, responsables, etc.)

e. **Sitio**: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)

f. **Estructura organizativa**: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las **amenazas** que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las **vulnerabilidades** que podrían aprovechar las amenazas y causar daños a los activos de información. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Para cada una de las **amenazas** analizaremos las **vulnerabilidades** (debilidades) que podrían ser explotadas.

Finalmente se identificarán las **consecuencias**, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

g) **Estimación del riesgo**

La estimación del riesgo busca establecer la *probabilidad* de ocurrencia de los riesgos y el *impacto* de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y

priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad**: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.

Dimensión del Riesgo de Seguridad y Privacidad de la Información	Valor Asignado	Acción Requerida
Riesgo Extremo	**Mayor o igual a 16**	Evitar el riesgo empleando controles que busquen reducir el nivel de probabilidad, reducir el riesgo empleando controles orientados a minimizar el impacto si el riesgo se materializa o compartir y/o transferir el riesgo mediante la ejecución de pólizas.
Riesgo Alto	**Mayor que 12 y menor a 16**	Evitar o mitigar el riesgo mediante medidas adecuadas y aprobadas, que permitan llevarlo a la zona de riesgo moderado o compartir y/o transferir el riesgo.
Riesgo Moderado	**Mayor que 4 y menor o igual 11**	Evitar o mitigar el riesgo mediante medidas prontas y adecuadas que permitan llevarlo a la zona de riesgo menor o compartir el riesgo.
Riesgo Bajo	**Menor o igual a 3**	Asumir el riesgo. Mitigar el riesgo con actividades propias del proceso y por medio de acciones detectivas y preventivas.

- **Impacto**: Hace referencia a las consecuencias que puede ocasionar a la Entidad la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

Formulario para el registro de la estimación de los riesgos de seguridad de la información:

Para realizar el análisis de riesgo de un proceso, se utilizará la metodología propuesta por el Departamento Administrativo de la Función Pública.

TRATAMIENTO Y SEGUIMIENTO A RIESGOS.

Esta actividad estará a cargo de la Oficina de Control Interno a través de los seguimientos cuatrimestrales con los líderes de las diferentes dependencias. Un aspecto de gran importancia, realizando seguimiento a las acciones propuesta a fin de evitar la materialización de los riesgos identificados.

CRONOGRAMA VALORACION DE RIESGOS DE SEGURIDAD DE LA INFORMACION

La Entidad presentará un cronograma de actividades para la realización de la valoración de los riesgos de seguridad de la información en los procesos de la organización al comité institucional de Gestión y Desempeño, basado con su criticidad y su valor para el cumplimiento en el objeto de la misionalidad de la entidad. Este cronograma estará ajustado al cronograma de actualización de los riesgos de la institución.

CRONOGRAMA PARA EL DESARROLLO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION												
Id Fase	Nombre Fase	2026										
		Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	Planeación y diagnósticoPlaneación y diagnóstico: - Revisión del contexto institucional, normativo y estratégico. - Actualización del inventario de activos de información. - Identificación y valoración de riesgos de seguridad y privacidad de la información. - Definición de roles y responsabilidades.											

CRONOGRAMA PARA EL DESARROLLO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Id Fase	Nombre Fase	2026										
		Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
2	Definición del tratamiento del riesgo: - Priorización de riesgos según impacto y probabilidad. - Definición de estrategias de tratamiento (mitigar, aceptar, transferir o evitar). - Formulación del plan de acción con responsables, recursos y plazos. - Aprobación del plan por la Alta Dirección.											
3	Implementación de controles: - Implementación de controles administrativos (políticas, procedimientos, acuerdos y capacitación). - Implementación de controles técnicos (seguridad lógica, respaldos, monitoreo y protección perimetral). - Implementación de controles físicos sobre activos críticos. - Articulación de las acciones con proyectos y actividades del PETI.											
4	Sensibilización y fortalecimiento de capacidades: - Jornadas de capacitación y sensibilización en seguridad y privacidad de la información. - Socialización de responsabilidades a funcionarios, contratistas y terceros. - Refuerzo de buenas prácticas de ciberseguridad.											
5	Seguimiento y evaluación: - Verificación de la efectividad de los controles implementados. - Identificación de desviaciones y oportunidades de mejora.											
6	Ajustes y mejora continua: - Actualización del análisis y tratamiento de riesgos. - Ajustes al plan de acción para la siguiente vigencia.											

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