

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN FÁBRICA DE LICORES DEL TOLIMA

1 OBJETO : Describir las actividades del plan de Seguridad y Privacidad de la Información, con las cuales se busca desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI del Departamento Administrativo de la Fábrica de Licores del Tolima.

2. ALCANCE El alcance del Plan de Seguridad y Privacidad de la Información se aplica a los procesos del Departamento Administrativo de la Fábrica de Licores del Tolima, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información.

3. TERMINOS Y DEFINICIONES

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 convierte 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.

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

1. Administrar los eventos de seguridad de la información de la Fábrica de Licores del Tolima.
2. Fortalecer la seguridad y disponibilidad de la información y plataforma tecnológica acorde con la declaración de aplicabilidad aprobada.
3. Cumplir con los requisitos legales aplicables a la naturaleza de la Entidad en materia de Seguridad de la Información.
4. Fomentar una cultura de seguridad de la información en los servidores públicos (funcionarios, contratistas, pasantes, judicantes y personal en comisión de la Presidencia de la Republica).

5. Fortalecer el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información.

5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

5.1 Roles y Responsabilidades

Alta Gerencia: Será el responsable de liderar la implementación de la Política de Gobierno Digital y la política de seguridad digital en la entidad.

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 la implementación, seguimiento y evaluación de la política de Gobierno Digital y la política de Seguridad Digital en la Fábrica de Licores del Tolima”

La Oficina de Control Interno de Gestión tiene la responsabilidad de hacer 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. La acción disciplinaria en respuesta a las violaciones de las políticas de seguridad de información es responsabilidad de la dirección de Control Interno Disciplinario, actuando conjuntamente con la Subgerencia Administrativa (Talento Humano.)

5.2 Responsabilidades en la Gestión Táctica y operativa de Seguridad Digital

La Fábrica de Licores identificará un análisis de interesados de las claves identificando si son funcionarios, contratistas, asesores, y el grado de influencia en esta. Es obligación de los funcionarios que tengan a cargo o sean responsables de archivos públicos velar por la integridad, autenticidad, veracidad y fidelidad de la información de los documentos de archivo, sean estos físicos o electrónicos, y serán responsables de su organización y conservación, de acuerdo a lo dispuesto en la Ley general de archivos.

6.SEGURIDAD EN EL RECURSO HUMANO Identificadas las condiciones de seguridad de la información , 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 se comprometen formalmente en la protección de información que se les confía, establecerá un acuerdo de buen uso, confidencialidad y no divulgación de la información sensitiva y de la información de carácter personal del ciudadano en procura de la protección y buen manejo de este activo. Con lo anterior, si algún trabajador, funcionario o contratista, deja de prestar sus servicios a la Entidad, o se traslada a otra dependencia asegura el retorno total de la información que gestionó durante el ejercicio de sus funciones, se obliga a no utilizar, comercializar o divulgar los productos o la información generada durante su gestión en la Entidad, por el periodo establecido en la normatividad aprobada de retención documental por la Fábrica de Licores del Tolima.

7. GESTION Y TRATAMIENTO DE RIESGOS.

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

Se incluirán en el mapa de riesgo institucional se identificarán los riesgos referentes a la seguridad y privacidad de la información según metodología del Departamento Administrativo de la Función Pública se contemplará como una de las actividades para este Plan.

7.2 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.

8. 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 con la Seguridad y Privacidad de la información.

Creando un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades 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 los roles, funciones y responsabilidades de operación y administración de los sistemas de información de la entidad a los, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.

9. ACTIVIDADES DEFINIDAS EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA VIGENCIA DE 2019.

- Identificar el marco normativo de seguridad y privacidad de la información.
- Constituir el Comité de Seguridad y Privacidad de la información.
- Revisar adherencia de procedimiento de copias de seguridad y actualizarlo si se considera necesario.
- Definir guía de Gestión de Incidentes Informáticos.
- Actualizar el inventario de Activos de Tecnologías de la Información en lo relacionado a Hardware y Licencias de Software.
- Definir formato para reporte de incidentes informáticos.