

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

1 OBJETO: Describir las actividades del plan de Seguridad y Privacidad de la Información, con las cuales se busca establecer los controles de seguridad bajo el modelo del Sistema de Gestión de Seguridad de la Información describiendo las actividades que se consideran de mayor relevancia para la entidad.

2. ALCANCE: Este plan aplica a los identificados procesos en el Sistema Integrado de Gestión entre ellos misionales, de apoyo y estratégicos.

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 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.

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.

5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

5.1 Roles y Responsabilidades

Para esta entidad

La Fábrica de Licores del Tolima 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.

5.2 Responsabilidades en la Gestión Táctica y operativa de Seguridad Digital

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 DE ACTIVOS

Para esta vigencia se tiene como actividad a desarrollar la identificación de activos de la información, clasificándolos, asignarles responsabilidades dichos activos y brindarles un tratamiento adecuado según dicha clasificación. Lo anterior con la metodología propuesta con MINTIC, y la ISO 27000

8. GESTION Y TRATAMIENTO DE RIESGOS.

8.1 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.

9. 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. Su revisión estará a cargo de la alta gerencia y se hará revisión de esta anualmente y se actualizará si se considera necesario.

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.

10. 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.

11. ACTIVIDADES DEFINIDAS EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA VIGENCIA DE 202.

Mapa de ruta vigencia Plan de Seguridad y Privacidad de la Información. Vigencia 2020

- 1 Elaboración del Manual de política basada en el MSPI (Modelo Seguridad y Privacidad de la Información)
- 2 Actualización de los Activos de Información (Vigencia 2020)
- 3 Diseño del Plan de Recuperación de desastres
- 4 Diseño del Plan anual de concientización de ciberseguridad
- 5 Hacerle seguimiento a los compromisos de FURAG relacionados con Seguridad de la Información
- 6 Implementación del plan de sensibilización de seguridad de la Información del la vigencia 2020
- 7 Identificación de los riesgos asociados a cada uno de los activos de información
- 8 Formular el plan de tratamiento de riesgos
- 9 Identificar cláusulas de seguridad en los contratos
- 10 Verificación de acceso con los logs de auditorías
- 11 Definir acuerdos de confidencialidad



FRANZ LEONARDO MARCELO BEDOYA RUBIO

Gerente General

Proyectaron:

NELKA POSADA SANCHEZ

Jefe Oficina de Control Interno

NORELLY BARRAGAN MENDEZ

Subgerente Administrativa

Ibagué, Enero de 2020