TABLA DE CONTENIDO

GRAFICAS

TABLAS

La Industria de Licores del Valle (ILV), Empresa Industrial y Comercial del Estado (EICE) se compromete a gestionar adecuadamente los riesgos Estratégicos, Operativos, y de Seguridad Digital e Información, de Seguridad y Salud en el Trabajo, Ambientales, Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo (SARLAFT) y subsistema de administración del riesgo de corrupción, la opacidad y el fraude (SICOF) y todas aquellos que puedan afectar el cumplimiento de los objetivos institucionales, mediante la implementación del modelo de líneas de defensa acatando la metodología propia para su gestión, determinando las acciones de control detectives y preventivas oportunas para evitar la materialización y la actuación correctiva inmediata ante las eventualidades para mitigar las posibles consecuencias a fin de mantener los niveles de riesgo aceptables"

INTRODUCCIÓN.

La estructuración del presente documento para la ILV está basada en la adaptación guía para la administración del riesgo expedida por el DAFP V. 05 vigente y el diseño de controles en entidades públicas y se establece para asegurar el cumplimiento de la misión institucional, los objetivos estratégicos y de proceso.

La política está compuesta por los objetivos, alcance, niveles de aceptación al riesgo, niveles para calificar el impacto, el tratamiento de riesgos, el seguimiento periódico según nivel de riesgo residual y responsabilidad de gestión para cada línea de defensa.

Con el propósito de garantizar un aseguramiento razonable y acorde a las necesidades de la empresa, bajo la filosofía de la mejora continua, fue fundamental la revisión de la política de riesgo establecida en la ILV, para así poder dar cumplimiento de su misión, visión, objetivos estratégicos y de procesos. Declara su política integral de administración del riesgo, acorde con lo establecido por el Modelo Integrado de Planeación y Gestión – MIPG-, el cual incorpora el Modelo Estándar de Control Interno - MECI- a través de la séptima dimensión, en articulación con los Sistemas de Gestión según la normatividad aplicable y con las normas técnicas que se adopten, y de conformidad con lo establecido en el artículo 133 de la Ley 1753 de 2015.

La presente política fue construida con la participación, de la Alta dirección y los lideres de proceso como de quienes lo operativizan.

La política integral de administración de riesgos debe ser una temática conocida por todos los funcionarios de la Entidad, para lo cual se utilizarán los medios de comunicación definidos en el Sistema Integrado de Gestión para su divulgación ante las partes interesadas pertinentes.

PROPÓSITO DEL DOCUMENTO

Establecer el marco general de actuación de todos los servidores públicos de la entidad para la adecuada gestión de los riesgos y los potenciales escenarios de pérdida de continuidad de negocio, mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales, disminuyendo las potenciales consecuencias negativas, reduciendo las vulnerabilidades ante las amenazas internas y externas o mejorando las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la Entidad.

GLOSARIO

Los siguientes son los términos que hacen parte de la NTC ISO 9001:2015

- ***Alta dirección:*** *Persona o grupo de personas que dirige y controla una organización al más alto nivel.*
- ***Compromiso:*** *Participación activa en, y contribución a, las actividades para lograr objetivos compartidos.*
- ***Organización:*** *Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.*
- ***Mejora:*** *Actividad para mejorar el desempeño.*
- ***Gestión:*** *Actividades coordinadas para dirigir y controlar una organización.*
- ***Proceso:*** *Conjunto de actividades mutuamente relacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado previsto.*
- ***Política:*** *Intenciones y dirección de una organización como las expresa formalmente su alta dirección.*
- ***Objetivo:*** *Resultado a lograr.*
- ***Seguimiento:*** *Determinación del estado de un sistema, un proceso, un producto, un servicio, o una actividad.*

Los siguientes son los términos que hacen parte de la NTC ISO 31000:2018

- ***Riesgo:*** *Efecto de la incertidumbre sobre los objetivos.*
- ***Amenazas:*** *situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.*
- ***Gestión del riesgo:*** *Actividades coordinadas para dirigir y controlar la organización con relación al riesgo.*
- ***Consecuencia:*** *Resultado de un evento que afecta a los objetivos.*
- ***Probabilidad:*** *Posibilidad de que algo suceda.*
- ***Control:*** *Medida que mantiene y/o modifica un riesgo.*
- ***Parte interesada:*** *Persona u organización que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.*
- ***Fuente de riesgo:*** *Elemento que, por si solo o en combinación con otros, tiene potencial de generar riesgo.*

Los siguientes son los términos que hacen parte de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, en su versión 5.

- ***Riesgo inherente****: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.*
- ***Riesgo residual:*** *El resultado de aplicar la efectividad de los controles al riesgo inherente.*
- ***Apetito del Riesgo:*** *es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.*
- ***Riesgo de seguridad de la información:*** *Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.*
- ***Riesgo de corrupción:*** *Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.*
- ***Causa:*** *todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.*
- ***Consecuencia:*** *Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.*

- ***Impacto:*** *Las consecuencias que puede ocasionar a la organización la materialización del riesgo.*
- ***Probabilidad:*** *Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de1 año.*
- ***Control:*** *Medida que permite reducir o mitigar un riesgo.*
- ***Causa Inmediata:*** *Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.*
- ***Causa Raíz:*** *Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.*
- ***Factores de riesgo:*** *Son las fuentes generadoras de riesgos.*

Los siguientes son los términos que hacen parte del Plan de Seguridad y Privacidad de la Información.

- ***Activo:*** *Es un recurso que tiene un valor específico para la entidad y debe ser protegido.*
- ***Antivirus:*** *Software diseñado para la detección, prevención y eliminación de programas y archivos maliciosos o dañinos en equipos de cómputo y dispositivos.*
- ***Ciberseguridad:*** *Procedimientos y herramientas que se implementan para proteger la información que se genera a través de equipos de cómputo, servidores, dispositivos móviles, redes y sistemas electrónicos.*
- ***Confidencialidad:*** *Propiedad de la información por la que se garantiza que está accesible únicamente a personal autorizado.*
- ***Control de acceso:*** *Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad.*
- ***Criptografía:*** *El procedimiento de transmitir datos y mensajes cifrados.*
- ***Encriptación:*** *Codificación de los datos para evitar que los usuarios no autorizados los modifiquen. Sólo los usuarios con acceso a una contraseña pueden descifrar y utilizar los datos.*
- ***Hacking Ético:*** *Actividades encaminadas a realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas para evitar daños y alterar los datos.*
- ***MSPI:*** *(Modelo de Seguridad y Privacidad de la información). Actividades, acciones y procesos para proteger el acceso, uso y divulgación del acceso a la información.*

- ***Seguridad de la información:*** *Preservación de la confidencialidad, integridad y disponibilidad de la información.*
- ***SGSI:*** *(Sistema de Gestión de Seguridad de la Información). Procesos y procedimientos para gestionar el acceso a la información encaminados a buscar confidencialidad, integridad y disponibilidad de los activos y minimizando los riesgos.*
- ***Sistema de Información:*** *Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.*
- ***Tecnología de la Información:*** *Se refiere al hardware y software operado por la entidad.*
- ***Vulnerabilidad:*** *Debilidad de un activo o control que puede ser explotado por una o más amenazas.*
- ***Amenaza Externa:*** *Amenaza que se origina fuera de una organización.*
- ***Amenaza Interna:*** *Amenaza que se origina en una organización*
- ***Análisis de Riesgos:*** *Uso sistemático de la información para identificar las fuentes y estimar el riesgo.*
- ***Antispam:*** *Es un producto que sirve como una herramienta o un servicio que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios.*
- ***Automatizar:*** *Hace referencia a la incorporación de herramientas tecnológicas a un proceso o sistema.*
- ***Advertencia:*** *Mensaje que comunica al usuario que una acción puede ocasionar u ocasionara la pérdida de datos del sistema del usuario.*
- ***Alerta:*** *Notificación automática de un suceso o error.*
- ***Brecha Digital:*** *Hace referencia a la diferencia Socioeconómica entre aquellas comunidades que tienen accesibilidad a las TIC y aquellas poblaciones que no lo tienen.*
- ***Certificado:*** *Los Sistemas criptográficos utilizan este archivo como prueba de identidad. Contiene el nombre del Usuario y la clave pública.*
- ***Cobertura:*** *Área geográfica en la que un operador de telecomunicaciones presta determinado tipo de servicio.*
- ***Contraseña:*** *Cadena exclusiva de caracteres que introduce un usuario como código de identificación para restringir el acceso a equipos y archivos confidenciales.*
- ***Firewall:*** *Es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el trafico es benigno o maligno.*

- ***Firma Digital o electrónica:*** *Es el valor numérico que se adhiere a un mensaje de datos y que utiliza un procedimiento matemático conocido vinculado a la clave del indicador y al texto del mensaje para determinar que este valor se haya obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no haya sido modificado después de efectuada la transformación.*
- ***Gobierno en Línea:*** *Estrategia definida por el Gobierno Nacional mediante Decreto 1151 de 2008, que pretende dar un salto de inclusión social y de competitividad TIC, Esta estrategia pretende contribuir a mejorar la eficiencia y transparencia del estado colombiano a través de la construcción gradual de un Gobierno electrónico.*
- ***Malware:*** *Programa informático que tiene efectos no deseados o maliciosos, este utiliza a menudo herramientas de comunicación populares como el correo electrónico y la mensajería instantánea y medios magnéticos extraíbles como USB, para difundirse y hacer daño a los sistemas de información.*

Los Siguientes son términos de la estructura de la organización

- ***CICCI:*** *Comité Institucional de Coordinación de Control Interno.*
- ***Contingencia:*** *posible evento futuro, condición o eventualidad.*
- ***Continuidad del negocio:*** *capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.*
- ***Crisis:*** *ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.*
- ***CIGD:*** *Comité Institucional de Gestión y Desempeño.*
- ***Mapa de Riesgos:*** *documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.*
- ***MIPG:*** *Modelo Integrado de Planeación y Gestión.*
- ***Restablecimiento:*** *capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.*

Los siguientes son los términos que hacen parte de la SUPERSALUD

- ***SARLAFT:*** *Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo.*

- ***SICOF:*** *(Sistema Integrado de Información de Control Fiscal) sistema que apoya los procesos de los negocios misionales: auditorías, investigaciones, juicios y jurisdicción coactiva. Proporciona información oportuna y exacta y permite adoptar y aplicar decisiones necesarias en el cumplimiento del ejercicio del control fiscal.*

NORMATIVIDAD

- ***Ley 87 de 1993:*** *Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones. (Modificada parcialmente por la Ley 1474 de 2011). En su artículo segundo, objetivos del Control Interno establece: Literal a). Proteger los recursos de la organización, buscando adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.*
- ***Ley 1474 de 2011:*** *Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.*
- ***Ley 1581 de 2012:*** *Reglamentada Parcialmente por el Decreto Nacional 1377 de 2013: Por la cual se dictan disposiciones generales para la protección de datos personales*
- ***Decreto 1072 de 2015:*** *Regula el sistema de gestión de seguridad y salud en el trabajo. La implementación del SG-SST es de obligatorio cumplimiento. Las empresas, sin importar su naturaleza o tamaño, deben implementar un Sistema de Gestión de la Seguridad y Salud en el Trabajo.*
- ***Decreto 1078 de 2015:*** *Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.*
- ***Decreto 1499 de 2017:*** *Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único del Sector Función Pública, establece el Modelo Integrado de Planeación y Gestión -MIPG- el cual surge de la integración de los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad en un solo Sistema de Gestión, y de la articulación de éste con el Sistema de Control Interno.*
- ***Decreto 1008 de 2018:*** *Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.*
- ***Resolución 0312 de 2019****: La nueva Resolución 0312 de 2019 deroga a la Resolución 1111 de 2017 dentro de la normatividad en seguridad y salud en el*

trabajo, estableciendo de esta manera los nuevos estándares mínimos para el Sistema de Gestión de Seguridad y Salud en el Trabajo y la implementación del SGSST de una empresa.

- ***Resolución 500 de 2021**: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.*
- ***NTC ISO 27001:2013:** Sistema de Gestión de Seguridad de la Información (SGSI). Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.*
- ***NTC ISO 9001:2015:** Requisitos Sistemas de Gestión de la Calidad. Esta Norma es la base del Sistema de Gestión de la Calidad – SGC-. Es una norma internacional que se centra en todos los elementos de la gestión de la calidad con los que una empresa debe contar para tener un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios.*
- ***NTC ISO 45001:2018:** Sistemas de Gestión de la Seguridad y Salud en el Trabajo. Es la norma internacional para sistemas de gestión de seguridad y salud en el trabajo, destinada a proteger a los trabajadores y visitantes de accidentes y enfermedades laborales.*
- ***NTC ISO 31000:2018:** Gestión del Riesgo. Directrices. Esta Norma ofrece las directrices y principios para gestionar el riesgo de las organizaciones. Además, provee una serie de técnicas para la identificación y evaluación de riesgos, tanto positivos como negativos.*
- ***NTC ISO 14001:2015:** Sistemas de Gestión Ambiental -SGA-.Ayuda a gestionar e identificar los riesgos ambientales que pueden producirse internamente en la empresa mientras realiza su actividad. La implementación de la norma ISO 14001 y un SGA es un activo de valor importantísimo para las empresas y organizaciones que lo poseen.*
- ***NTC ISO 37001:2016** Sistemas de Gestión Antisoborno. La ISO 37001 es la norma internacional para los sistemas de gestión Antisoborno. La norma está diseñada para ayudar a las organizaciones a implantar y mantener medidas específicas que les ayuden a prevenir, detectar y abordar el soborno en toda la organización y sus actividades comerciales.*
- ***Guía para la Administración de Riesgo y Diseño de Controles en entidades públicas, del Departamento Administrativo de la Función Pública versión 05:** propone la metodología para la administración del riesgo. En esta versión se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo.*

- ***CIRCULAR EXTERNA 20211700000005-5 DE 2021:*** instrucciones: *generales relativas al subsistema de administración del riesgo de corrupción, opacidad y fraude (sicof) y modificaciones a las circulares externas 018 de 2015, 009 de 2016, 007 de 2017 y 003 de 2018.*

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La política de administración de riesgos de la Industria de Licores del Valle –ILV-, tiene un carácter estratégico y está fundamentada en el modelo integrado de planeación y gestión, la guía de administración del riesgo y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la Empresa.

Aplica para todos los niveles, áreas y procesos de la Industria e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

- Los Riesgos estratégicos son los que pueden afectar el cumplimiento del plan estratégico institucional.
- Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.
- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de seguridad digital que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.
- Los riesgos de continuidad de negocio que impiden la prestación normal de los servicios institucionales debido a eventos calificados como crisis.

La herramienta para identificar, valorar, evaluar y administrar los riesgos de gestión, de corrupción y de seguridad digital, se toma como base la diseñada por el DAFP, que presenta en la caja de herramientas en los formatos en Excel, que son adecuados a las necesidades de la ILV, para lo cual la Subgerencia de Planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento, actualización de información y dispone un manual de uso para el servicio de todos los procesos.

El periodo de revisión e identificación de los riesgos institucionales se debe realizar cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción anual, asegurando la articulación de éstos con los compromisos de cada proceso.

OBJETIVO DE LA POLÍTICA DE RIESGOS

Alcanzar un nivel aceptable de riesgos residuales en todos los procesos, Estableciendo los principios básicos y el marco general a través de la gestión de acciones de control, con el fin de asegurar el cumplimiento de la misión institucional, los compromisos de gobierno, los objetivos estratégicos y de procesos vigentes.

OBJETIVOS ESPECIFICOS

- Establecer los mecanismos de comunicación utilizados para dar a conocer la política de administración de riesgos.
- Adoptar las metodologías que permitan a la Industria de Licores del Valle gestionar de manera efectiva los diferentes tipos de riesgos identificados en la declaración de política de administración del riesgo.
- Establecer los niveles de aceptación al riesgo, niveles para calificar la probabilidad y el impacto, alternativas de tratamiento de riesgos, periodicidad de seguimiento a la gestión de riesgos.
- Establecer los niveles de líneas de defensa y de responsabilidad frente al manejo de riesgos

ALCANCE

Aplica a todos los procesos, proyectos, servicios y planes de la entidad, conforme a cada tipo y clasificación de riesgo, Incluye los riesgos estratégicos, de proceso, de corrupción, de seguridad de la información, de seguridad y salud en el trabajo, ambientales, y todos aquellos que puedan afectar el cumplimiento de los objetivos

estratégicos y de los procesos; bajo la responsabilidad de los líderes de proceso, líneas de defensa y a todos los servidores públicos en las actividades que ejecutan en la operatividad de la ILV.

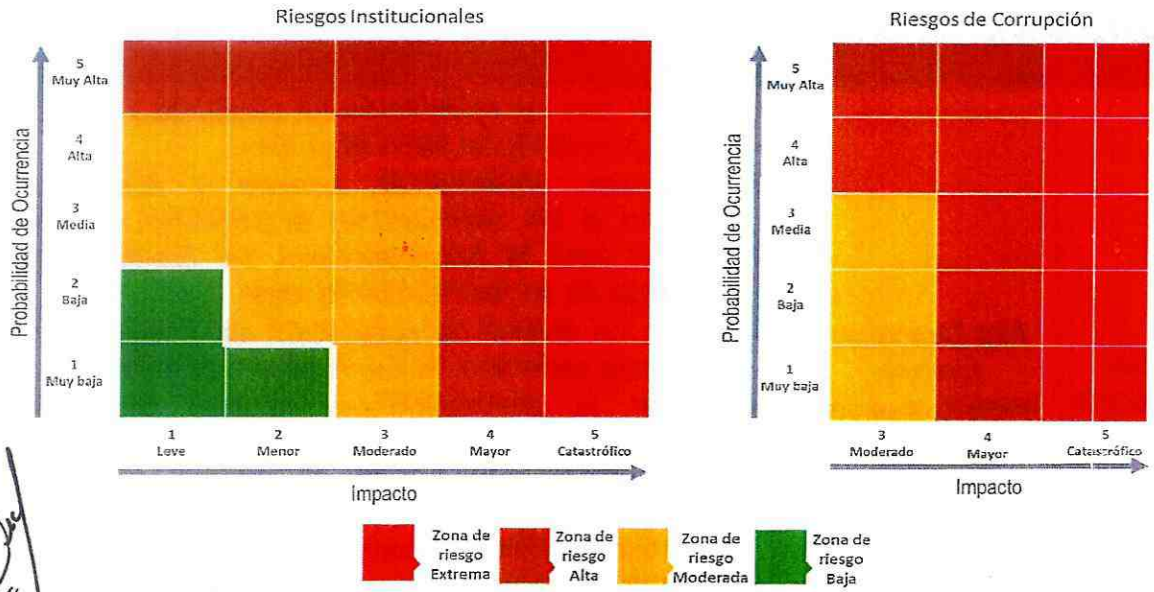
NIVELES DE ACEPTACIÓN DEL RIESGO

Acorde con los riesgos residuales aprobados por los líderes de procesos y socializados en el comité institucional de coordinación de control interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados.

La Industria de Licores del Valle, determina que para los riesgos residuales de gestión y seguridad digital que se encuentren en zona de riesgo baja, está dispuesto a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento.

Gráfica 1. Matriz de calificación de nivel de severidad del riesgo



RESPONSABILIDADES

La responsabilidad está definida mediante las líneas de defensa y en la entidad se acogen según la siguiente tabla:

Tabla 1. *Responsabilidades de las Líneas de Defensa*

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Alta Dirección Comité Institucional de Gestión y Desempeño	• Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. • Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • Recomendaciones de mejoras a la política de operación para la administración del riesgo. • Ejercer el rol de línea estratégica para la administración del riesgo, en articulación con el comité Institucional de Coordinación de Control Interno.
Líneas de Defensa	**Responsable**	**Responsabilidad frente al riesgo**
Línea Estratégica	Alta Dirección Comité Institucional de Gestión y Desempeño	• Cumplir con los estándares de conducta y la práctica de los principios del servicio público. • Establecer, implementar, evaluar y actualizar de acuerdo a los cambios en el contexto, la Política Integral para la Administración del Riesgo, bajo el liderazgo de su representante legal. • Definir los niveles de aceptación del riesgo, teniendo en cuenta cada uno de los objetivos establecidos. • Evaluar la planeación estratégica, considerando alertas frente a posibles incumplimientos, necesidades de recursos, cambios en el entorno que puedan afectar su desarrollo, entre otros aspectos que garanticen de forma razonable su cumplimiento. • Establecer líneas de reporte dentro de la entidad para evaluar el funcionamiento del Sistema de Control Interno bajo el liderazgo del representante legal, a fin de garantizar su adecuada formulación y afectación

		frente a la gestión del riesgo. • Establecer mecanismos frente a la detección y prevención del uso inadecuado de información privilegiada u otras situaciones que puedan implicar riesgos para la entidad. • Analizar la información asociada con la generación de reportes financieros y sus riesgos asociados. • Evaluar periódicamente los objetivos establecidos para asegurar que estos continúan siendo consistentes y apropiados para la Entidad. • Analizar los resultados de la información consolidada y reportada por la segunda línea de defensa, y en especial considerar sí se han presentado materializaciones de riesgo. • Definir los procesos, programas o proyectos (según aplique), susceptibles de posibles actos de corrupción, acorde con el análisis del entorno interno y externo. • Monitorear los riesgos de corrupción con la periodicidad establecida en la Política de Administración del Riesgo. • Realizar adecuada división de las funciones y que éstas se encuentren segregadas en diferentes personas para reducir el riesgo de acciones fraudulentas.
Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Alta Dirección Comité Institucional de Gestión y Desempeño	• Analizar el impacto sobre el control interno por cambios en los diferentes niveles organizacionales. • Evaluar fallas en los controles (diseño y ejecución) para definir cursos de acción apropiados para su mejora basados en los informes de la segunda y tercera línea de defensa. • Analizar los riesgos asociados a los bienes y servicios adquiridos externamente y/o actividades tercerizadas que afecten la prestación del servicio a los usuarios, basados en los informes de la segunda y tercera línea de defensa. • Monitorear los riesgos aceptados revisando que sus condiciones no hayan cambiado y definir su pertinencia para sostenerlos o ajustarlos. • Orientar el Direccionamiento Estratégico y la Planeación Institucional

		• Determinar las políticas y estrategias que aseguran que la estructura, procesos, autoridad y responsabilidad estén claramente definidas para el logro de los objetivos de la entidad • Desarrollar los mecanismos incorporados en la Gestión Estratégica del Talento Humano • Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la entidad. • Establecer las políticas de operación encaminadas a controlar los riesgos que pueden llegar a incidir en el cumplimiento de los objetivos institucionales • Responder por la fiabilidad, integridad y seguridad de la información, incluyendo la información crítica de la entidad independientemente de cómo se almacene • Establecer políticas apropiadas para el reporte de la información fuera de la entidad y directrices sobre información de carácter reservado, personas autorizadas para brindar información, regulaciones de privacidad y tratamiento de datos personales y en general todo lo relacionado con la comunicación de la información fuera de la entidad. • Asegurar que los servidores responsables (tanto de la segunda como de la tercera línea defensa cuenten con los conocimientos necesarios y que se generen recursos para la mejora de sus competencias
Líneas de Defensa	**Responsable**	**Responsabilidad frente al riesgo**
Línea Estratégica Alta Dirección e instancias institucionales de Toma de Decisión, Dirección y Control	Comité Institucional de Control Interno.	• Someter a aprobación del Gerente la política de administración del riesgo previamente estructurada por parte de la oficina asesora de planeación, como segunda línea de defensa en la entidad; hacer seguimiento para su posible actualización y evaluar su eficacia frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. • Revisar la política de administración del riesgo por lo menos una vez al año para su actualización y validar su eficacia a la gestión del riesgo institucional. se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta.

		• Aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. • Garantizar el cumplimiento de los planes de la entidad. • Aprobar y hacer seguimiento al Plan Anual de Auditoría con enfoque basado en riesgos, presentado y ejecutado por parte de la Oficina de Control Interno. • Realimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. Así mismo, hacer seguimiento a su gestión, gestionar los riesgos y aplicar los controles • Evaluar y dar línea sobre la administración de los riesgos en la entidad • Realizar análisis de eventos y riesgos críticos
Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Primera línea	Líderes de Procesos Responsable del Proyecto Servicios en General	• Asegurar que al interior de su grupo de trabajo se reconozca el concepto de "administración de riesgo" la política, metodología y marco de referencia de Función Pública aprobado por la línea estratégica. • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos a todo nivel que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso y realizar seguimiento al mapa de riesgo del proceso a cargo. • Delegar, por parte del líder del proceso, el (los) profesionales que se encargaran de la identificación, monitoreo, reporte y socialización de los riesgos. • Informar a la segunda línea de defensa los cambios de responsables de reporte en caso de ausentismo laboral • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • Revisar el adecuado diseño y ejecución de los

		controles establecidos para la mitigación de los riesgos y su documentación se evidencie en los procedimientos de los procesos. • Revisar de acuerdo con su competencia y alcance la documentación de continuidad del negocio. • Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de preparación frente a la pérdida de continuidad de negocio. • Reportar a la segunda línea de defensa en los instrumentos definidos, los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • Realizar la medición y análisis a la gestión efectiva de los riesgos. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.
Líneas de Defensa	**Responsable**	**Responsabilidad frente al riesgo**
Primera línea	Líderes de Procesos Responsable del Proyecto Servicios en General	• Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo y aplicar las acciones correctivas o de mejora necesarias. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces. • En caso de la materialización de un riesgo no identificado, este debe ser gestionado en los instrumentos definidos por la ILV y ser incluido en el mapa de riesgo institucional. <u>El líder del proceso debe:</u> • Verificar las acciones preventivas y registrar el avance junto con la evidencia, en los instrumentos definidos por la ILV, de acuerdo con la periodicidad definida.

		• Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación. • Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo, así como las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir. • Comunicar al equipo de trabajo los resultados de la gestión del riesgo. • Asegurar que se documenten las acciones de corrección o prevención en el plan de mejoramiento. • Revisar y actualizar el mapa de riesgos con el acompañamiento de la Subgerencia de Planeación. <u>Los servidores en general deben:</u> • Participar en el diseño de los controles que tienen a cargo. • Ejecutar el control de la forma como está diseñado. • Proponer mejoras a los controles existentes.
Líneas de Defensa	**Responsable**	**Responsabilidad frente al riesgo**
Primera línea	Líderes de Procesos Responsable del Proyecto Servicios en General	<u>El responsable del proyecto debe:</u> • Realizar la identificación de los riesgos del proyecto. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad
Líneas de Defensa	**Responsable**	**Responsabilidad frente al riesgo**
Segunda línea	Subgerencia de Planeación y Sistemas de Gestión	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual.

		• Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del CICCI. • Capacitar al grupo de trabajo de cada dependencia en la metodología y herramienta para la gestión del riesgo con la asesoría de la Dirección de Gestión y Desempeño Institucional como líder de la política de control interno. • Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. • Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología. • Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo residual aceptado por la entidad
Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Segunda línea	Subgerencia de Planeación y Sistemas de Gestión	• Hacer seguimiento al plan de acción establecido para la mitigación de los riesgos de los procesos registrados en el Sistema Integrado de Gestión. • Revisar que el reporte de información al el Sistema Integrado de Gestión esté acorde con lo aprobado por el líder del proceso. • Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para análisis y seguimiento ante el CIGD. • Presentar al Comité Institucional de Coordinación de Control Interno-CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos o proyectos. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. • Coordinar con los líderes de proceso el responsable de reporte de seguimiento a los riesgos, controles y

		planes de acción en los instrumentos definidos por el Sistema Integrado de Gestión. • Liderar la elaboración de planes de mejoramiento resultantes de la evaluación independiente respecto al cumplimiento de la política integral de administración del riesgo realizada por la tercera línea de defensa. • Liderar la identificación de aspectos e impactos ambientales en la operación de los procesos, en el ciclo de vida de los bienes y servicios adquiridos externamente y/o en las actividades tercerizadas. • Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso. • Comunicar a los líderes de proceso los resultados de la gestión del riesgo. • Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos (mapa de riesgo del proceso). • Socializar y publicar el mapa de riesgos institucional.
Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Segunda línea	Subgerencia de Planeación y Sistemas de Gestión	• Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y logar el cumplimiento a los objetivos. • Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el cual debe ser gestionado en los instrumentos definidos por el Sistema Integrado de Gestión y ser incluido en el mapa de riesgo institucional. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten

		los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean gestionados por la primera línea de defensa.
Líneas de Defensa	**Responsable**	**Responsabilidad frente al riesgo**
Segunda Línea	Secretaria General y Jurídica	• Orientar a la primera línea de defensa para definir la estrategia de continuidad del negocio identificando los escenarios. • Actualizar la documentación que soporta la estrategia de continuidad del negocio. • Identificar, valorar, evaluar y gestionar los riesgos de pérdida de continuidad del negocio.
Segunda Línea	Subgerencia de Planeación y Sistemas de Gestión Subgerencia Administrativa (Gestión del Talento Humano – Gestión de TIC)	• Liderar mesas de trabajo para la determinación del análisis de impacto del negocio, documentación de los escenarios de riesgos y plan de continuidad de negocio institucional. • Actualizar, según se requiera, los escenarios de riesgos de continuidad y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad. • Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio.
Líneas de Defensa	**Responsable**	**Responsabilidad frente al riesgo**
Segunda Línea	Secretaria General y Jurídica (Gestión Jurídica)	• Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Los supervisores e interventores de contratos deben realizar seguimiento a los riesgos de estos e informar las alertas respectivas.

		• Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. • Participar en las pruebas del plan de continuidad del negocio y en la implementación. • En la Defensa Jurídica tendrá el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico. • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. • Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.
Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Segunda Línea	Subgerencia Financiera	• Monitorear los riesgos identificados en la gestión contable y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad del área contable.
Segunda Línea	Subgerencia Administrativa (Gestión del Talento Humano y TIC)	• Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Liderar la identificación de peligros y valoración de riesgos de Seguridad y Salud en el Trabajo. • Liderar la identificación, valoración y tratamiento de los riesgos de seguridad de la información. • Realizar monitoreo de los riesgos y controles tecnológicos • Establecer procesos para monitorear y evaluar el

		desarrollo de exposiciones al riesgo relacionadas con tecnología nueva y emergente.
Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Tercera Línea	Subgerencia de Control Interno	• Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. • Establecer el plan anual de auditoría basado en riesgos, priorizando aquellos procesos de mayor exposición • Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.
Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Tercera Línea	Subgerencia de Control Interno	• Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. • Llevar a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI. • Evaluar el diseño y efectividad de los controles y provee información a la alta dirección y al Comité de Coordinación de Control Interno referente a la efectividad y utilidad de los mismos. • Realizar seguimiento a la implementación de mejoras sobre los lineamientos de continuidad del negocio. • Realizar seguimiento a la implementación de la estrategia de continuidad del negocio y a las pruebas efectuadas. • Recomendar mejoras a la política de operación para la administración del riesgo. • Evaluar la eficacia de las estrategias de la entidad

		para promover la integridad en el servicio público, especialmente, si con ella se orienta efectivamente el comportamiento de los servidores hacia el cumplimiento de los estándares de conducta e Integridad (valores) y los principios del servicio público; y si apalancan una gestión permanente de los riesgos y la eficacia de los controles • Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa • Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías • Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad • Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.
Líneas de Defensa	**Responsable**	**Responsabilidad frente al riesgo**
Tercera Línea	Subgerencia de Control Interno	• Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos • Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles. • Proporcionar seguridad razonable con respecto al diseño e implementación de políticas, procedimientos y otros controles • Proporcionar información sobre la eficiencia, efectividad e integridad de los controles tecnológicos y, según sea apropiado, puede recomendar mejoras a las actividades de control específicas. • Informar sobre la confiabilidad y la integridad de la información y las exposiciones a riesgos asociados y las violaciones a estas • Comunicar a la primera y la segunda línea, aquellos aspectos que se requieren fortalecer relacionados con la información y comunicación • Generar información sobre evaluaciones llevadas a cabo por la primera y segunda línea de defensa • Evaluar si los controles están presentes (en políticas y

		procedimientos) y funcionan, apoyando el control de los riesgos y el logro de los objetivos establecidos en la planeación institucional

LINEAMIENTOS GENERALES DE LA POLITICA INTEGRAL DE ADMINISTRACION DEL RIESGO

LINEAMIENTOS PARA RIESGOS ESTRATÉGICOS Y OPERATIVOS (DE PROCESO).

En la Industria de Licores del Valle, para riesgos estratégicos, operativos y los de seguridad digital, se adoptan la metodología como los criterios para definir el nivel de probabilidad e impacto propuestos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5 y/o sus actualizaciones. Se adecua a las condiciones de la empresa en este, lo referente a la frecuencia como lo de la descripción económica y presupuestal en el impacto.

NIVEL DE CALIFICACION DE PROBABILIDAD PARA RIESGOS.

Nivel para Calificación de probabilidad para riesgos de proceso y seguridad digital

La probabilidad de ocurrencia estará asociada a la exposición al riesgo de la actividad que se esté analizando.

De este modo, para riesgos operativos la probabilidad inherente será el número de veces que se pasa por el punto crítico de riesgo en el periodo de un año. Para ello, se puede tomar como referencia la tabla de 2 que ha definido la empresa en el presente documento, la cual está acorde con la gestión de la misma.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, v 4 - Dirección de Gestión y Desempeño Institucional, octubre 2018*

NIVEL DE CALIFICACION DE IMPACTO

La calificación del impacto para los riesgos estratégico, operativos y de seguridad de la información se tendrá en cuenta la siguiente escala, de acuerdo con la realidad de la Industria de Licores del Valle.

Tabla 4. *Calificación de impacto para riesgos de proceso y seguridad digital*

TABLA CRITERIO PROBABILIDAD ILV			
NIVEL	**IMPÁCTO**	**DESCRIPCIÓN ECONOMICA O PRESUPUESTAL**	**DESCRIPCIÓN REPUTACIONAL**
20%	LEVE	Pérdida económica hasta 10 SMLV	Solo de conocimiento de algunos funcionarios.
40%	MENOR	Pérdida económica de 11 hasta 30 SMLV	De conocimiento general de la entidad a nivel interno, Dirección General, Comités y Proveedores.
60%	MODERADO	Pérdida económica de 31 hasta 200 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Local o Sectores Administrativos
80%	MAYOR	Pérdida económica de 201 hasta 1000 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Nacional o Territorial
100%	CATASTROFICO	Pérdida económica superiores a 1000 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel internacional.

Fuente: *Subgerencia de Planeación*

La calificación del impacto para los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración establecida por Secretaria de Transparencia de la Presidencia de la República. Cada riesgo identificado es valorado de acuerdo con las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

Tabla 5. *Calificación del Impacto para los riesgos de Corrupción*

Tabla 2. *Calificación de probabilidad para riesgos proceso y seguridad digital*

TABLA CRITERIO PROBABILIDAD ILV			
	FRECUENCIA DE LA ACTIVIDAD	***PROBABILIDAD***	
MUY BAJA	La actividad se realiza máximo 4 veces al año	20%	
BAJA	La actividad se realiza entre 5 a 12 veces al año	40%	
MEDIA	La actividad se realiza entre 13 a 60 veces al año	60%	5 VECES /MES*12
ALTA	La actividad se realiza entre 61 a 365 veces al año	80%	1 POR DÍA
MUY ALTA	La actividad se realiza más 365 veces al año	100%	

Fuente: *Oficina Asesora de Planeación ILV*

Nivel de calificación de probabilidad para riesgos de corrupción

Tabla 3. *Calificación de probabilidad para riesgos de corrupción*

Nivel	Probabilidad		Descripción
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

No	Pregunta: Si el Riesgo de corrupción se materializa podría	Respuesta	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimientode metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

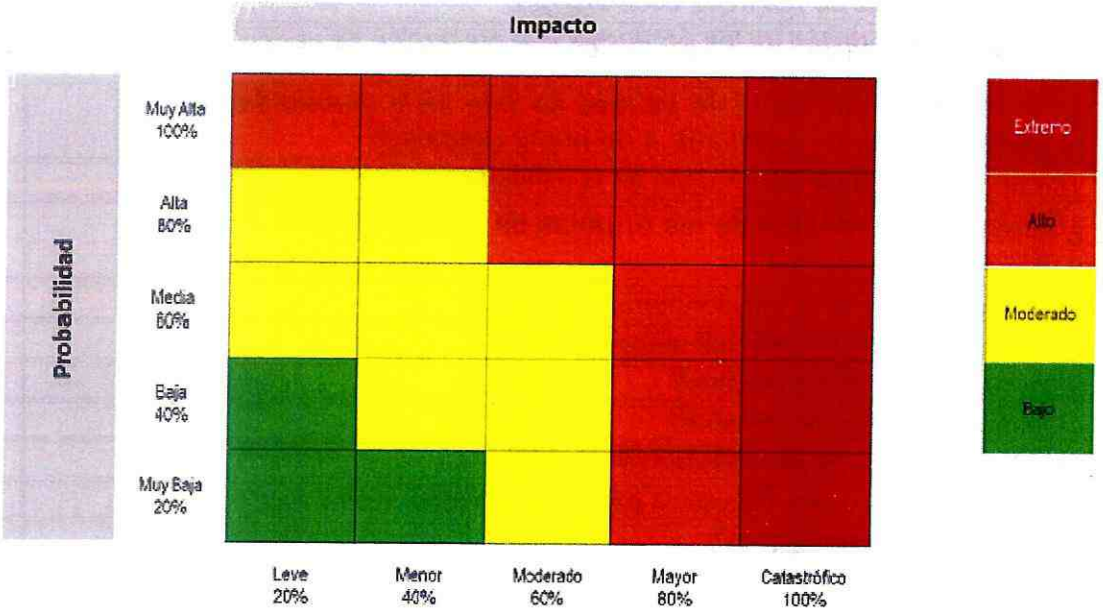
Nivel	Descriptor	Descripción	Respuestas afirmativas
1	Moderado	Genera medianas consecuencias sobre la Entidad.	1 a 5
2	Mayor	Genera altas consecuencias sobre la entidad.	6 a 11
3	Catastrófico	Genera consecuencias desastrosas para la Entidad.	12 a 19

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas v 5.*

Niveles de severidad

En el riesgo inherente, se trata de determinar los niveles de severidad a través de la combinación entre probabilidad y el impacto. Se adopta la metodología establecida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5, donde se definen cuatro (4) zonas de severidad en la matriz de calor: Extremo, alto, moderado y bajo.

Tabla Matriz de calor (Niveles de severidad del riesgo)



Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas. Versión 5*

Nivel de aceptación o tolerancia al riesgo

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. Para la Industria de Licores del Valle se establece de la siguiente manera:

Riesgos residuales estratégico y operativo (de proceso)	**Bajo** **Se ACEPTA.** Cumple con los criterios de aceptación de riesgo no es necesario diseñar controles; deben estar sujetos a monitoreo por parte de la primera línea de defensa.

Determinación de la tolerancia, capacidad de riesgo y valor máximo de la escala

Aplicando los valores de probabilidad e impacto propuestos en la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5, la Alta Dirección, representada por el Comité Institucional de Coordinación de Control Interno, adopta la matriz de calor (niveles de severidad del riesgo) propuesta en dicha guía. Igualmente se adoptan las siguientes definiciones:

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. Para la Entidad este valor se define como moderado.

Riesgo residual estratégico y operativo (de proceso)	**Moderado** Se establecen acciones de control detectivas/ preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo y/o correctivas para REDUCIR el impacto. Se debe realizar seguimiento trimestral por parte de la primera línea de defensa.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad. Para la Entidad este valor se define como moderado.

Riesgo residual estratégico y operativo (de proceso)	**Moderado** Se establecen acciones de control detectivas/ preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo y/o correctivas para REDUCIR el impacto. Se debe realizar seguimiento trimestral por parte de la primera línea de defensa.

Valor máximo de la escala: es el valor máximo de la escala que resulta de combinar la probabilidad y el impacto.

	Riesgo extremo
Riesgo operacional (de proceso)	Se establecen acciones de control detectivas/ preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo y/o correctivas para REDUCIR el impacto. Se debe realizar seguimiento mensual por parte de la primera línea de defensa

Tratamiento y opciones de manejo

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de corrupción.

De acuerdo a lo establecido en la declaración de la Política de Riesgos de la entidad, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento.

Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción, la respuesta será evitar o reducir el riesgo.

Las estrategias para combatir el riesgo, hace referencia de la decisión que se toma frente a un determinado nivel del riesgo y pueden ser aceptar, evitar y reducir.

Aceptar: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización

.

Evitar: Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

Reducir: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.

PERIODICIDAD DE SEGUIMIENTO A CONTROLES

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	NIVEL DE ACEPTACIÓN Y PERIODICIDAD
Riesgo operativo	Bajo	Realiza seguimiento semestral al control en la herramienta de Gestión de Riesgos y se registra sus avances en la Matriz de administración de Riesgos desde la primera línea de defensa.
Riesgo operativo	Moderado	Se define el tratamiento del riesgo: Evitar, reducir (compartir), reducir (mitigar). Se realiza seguimiento trimestral al control y se establecen planes de acción (cuando el tratamiento es reducir) para fortalecer las actividades de control y evitar la posible materialización del riesgo. Se hace seguimiento Trimestral al plan de acción y se registra sus avances en la Matriz de administración de Riesgos desde la primera línea de defensa.
Riesgo operativo	Alto y Extremo	Se define el tratamiento del riesgo: Evitar, reducir (compartir), reducir (mitigar). Se realiza seguimiento mensual al control y se establecen planes de acción (cuando el tratamiento es reducir) para fortalecer las actividades de control y evitar la posible materialización del riesgo. Se hace seguimiento Trimestral al plan de acción y se registra sus avances en la Matriz de administración de Riesgos desde la primera línea de defensa.

LINEAMIENTOS PARA RIESGOS DE CORRUPCIÓN, RIESGOS DE SEGURIDAD Y SALUD EN EL TRABAJO, RIESGOS DE GESTIÓN AMBIENTAL, RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo a las responsabilidades definidas en la presente política, cada dependencia y/o proceso líder de cada tipo de riesgo debe definir los niveles de aceptación, tolerancia, capacidad del riesgo y tratamiento a los mismos, de conformidad a lo establecido en el aparte de Responsabilidades de la presente política, los cuales deberán ser incorporados como parte integral de esta política.

Igualmente, cada dependencia y/o proceso líder de cada tipo de riesgo debe desarrollar un procedimiento y una herramienta específica que permita establecer el conjunto de actividades para operativizar la gestión de los riesgos.

CRITERIOS PARA LA EVALUACIÓN DE IMPACTO DE PÉRDIDA DE CONTINUIDAD

La determinación de las prioridades de recuperación de servicios en caso de materialización de escenarios de pérdida de continuidad de negocio se realiza mediante la valoración del impacto percibido por los líderes de los procesos. Mediante mesa de trabajo los participantes califican los impactos en cada variable y definen el orden de recuperación de los servicios asignando la secuencia de reactivación de los mismos primero a los servicios con mayor impacto y de manera secuencia a los servicios con menor impacto percibido.

Tabla 6. *Criterios para la evaluación de impacto de pérdida de continuidad*

Criterio	Descripción
Financiero	Nivel de pérdidas económicas
Reputacional	Nivel de pérdida de la confianza de los grupos de valor en la entidad
Legal / Regulatorio	Nivel de incumplimiento de normas y regulaciones a las que está sometida la entidad
Contractual	Impactos asociados al incumplimiento de cláusulas en obligaciones contractuales

Misional	Nivel de incumplimiento o impacto percibido por imposibilidad de cumplir los objetivos y obligaciones misionales.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas v5.*

De igual manera, en el instructivo de análisis de impacto al negocio se amplía esta información:

https://www.funcionpublica.gov.co/web/intranet/manuales-proceso-direccionamiento-estratégico

ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla "acciones de respuesta a riesgos".

Tabla 7. *Acciones de respuesta a riesgos*

Tipo de Riesgo	Responsable	Acción
		• Informar a la Subgerencia de Planeación y sistemas de gestión como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado y marcar en el SGI la alerta de posible materialización.

Riesgo de Corrupción	*Líder del Proceso*	• Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento. • Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Revisar los controles existentes y actualizar el mapa de riesgos.
	Subgerencia de Control Interno	• Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Informar a discreción los posibles actos de corrupción al ente de control.

Tipo de Riesgo	Responsable	Acción
Riesgo de Gestión y Seguridad Digital	*Líder del Proceso*	• Informar a la Oficina Asesora de Planeación como segunda línea de defensa, el evento o materialización de un riesgo. • Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento. • Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos. • Dar cumplimiento al procedimiento plan de mejoramiento.
	Subgerencia de Control Interno	• Informar al líder del proceso sobre el hecho encontrado • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente. • Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el

		procedimiento.
Tipo de Riesgo	**Responsable**	**Acción**
Riesgo de Continuidad del Negocio	*Comité de Crisis*	• Activar el plan de continuidad de negocio.

Tabla 8.*Seguimiento al mapa de riesgos y controles*

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de Tratamiento-Controles
Riesgos de Gestión y Seguridad Digital	Baja	Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances en el módulo de riesgos- SGI.
	Moderada	Se realiza seguimiento a los controles con periodicidad TRIMESTRAL y se registran sus avances en el módulo de riesgos- SGI.
	Alta	Se realiza seguimiento a los controles con periodicidad BIMESTRAL y se registran sus avances en el módulo de riesgos- SGI.
	Extrema	Se realiza seguimiento a los controles con periodicidad MENSUAL y se registra en el módulo de riesgos – SGI.
Riesgo de Corrupción	Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento MENSUAL y se registra en el módulo de riesgos – SGI.	

ESTRATEGIA DE SEGUIMIENTO AL PLAN DE ACCIÓN

Tipo de Riesgo	Zona de Riesgo Residual o severidad	Estrategia de Tratamiento-Plan de Acción
Riesgos de Gestión y Seguridad Digital	Baja	No se debe realizar plan de acción por que está dentro del nivel de aceptación del riesgo por Función Pública.
	Moderada de Alta Extrema	El líder del proceso define acciones que permita mitigar el riesgo residual. Asimismo, determina la fecha de inicio y finalización de estas y establece los seguimientos que va a realizar durante la ejecución de la acción correspondiente a su avance, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles. Después de haber implementado la acción debe realizar un seguimiento con el fin de evaluar la efectividad del plan de acción.

ANEXOS

Para una mayor comprensión de la política de operación para la administración del riesgo, se define que los anexos son parte fundamental de este documento técnico, por tanto, se recomienda su consulta y conocimiento por parte de todos los servidores públicos de la Entidad.

- Manual operativo MIPG https://www.funcionpublica.gov.co/documents/34645357/34702994/Modelo_integ rado_planeacion_gestion.pdf/7f3d55ea-4ad6-3bdc-3f05-a23d287ca69b?t=1615223466439

- Manual Metodología de riesgos https://www.funcionpublica.gov.co/documents/34645357/34702994/Manual_meto dologia_riesgos.pdf.pptx/8b3d4a02-7c0d-41a7-b609-

3752cb063bc8?t=1536162961916

- Guía para la Administración del riesgo de FP
https://www.funcionpublica.gov.co/documents/34645357/34702994/Guia_externa_administracion_riesgo_direccinamiento_estrategico.pdf/0330fa64 -0a6a-4772- 887f-27aae325afa5?t=1614199851989

- Superintendencia Nacional De Salud
Circular Externa 20211700000005-5 De 2021

- Superintendencia Nacional De Salud
Circular Externa 000009 Del 21 De Abril De 2016