PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

1. OBJETIVO.

Identificar y controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en la entidad con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso y gestión de usuarios, en el marco del Modelo Integrado de Planeación y Gestión.

2. ALCANCE

Este Plan aplica para todos los procesos del Sistema Integrado de Gestión de la Fábrica de Licores del Tolima, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación, esto anterior en el marco de implementación del Modelo integrado de Planeación y Gestión.

3. DEFINICIONES

- **Acceso a la Información Pública**
- Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- **Activo En relación con la seguridad de la información**, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Archivo Conjunto de documentos**, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).
- **Amenazas** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Ciberseguridad** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Control** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Abiertos** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones.

- **Datos Personales** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- **Datos Personales Privados** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- **Datos Personales Mixtos** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

- Declaración de aplicabilidad Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

- **Encargado del Tratamiento de Datos** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)
- **Gestión de incidentes de seguridad de la información** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Evento de seguridad de la información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de Seguridad de la Información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Información Pública Clasificada** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

- **Incidente de seguridad de la información:** Un evento o serie de eventos de Seguridad de la Información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información Pública** Reservada Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Plan de continuidad del negocio** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las

funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Responsabilidad Demostrada** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- **Responsable del Tratamiento de Datos** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **Riesgo** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Seguridad de la información** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

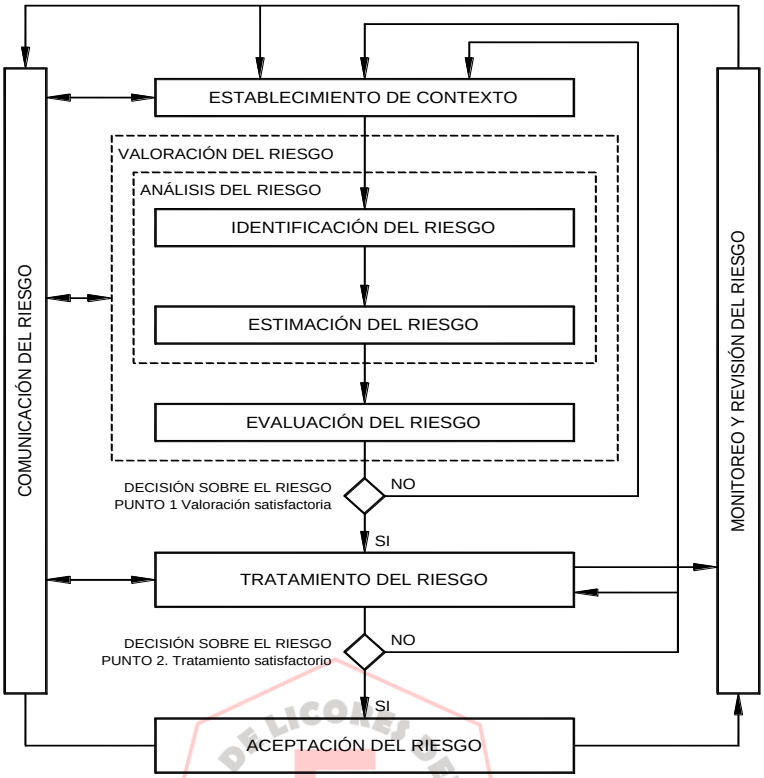
- **Sistema de Gestión de Seguridad de la Información** SGSI Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Titulares de la información** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

- **Trazabilidad** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

4. 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 Y ALTA DIRECCION: 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

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

Se toma como criterio 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:

- El valor estratégico del proceso de información.
- La criticidad de los activos de información involucrados.
- Los requisitos legales y reglamentarios, así como las 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:

- Nivel de clasificación de los activos de información impactados
- Brechas en la seguridad de la información (pérdida de la confidencialidad, integridad y disponibilidad)
- Operaciones deterioradas (afectación a partes internas o terceras partes)
- Pérdida del negocio y del valor financiero
- Alteración de planes o fechas límites
- Daños en la reputación

- 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.

6. 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 detectivas 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.

ii. 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													
IdTarea	Nombre Tarea	2020											
		Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	
0	**DIAGNOSTICO DEL ESTADO DE IMPLEMENTACION DE ISO 27001 / SOCIALIZACION AUTODIGNOSTICO GOBIERNO DIGITAL**												
1	**CONTEXTO DE LA ORGANIZACIÓN**												
1.1	Comprensión De Las Necesidades Y Expectativas De Las Partes Interesadas												
1.2	Determinación del alcance del sistema de gestión de la seguridad de la información												
2	**LIDERAZGO**												
2.1	Revisión de la Política de Seguridad de la Información												
2.2	Roles, Responsabilidades y Autoridades de Seguridad de la Información en la entidad												
2.3	Política de Segregación de Funciones												
2.4	Apoyo e la identificación de contenido de seguridad y protección de la información en Acuerdo de Confidencialidad y Transparencia												
3	**PLANIFICACION**												
3.1	Valoración de riesgos de la seguridad de la información (Modelo de Gestión de Riesgos)												
3.2	Tratamiento de los riesgos de seguridad de la información												
3.3	Diligenciamiento de la declaración de aplicabilidad												
4	**OPERACIÓN**												
4.1	Valoración de Riesgos de seguridad de la información												
4.2	Tratamiento de los riesgos de seguridad de la información del Sistema Integrad de gestión												
6	**EVALUACION DE DESEMPEÑO**												
6.1	Seguimiento, Medición y Evaluación de seguridad de la información												
6.2	Auditoría Interna de seguridad de la Información												
7.	**CONTROLES DE SEGURIDAD DE LA INFORMACION**												
7.1	Contacto con Autoridades y grupos de interes												
7.2	Propuesta seguridad de la información en proyectos												
7.3	Inventario de Activos de Información (procesos del sistema Integrado de gestión)												
7.4	Lineamientos de uso aceptable de Activos de Información												
7.5	Política de control de acceso lógico (usuarios - contraseñas)												
7.6	Procedimiento de custodia de contraseñas de usuarios privilegiados												
8	**SEGURIDAD FISICA**												
8.1	Valoración de la seguridad física y de entorno de las áreas seguras (Centro de datos ANI y de cableados en pisos)												
8.2	Apoyo en el protocolo de seguridad de la sala de evaluación de propuestas												
9	**SEGURIDAD DE LAS COMUNICACIONES**												
9.1	Definición de políticas de acceso seguro y uso adecuado del servicio de internet												
9.2	Política de configuración y aseguramiento de conexión inalámbrica												
10	**INCIDENTES DE SEGURIDAD DE LA INFORMACION**												
10.1	Establecimiento del modelo de gestión de incidentes de seguridad de la información												
10.2	**CONTINUIDAD DE NEGOCIO**												
10.3	Ejecución de actividades para el establecimiento del BIA (Business Impact Analysis de la ANI)												
11	**CUMPLIMIENTO**												
12	Apoyo en la identificación de la legislación aplicable a seguridad y protección de la información (normograma)												
13	Control de instalación de software no autorizado												

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