PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025

TABLA DE CONTENIDO

INTRODUCCIÓN

Este documento establece los lineamientos necesarios para la implementación del PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN y de las mejoras dadas a las políticas de seguridad informática y comunicación con lineamientos otorgados por del Departamento de la Función pública en sus estrategias MIPG y GOBIERNO DIGITAL.

Su propósito es garantizar la protección de los activos informáticos mediante el cumplimiento de las políticas de seguridad existentes y la aplicación de mejoras continuas.

2. OBJETIVO GENERAL

Implementar un plan efectivo, que permita gestionar, controlar y minimizar los riesgos de seguridad y privacidad de la información relacionada a los procesos de la industria licorera del cauca.

2.1 OBJETIVOS ESPECÍFICOS:

- Identificar y evaluar los principales activos que requieren protección.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo en la Industria Licorera Del Cauca
- Desarrollar y aplicar mejoras a las políticas de seguridad informática y comunicación vigentes en la ILCAUCA.
- Definir estándares de protección y monitoreo a cada tipo de riesgo y de información.
- Garantizar el cumplimiento de las normativas vigentes en Ciberseguridad y protección de datos.

3. MARCO LEGAL

- **Ley 1266 de 2008**: Régimen de Habeas Data.
- **Ley 1581 de 2012**: Protección de Datos Personales.
- **Decreto 1078 de 2015**: Decreto Único Reglamentario del Sector TIC, actualizado con modificaciones relevantes hasta 2024.
- **Ley 1928 de 2018**: Fortalecimiento de la Ciberseguridad y Ciberdefensa Nacional.
- **Resolución 1742 de 2022**: Lineamientos actualizados para la gestión de la seguridad de la información.
- **ISO/IEC 27001:2022**: Estándar internacional para la implementación de sistemas de gestión de seguridad de la información.

- **ISO/IEC 27005:2022**: Estándar para la gestión de riesgos de seguridad de la información.

4. TERMINOS Y DEFINICIONES:

- **Riesgo:** Posibilidad de ocurrencia del evento que tiene un efecto positivo o negativo sobre el producto o servicio generado de un proceso o el cumplimiento de los objetivos institucionales.
- **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 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.
- **Riesgo Positivo:** Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.
- **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. RESPONSABLES

- **Empleados y contratistas:** Todos los usuarios que acceden, procesan o almacenan información sensible.
- **Oficina de gestión tecnológica y Sistemas:** Infraestructura tecnológica, aplicaciones de software, y equipos físicos utilizados en la organización.
- **Información y datos:** Todos los tipos de datos, incluyendo datos personales y corporativos, manejados por la Industria Licorera del Cauca.
- **Procesos y operaciones:** Todas las actividades y procedimientos que involucren el uso de información y sistemas tecnológicos.

6. RECURSOS:

Humano: Gerente, Líderes de Proceso o área, líder de proceso de planeación, equipo que integra área de Gestión Tecnológica.
Físico: Infraestructura Tecnológica de la Industria Licorera Del Cauca.

7. POLÍTICAS ACTUALES DE LA INDUSTRIA LICORERA DEL CAUCA

7.1 POLÍTICA DE COMUNICACIÓN

La Industria Licorera del Cauca, una empresa de los caucanos, con el compromiso de garantizar una comunicación efectiva y fluida externa e interna para los usuarios, establece que el grupo interno de trabajo en el proceso de gestión tecnológica y de la información será el encargado de apoyar técnicamente las necesidades de la organización en materia de información que se desarrolle a través de los diferentes canales (Pagina WEB, Redes Sociales, Boletín Interno de Comunicaciones, Correos electrónicos, radio y televisión).

En tal sentido, a partir de la resolución número 10539 de 2016, por la cual se adopta el software Sevenet y mediante la resolución 1006 del 2022 donde se continúa y fortalece dicho proceso. El proceso de gestión tecnológica y de la información coordinará la puesta en marcha las estrategias de comunicación interna y externa de acuerdo a las instrucciones recibidas por la alta gerencia, teniendo en cuenta la adquisición de éste software para facilitar la gestión de la información.

7.2 POLÍTICA SEGURIDAD INFORMÁTICA

La definición de políticas de seguridad informática busca establecer en la Industria Licorera del Cauca una cultura de buenas prácticas que salvaguarden la seguridad de la información, sistemas de información y recursos tecnológicos de la empresa. La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de Industria Licorera del Cauca en materia de seguridad.

Las políticas de seguridad informática establecen normas, reglas, procedimientos y controles que regulan la forma como la Industria Licorera del Cauca prevenga y maneje los riesgos de seguridad en diferentes circunstancias, el personal que utilice los servicios de la infraestructura tecnológica de la empresa deberá conocer y aceptar las políticas actuales sobre su uso, el desconocimiento de las mismas no exonera de responsabilidad al usuario ante cualquier eventualidad que involucre la seguridad de la información o de la red de la empresa.

7.3 ACCIONES DE MEJORAS IMPLEMENTADAS A LAS POLITICAS DE LA INDUSTRIA LICORERA DEL CAUCA.

Acerca de los riesgos identificados actualmente sin una herramienta de autodiagnóstico precisa, se crea un plan de acciones de mejora con el fin de proteger y preservar los recursos electrónicos, informáticos y equipos de cómputo el cual incluye:

- Crear una circular de uso adecuado y aceptable en el que se informa a los funcionarios de la ILCAUCA de lo que pueden y no pueden hacer en los equipos de la empresa.
- Concientización a los funcionarios proactivamente a través de comunicaciones periódicas y las actualizaciones en las políticas.

Así mismo y teniendo en cuenta la importancia que representa el uso adecuado de los activos informáticos instalados en la ILCAUCA, se indican a continuación normas pertinentes con el objetivo de que cada funcionario se comprometa a dar un uso adecuado a los mismos, siendo consciente del riesgo en que incurre la entidad al incumplirlas.

RECOMENDACIONES FRENTE AL USO DE EQUIPOS Y POLITICAS DE LA INDUSTRIA LICORERA DEL CAUCA 2023 -2026		
POLITICA DE SEGURIDAD INFORMATICA Y COMUNICACIÓN		
REFERENTE A:	**RIESGO**	**DESCRIPCION**
USUARIOS Y CLAVES DE ACCESO	Suplantación de identidad que podría llevar al acceso irresponsable a los sistemas informáticos y sustraer todo tipo de información, o bien utilizar esta entrada para modificar o incluso eliminar archivos, con las consecuencias económicas, de responsabilidad jurídica y pérdidas de imagen que ello supondría.	1. La Identificación de usuario y la contraseña debe ser confidencial e intransferible.
		2. cuando se ingrese al sistema de Información (sevenet-apoteosys-siaobserba-secop), no se debe dejar desatendida la pantalla evitando el uso del equipo por otras personas con su identificación de usuario.
		3. Todos los equipos que no se estén utilizando deben estar en modo ingreso o apagados.
		4. Las contraseñas se deben cambiar al menos cada 60 días.
		5. El acceso a los sistemas efectuado por contratistas, y otras personas no vinculadas directamente a la ILCAUCA, debe ser estrictamente limitado a que realice sus proyectos asignados, donde es responsabilidad del Jefe Inmediato informar oportunamente y por escrito a gestión tecnológica sobre la labor a realizar y la necesidad de asignación del usuario.
		6. Cuando el contratista traiga equipos propios, la ILCAUCA no se hará responsable por la autenticidad y legalidad de los programas que tenga instalados en los mismos. No se le dará acceso a la red, para esto deberá trabajar en un equipo asignado por gestión tecnológica
		7. En el evento excepcional que un usuario requiera dar a conocer su contraseña a otra persona de manera temporal, deberá documentar oportunamente este hecho enviando copia a gestión tecnológica.
SOFTWARE Y EQUPOS INFECTADOS	Infección de los equipos por virus que pueden llegar a afectar los activos informáticos de forma lógica (software) o física (hardware)	1.Los programas instalados y configurados por gestión tecnológica en los equipos de cómputo son para el uso de los usuarios de la ILCAUCA por tal motivo no está permitido instalar ni desinstalar ningún aplicativo de dichos equipos, ni cambiar parcial o totalmente su configuración
		2. nunca utilizar programas copiados u obtenidos libremente a través de internet, y tampoco copias ilegales de programas o de origen desconocido. Usar únicamente programas originales autorizados por la ILCAUCA.
		3. No usar software enviado por proveedores con fines de evaluación sin consultar con gestión tecnológica de la ILCAUCA y sin estar seguro de su procedencia.

RECOMENDACIONES FRENTE AL USO DE EQUIPOS Y POLITICAS DE LA INDUSTRIA LICORERA DEL CAUCA 2023 -2026		
POLITICA DE SEGURIDAD INFORMATICA Y COMUNICACIÓN		
REFERENTE A:	**RIESGO**	**DESCRIPCION**
		4. No copiar CD`S de programas u otro medio magnético de la ILCAUCA sin la debida aprobación de gestión tecnológica.
		5. Los medios magnéticos ajenos a la ILCAUCA y que se requieran para el trabajo deben ser examinados antes de ser utilizados en algún pc, para asegurar que no tengan virus y sean datos compatibles con los equipos.
		6.Si un Virus es detectado debe inmediatamente prohibirse el uso del equipo, documentar la ocurrencia por escrito e informar a área de gestión tecnológica
		7. no se deben cambiar las configuraciones de los protectores de pantalla, papel tapiz y demás elementos configurables de los equipos. Lo anterior debido a los continuos bloqueos y con el fin de mejorar la productividad y velocidad de los equipos de cómputo.
		8. no descargar copias ilegales de software pirata para uso personal o entidades diferentes a la ILCAUCA.
		9. la asignación de equipos de cómputo para el personal de transito temporal como contratistas, pasantes están sujetas a disponibilidad del recurso en el área de gestión tecnológica.
		10. las asignaciones de usuarios y contraseñas de los diferentes servidores están sujetas a disponibilidad de recurso.
		11. los usuarios están en la obligación de brindar la colaboración necesaria para que el área de gestión tecnológica puedan realizar labores proactivas al software, hardware, mantenimientos preventivos y o correctivos.
		12. aquella información que sea considerada confidencial, se recomienda su protección con contraseñas de seguridad.
		13. Ninguna de las partes del activo debe ser modificada ni para quitar, ni para agregar partes, por personal ajeno a gestión tecnológica.
DISPOSITIVOS DE ENTRADA Y SALIDA DE LOS ACTIVOS INFORMATICOS	Deterioro del hardware	1.Todo equipo o dispositivo electrónico conectado a los activos informáticos de la ILCAUCA, como Cámaras Digitales, Webcam, Parlantes, Micrófonos, impresoras, Scanner, Lectores, Tarjetas, etc., debe estar debidamente autorizado por GESTION TECNOLOGICA, quienes analizaran entre otras características la compatibilidad, capacidad del equipo para tener determinado equipo conectado, configuración y así poder lograr la Interoperabilidad de los dispositivos conectados.
		2. no se debe ingerir alimentos, ni bebidas cerca de los equipos de cómputo con el fin de evitar daños.
		3. Los equipos deben estar ubicados teniendo en cuenta características de ergonomía, energía y cableado entre otras y cualquier movimiento de los equipos debe ser solicitado y realizados por gestión tecnológica de la ILCAUCA.
		5. cada oficina está dotada de puntos de red, puntos de voz, corriente regulada, tomas de corriente, y algún cambio a alguno de estos debe ser realizado y autorizado por el área de gestión tecnológica.
		6. los equipos de la ILCAUCA deben ser utilizados estrictamente para la ejecución de labores propias a la ILCAUCA, salvo autorización expresa de quien corresponda.
		8. se prohíbe modificar los privilegios de acceso a las redes internas o externas para obtener acceso no autorizado a dichos recursos.

RECOMENDACIONES FRENTE AL USO DE EQUIPOS Y POLITICAS DE LA INDUSTRIA LICORERA DEL CAUCA 2023 -2026		
POLITICA DE SEGURIDAD INFORMATICA Y COMUNICACIÓN		
REFERENTE A:	**RIESGO**	**DESCRIPCION**
		9.se prohíbe la modificación de los parámetros o configuración de los equipos de la ILCAUCA para darle capacidad de recibir llamadas o accesos remotos que permita intromisiones no autorizadas a la red de la ILCAUCA
USO DE CORREO ELECTRONICO	La Confidencialidad es un riesgo asociado al envío de correo electrónico. El mensaje de correo electrónico pasa a través de numerosos sistemas antes de llegar al destinatario. Si el mensaje no está cifrado, cualquier pirata informático podría hacerse con él y leerlo en cualquier punto de la ruta de entrega e inundación de correo masivo (spam)	1. El uso de correo electrónico debe ser utilizado solo con fines laborales
		2. No reenviar cadenas de correo electrónico
		3. No utilizar el correo como medio de distribución de publicidad
		4. El usuario es responsable por el uso de su cuenta y no debe permitirle a nadie más que tenga acceso al servicio a través de su cuenta. Se Deberá notificar inmediatamente a gestión tecnológica cualquier uso no autorizado de su contraseña o cuenta o de cualquier otra falla de seguridad.
		5. El usuario entiende que Internet contiene material sin editar, algunos de los cuales son sexualmente explícitos o pudieran ser ofensivos. Gestión tecnológica no tiene control sobre este material y no acepta responsabilidad por ello. Por lo tan to, es probable que el usuario reciba dichos materiales, más su divulgación y/o distribución a otros a través de su cuenta no es permitida.
		6. Sistemas de información no se hace responsable por la contaminación con virus adquiridos a través del correo electrónico.
		7. Gestión tecnológica bloqueara y prohíbe la descarga de archivos con las siguientes extensiones pps, mp3
		8. Se prohíbe el envío a otras personas de copia de un mensaje de correspondencia electrónica recibido sin el conocimiento o consentimiento del remitente original.
		9. Se prohíbe leer, revisar, o interceptar cualquier tipo de comunicación electrónica de la ILCAUCA o de cualquier otra persona o entidad, sin el consentimiento expreso del remitente y del destinatario de correo
		10. El correo debe ser revisado a diario pues los comunicados emitidos y recibidos tienen carácter oficial.
		11. Se prohíbe el envío fuera de la ILCAUCA de documentos electrónicos o mensajes por medio e-mail que contengan información confidencial.
		12. Se prohíbe el envío o recepción de mensajes de correo electrónico o de cualquier tipo entre personal de la ILCAUCA y personas que no pertenezcan a la misma
NAVEGACION E INTERNET	El robo de contraseñas, la suplantación de identidad y el uso fraudulento de las tarjetas de crédito son problemas que	1. La información contenida en los activos, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica (e-mail) información de internet, los documentos y programas existentes no podrán reproducirse o utilizarse para fines ajenos a las funciones y poderes de la ILCAUCA.
		2. se prohíbe el uso de los sistemas y comunicaciones de la ILCAUCA para propósitos personales, de recreo para manejo de un negocio o asunto privado del usuario o para envío de mensajes en cadenas.

RECOMENDACIONES FRENTE AL USO DE EQUIPOS Y POLITICAS DE LA INDUSTRIA LICORERA DEL CAUCA 2023 -2026		
POLITICA DE SEGURIDAD INFORMATICA Y COMUNICACIÓN		
REFERENTE A:	**RIESGO**	**DESCRIPCION**
	nos pueden estar acechando en el próximo sitio web, Phishing, Virus.	3. Los usuarios no tienen permiso para utilizar los recursos electrónicos de la ILCAUCA para hacer compras, jugar, participar en encuestas o concursos o cualquier otro servicio ajeno a las funciones de la ILCAUCA.
		4. se prohíbe acceder a, o utilizar propiedad intelectual (copyright información) que viole los derechos de autor.

8. METODOLOGIA DE LA IMPLEMENTACION DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información en adelante **(MSPI)** en la ILCAUCA, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

9. ACTIVIDADES A REALIZAR EN EL PLAN

- Realizar diagnóstico, levantamiento de información sobre aspectos de vulnerabilidad.
- Elaborar el alcance del plan del tratamiento de riesgos de seguridad y privacidad de la información.
- Realizar la identificación de los riesgos con los líderes del proceso.
- Valoración del riesgo y del riesgo residual.
- Realizar de mapas de calor donde se ubican los riesgos.
- Plantear plan de tratamiento de riesgos aprobado por los líderes de la ILCAUCA.
- Realizar actividades de sensibilización, inducción, reinducción al personal frente a las mejoras propuestas a las políticas de la ILCAUCA.

10. CUMPLIMIENTO DE IMPLEMENTACION

De acuerdo con las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo con lo establecido por la ILCAUCA.

- Revisión y/o modificación de la Política de Seguridad actual de la ILCAUCA.
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

11. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA IFORMACION.

El presente plan está diseñado para cumplir la fase de determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de La Industria Licorera del Cauca. Para realizar este paso los responsables del plan deben efectuar la recolección de la información con la ayuda de la guía de autoevaluación, guía de encuesta y guía metodológica de las pruebas de efectividad del modelo MSPI estrategia de MINTIC.

MARIBEL PERFAN GALLARDO
GERENTE

Elaborado por: Ivon Lucia Sarria Mosquera – Jefe División de Planeación.

12. CRONOGRANA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA INDUSTRIA LICORERA DEL CAUCA DEL AÑO 2025.

CRONOGRANA DE ACTIVIDADES PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE LA INDUSTRIA LICORERA DEL CAUCA																																				
FASE	ACTIVIDAD		ABRIL				MAYO				JUNIO				JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
	#	ACTIVIDAD POR SEMANA	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	1	Determinar las amenazas y vulnerabilidades existentes.																																				
	2	Evaluar el estado actual de seguridad y privacidad.																																				
	3	Proporcionar capacitación sobre seguridad y privacidad.																																				
2	4	Identificar controles existentes y su efectividad.																																				
	5	Identificar controles adicionales necesarios.																																				
3	6	Crear nuevos controles o mejorar los existentes.																																				
	7	Realizar auditorías de seguridad periódicas.																																				
	8	Seguimiento y control																																				

13. SEGUIMIENTO Y EVALUACIÓN

Al finalizar las actividades descritas en el cronograma se realizará una reunión con los responsables, para presentar el informe del avance del plan y de esta manera evaluar todos los pasos se ha ido realizado para lograr la aprobación y publicación del plan definitivo.

14. RESULTADOS

- Informe de avance o resumen ejecutivo de cada etapa.
- Acta de Reunión.
- Plan de tratamiento de riesgo aprobado por los líderes.
- Productos de cada etapa.

ELABORÓ:

_____
JHON JAIME MARTINEZ
TECNICO PROGRAMADOR EN SISTEMAS

REVISÓ:

_____
IVON LUCIA SARRIA MOSQUERA
JEFE DE PLANEACION INDUSTRIA LICORERA DEL CAUCA

APROBÓ:

_____
MARIBEL PERAFAN GALLARDO
GERENTE DE LA INDUSTRIA LICORERA DEL CAUCA.