****

**PROCEDIMIENTO PARA LA**

**GESTION DEL RIESGO**

**CÓDIGO:** PD-GOP-04 **VERSIÓN:** 01

**FECHA:** 24/02/2017

**REVISADO: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Director de Operaciones**

**APROBADO: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Gerente General**

1. **OBJETIVO**

Establecer el procedimiento para la Gestión del Riesgo, tendiente a determinar los riesgos, evaluar tanto la probabilidad de ocurrencia como su potencial impacto, generar planes de contingencia y monitorear y controlar su evolución en el tiempo.

1. **ALCANCE**

Este procedimiento comprende desde la identificación del riesgo hasta el control en el tiempo.

1. **DEFINICIONES**

* **Agente Generador:** Los objetos o sujetos que tienen la capacidad de originar un riesgo, se podrían clasificar en 5 categorías: personas, equipos, materiales, instalaciones y entorno.
* **Amenaza**: Peligro latente que representa la probable manifestación de un fenómeno físico de origen natural, socio-natural o antropogénico, que se anticipa, puede producir efectos adversos en las personas, la producción, la infraestructura y los bienes y servicios..
* **Barrera:** Obstáculo construido con el fin de impedir acceso a cierto lugar.
* **Causa:** Son las razones o motivos por los cuales se genera un riesgo
* **Control de accesos:** Procedimientos que se desarrollan en una propiedad para establecer que todo lo que ingrese o salga se encuentre de acuerdo con las normas establecidas en la propiedad y éstas con soporte en las leyes vigentes.
* **Controles existentes**: Especificar cuál es el control que la empresa, organización o propiedad horizontal tiene implementado para combatir, minimizar o prevenir el riesgo.
* **Cliente Crítico:** Es aquel cuya actividad económica está dedicada al comercio exterior (exportación e importación).
* **Efecto / consecuencia:** Son las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad.
* **Intención**: Idea o propósito malicioso que encubre cierta acción o comportamiento
* **Involucrados:** Son las dependencias o áreas encargadas de adelantar las acciones propuestas.
* **Impacto:** Consecuencias que puede ocasionar a la organización la materialización del riesgo.
* **Plan de contingencia:** Es una forma de organizarse para actuar frente a un evento posible.
* **Probabilidad:** Es la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.
* **Proceso:** conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) con un fin determinado.
* **Riesgo**: Es toda posibilidad de ocurrencia de aquella(s) situación(es) que pueda(n) entorpecer el normal desarrollo de nuestras funciones e impidan el logro de los objetivos.
* **SIG-HSEQ- BASC:** Sistema Integrado de Gestión de Calidad, Gestión SISO, Gestión Ambiental y Control y Seguridad.
* **Tratamiento:** es la aplicación concreta de las opciones del manejo del riesgo que entrarán a prevenir o a reducir el riesgo y harán parte del plan de manejo del riesgo.
* **Vulnerabilidad:** Elemento interno del riesgo. Factor interno del riesgo, es una medida de que tan susceptible es un bien, o un ser expuesto a ser afectado por un fenómeno perturbador

1. **PROCEDIMIENTO**
   1. **IDENTIFICACION DE RIESGOS:**

Basados en la contextualización de la compañía se identifican los riesgos conforme la planta física de la empresa, por áreas, por el entorno y por las medidas de control existentes en visita a puesto con administrador, representante legal o personal encargado de los servicios a prestar con cita debidamente programada dentro de los 15 días contados a partir del acta de instalación de los puestos. De igual forma se analiza en el proceso de cada puesto las consignas particulares y demás requisitos acordados por la empresa y el cliente para determinar conforme las actividades y operatividad que riesgos se pueden presentar.

En el proceso de identificación de riesgos se debe tener en cuenta la siguiente información como referencia:

**Proceso / subproceso**

* Para identificación de riesgos por proceso de la empresa

|  |  |
| --- | --- |
| **Proceso** | **subproceso** |
| GERENCIAL | Dirección estratégica |
| Mejora continua |
| Revisión gerencial |
| OPERATIVA | Comercial |
| Operaciones |
| Servicio al cliente |
| DE APOYO | Almacén |
| Armamento |
| Compras |
| Documental |
| Jurídica |
| Mantenimiento |
| Talento Humano |
| SIG- HSEQ BASC |

* Para identificación de riesgos clientes

|  |  |
| --- | --- |
| **Proceso** | **Subproceso** |
| OPERATIVA | Operaciones |

**Riesgo**

|  |
| --- |
| * **Riesgos estratégicos**: riesgos que afectan el Direccionamiento Estratégico de la Entidad, es decir la planeación |
| * **Riesgos operativos**: riesgos que afectan los procesos misionales o esenciales de la Entidad. |
| * **Riesgos financieros**: riesgos que afectan los recursos financieros de la Entidad, donde se incluye la planeación y ejecución presupuestal, elaboración de estados financieros, pagos, manejos de bienes, contratación etc. |
| * **Riesgos de cumplimiento**: asociados con la capacidad de la Entidad para cumplir con los requisitos legales, contractuales, de transparencia y en general con su compromiso ante la comunidad. |
| * **Riesgos tecnológicos**: se asocian con la capacidad de la Entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la Entidad y soporten el cumplimiento de la misión. |

**Descripción** (Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.)

**Causa**

**Efectos / consecuencias**:

* Pérdidas económicas
* Pérdida de imagen
* Insostenibilidad financiera
* Incumplimientos legales
* Daños a la integridad física
* Llamados de atención
* Sanciones
* Reprocesos
* Insatisfacción del usuario

**Controles existentes**

Se deben identificar la gestión, los sistemas técnicos y procedimientos existentes para controlar e riesgo y evaluar sus fortalezas y debilidades.

* 1. **ANALISIS, EVALUACION Y VALORACIÓN DEL RIESGO**

Se analiza cada riesgo con su descripción, agente generador, causa y efecto; de igual manera las medidas de control existentes encontradas, narradas y ejecutadas para cada uno de los riesgos identificados y en general todas las variables que puedan intervenir en hacer más vulnerable o no la compañía frente al riesgo, y así establecer la probabilidad y consecuencia (impacto) (Registros pasados, Literatura publicada, experiencia, juicios, etc.). Los criterios para valorar de acuerdo a lo evidenciado de cada aspecto están descritos en numeral 4.1. Metodología de evaluación y valoración del riesgo.

**Nota:** El análisis, evaluación y valoración de riesgosde cada Asociado en Matriz FT-GOP-27 se actualizará anualmente, en los casos que se materialice alguno de las riesgos identificados o se incluya algún riesgo de acuerdo a modificaciones de procesos, instalaciones y demás circunstancias se realizará de forma inmediata y se comunicará a los interesados.

* + 1. **METODOLOGÍA DE EVALUACIÓN Y VALORACIÓN DEL RIESGO**

Para determinar el nivel de riesgo y poder contar con decisiones y controles objetivos, se cuenta con la matriz de evaluación del riesgo en formato **FT-GOP-27 Matriz de evaluación y valoración de riesgos**, la cual ha sido formulada conforme los principios de la metodología establecida. Esta matriz especifica los criterios a evaluar y da la opción para que el evaluador de la calificación conforme lo planteado ítem por ítem, al final la matriz indicara cual es el nivel de riesgo conforme la selección realizada por el evaluador.

El nivel del riesgo se calcula del factor entre la probabilidad y la consecuencia de acuerdo a escalas de valoración ya establecidos para cada uno:

**NIVEL DE RIESGO= PROBABILIDAD x CONSECUENCIA**

En donde la probabilidad se conforma del producto entre:

**PROBABILIDAD= AMENAZA x VULNERABILIDAD**

|  |  |  |
| --- | --- | --- |
| **PROBABILIDAD (P) = Amenaza \* Vulnerabilidad** | | |
| **AMENAZA** | | |
| **Capacidad e intención de la amenaza para materializarse o aprovecharse de las vulnerabilidades** | | |
| **0,25** | **BAJA** | Amenaza sin capacidad y/o intensión. No se han presentado eventos relacionados con esta fuente de riesgo en el contexto externo de la organización hace 5 años o más. |
| **0,5** | **MEDIA** | Amenaza con capacidad y se han presentado eventos en el contexto externo con características atribuibles a esta fuente de riesgo dentro de los 2 a 5 años anteriores a la valoración. |
| **0,75** | **ALTA** | Amenaza con capacidad e intensión. Se han presentado eventos en el contexto externo atribuibles a esta fuente de riesgo dentro de 1 año a 2 años anteriores a la valoración. |
| **1** | **MUY ALTA** | Amenaza con capacidad e intención. Se han presentado eventos en el contexto externo atribuibles a esta fuente de riesgo dentro del año anterior a la valoración. |

A continuación se da a conocer los factores del contexto externo para valorar en anterior criterio (Amenaza):

|  |
| --- |
| **CONTEXTO EXTERNO** |
| Político/Legal: regulaciones estatales y gubernamentales, lineamientos de las comunidades y vigilados, normas – deberes y derechos. |
| Económico: presupuesto |
| Social: clases sociales, pobreza, salud, desempleo, vivienda, educación, incluyendo los aspectos culturales |
| Orden Público: Situación de orden público en el país y gobernabilidad. |
| Tecnología: medios, equipos y comunicaciones, rapidez con que sobrevienen los cambios y actualizaciones tecnológicas. |
| Ambientales: agrupa al conjunto de normas, regulaciones y permisos ambientales |
| requeridos para operar |

|  |  |  |
| --- | --- | --- |
| **VULNERABILIDAD** | | |
| **Debilidades que permiten el aprovechamiento por parte de la amenaza** | | |
| **0,25** | **BAJA** | Los controles de seguridad establecidos y aplicados en la empresa son totalmente eficaces para evitar la materialización del riesgo. No se requiere de la implementación de más controles |
| **0,5** | **MEDIA** | Los controles de seguridad establecidos y aplicados son suficientes para evitar la materialización del riesgo. Es viable implementar más controles para asegurar una total eficacia. |
| **0,75** | **ALTA** | Los controles de seguridad establecidos y aplicados son insuficientes y presentan fallas para evitar la materialización del riesgo. |
| **1** | **MUY ALTA** | No se han establecido y aplican controles de seguridad para evitar la materialización del riesgo. |

Una vez identificado tanto la amenaza como la vulnerabilidad el producto de éstos criterios determina la probabilidad de ocurrencia del riesgo y es determinado por la siguiente escala:



Para la valoración de la consecuencia se determina de acuerdo a los siguientes criterios:

|  |  |  |
| --- | --- | --- |
| **CONSECUENCIA (C) (Impacto / Daño)** | | |
| **Consecuencias que puede ocasionar a la organización la materialización del riesgo. Pueden ser sociales, legales, económicas, físicas, operativa, etc.** | | |
| **0,25** | **BAJA** | **Económico:** Pérdidas hasta por un SMLMV **Humano:** Sin Lesiones Físicas **Imagen:** Solo conocimiento de personal específico de la Empresa de acuerdo al caso a tratar. |
| **0,5** | **MEDIA** | **Económico** Pérdidas superiores a un SMMLV y hasta 5 SMMLV **Humano:** Lesiones leves sin incapacidad **Imagen:** El evento es de conocimiento de la totalidad de la Empresa |
| **0,75** | **ALTA** | **Económico** Pérdidas superiores a 5 SMMLV y hasta 20 SMMLV **Humano:** Lesiones leves con incapacidad **Imagen:** El evento es de conocimiento de la Empresa, la Administración y las Autoridades |
| **1** | **MUY ALTA** | **Económico:** Pérdidas superiores a 20 SMMLV **Humano:** Victima grave o Muerta **Imagen:** El evento es de conocimiento de la Empresa, la Administración, las Autoridades, medios de comunicación Regional y Nacional |

**ESCALA DE NIVEL DE RIESGO PARA PRIORIZACION DE RIESGOS**

|  |  |  |
| --- | --- | --- |
| **NIVEL DE RIESGO (NR) Probabilidad (P) \* Consecuencia (C)** | | |
| **Posibilidad de ocurrencia del riesgo que afecte los objetivos.** | | |
| **0 - 0,25** | **BAJO** | Mantener el monitoreo sobre los controles establecidos para evitar la materialización del riesgo. Tomar acciones correctivas para los riesgos materializados |
| **0,26- 0,5** | **MEDIA** | Tomar acciones e implementar medidas de control para reducir la vulnerabilidad y consecuencias |
| **0,51- 0,75** | **ALTA** | Implementar programas y medidas de seguridad, protección de activos y prevención de pérdidas. Tomar acciones e implementar medidas de control para reducir la vulnerabilidad y consecuencias. Requiere la atención por parte de los líderes de procesos. |
| **0,76- 1** | **MUY ALTA** | Requiere implementar medidas urgentes para atacar las vulnerabilidades. Diseñar e implementar un Plan de continuidad del negocio (BCP) puntual para reducir las consecuencias. Dar prioridad en el tratamiento. |

* 1. **TRATAMIENTO DEL RIESGO**

Para el tratamiento de los riesgos es necesario tener en cuenta los resultados de la valoración de la matriz de evaluación de riesgos FT-GOP-27, para determinar en Matriz FT-GOP-28 Control y seguimiento del tratamiento del riesgos el plan operativo en donde se registra el riesgo con su nivel y las actividades que se han planteado para el control con los respectivos responsables, recursos, fechas de ejecución, fechas de seguimiento y confirmación del cierre de las actividades.

* 1. **MONITOREO Y REVISION:**

Es necesario monitorear continuamente los riesgos, la efectividad del plan de tratamiento, las estrategias y el sistema de administración que se establece para controlar la implementación este registro del proceso de ejecución de las medidas de control se llevara a cabo en matriz FT-GOP-28 Control y seguimiento de tratamiento evaluando el cierre del plan de acción para cada riesgo.

De igual manera se desarrollaran actividades adicionales que van relacionadas con revisión de la ejecución de los controles de los riesgos como lo son mantenimiento de equipos, auditorias de proceso, pruebas a los dispositivos implementados, etc….; adicional para monitorear las medidas de prevención del riesgo se desarrollarán pruebas de vulnerabilidad en formato FT-GOP-29 de acuerdo al cronograma de ejecución de las mismas conforme lo estipulado en matriz FT-GOP-35 Cronograma de pruebas de vulnerabilidad.

* 1. **COMUNICACIÓN Y CONSULTA**

Los planes de control del riesgo son divulgados a los interesados (asociados de negocio) para la ejecución, seguimiento y control, para clientes se remite en formato de Seguimiento de recomendaciones de seguridad FT-GOP-04, en caso que se deba remitir recomendaciones de seguridad o notificación de actividades a proveedores, contratista y subcontratistas se remitirá a través de Memorando FT-GDE-11, para trabajadores directos de la empresa se remitirá copia de la matriz de identificación con sus debidas actualizaciones a los líderes de procesos a nivel nacional para que deleguen las respectivas actividades a cada colaborador.

* 1. **PLANES DE CONTINGENCIA**

El Plan de contingencia establece las medidas a tomar con las indicaciones para actuar en caso de materialización de un riesgo en las diferentes etapas (antes, durante y después).

La formulación de planes de contingencia es aplicable para aquellos riesgos en los cuales se decidió “Asumir el riesgo” y por ende se tienen identificados y valorados, y la descripción para los riesgos en general se establece en formato FT-GOP-30 Planes de contingencia.

1. **DOCUMENTOS ASOCIADOS**

FT-GOP-27 IDENTIFICACION Y VALORACION DE RIESGOS

FT-GOP-28 CONTROL Y SEGUIMIENTO TRATAMIENTO DEL RIESGO

FT-GOP-29 PRUEBAS DE VULNERABILIDAD

FT-GOP-30 PLANES DE CONTINGENCIA

FT-GOP-35 CRONOGRAMA PRUEBAS DE VULNERABILIDAD

1. **MEDICIÓN**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NOMBRE** | **INDICADOR** | **RESPONSABLE** | **FRECUENCIA** | **META** |
| Gestión de riesgos | Clientes con Nivel de riesgo Muy alto y/o alto  ---------------------------------------------------x 100  Total de clientes valorados | Analista de riesgos / Gerente sucursal | Trimestral | <=40% |

1. **CONTROL DE CAMBIOS**

|  |  |  |
| --- | --- | --- |
| **VERSIÓN** | **FECHA** | **CAMBIO** |
| 1 | /2017 | Reestructuración total del procedimiento, Cambio de logo y modificación de código- |