POLÍTICA DE MANEJO DE RIESGOS OPERATIVOS

PROPÓSITO

Identificar, analizar y evaluar los riesgos y las amenazas que potencialmente pueden impactar negativamente las actividades operativas y estratégicas de la Fundación Mejorhabitat, verificar los controles existentes en los desplazamientos de personal directivo, administrativo y operativo, así como la seguridad física de la sede y los procedimientos administrativos de la Fundación, que puedan influir positiva o negativamente en la seguridad. Analizarlos y evaluarlos para determinar el nivel del Riesgo Absoluto y el nivel del Riesgo con Control, para gestionar cambios o ajustes en los mismos.

ALCANCE

Esta política contempla los riesgos estratégicos, financieros, operativos y de corrupción para todos los empleados de la Fundación en sus funciones relacionadas con el Riesgo Operativo (RO).

OBJETIVO

Contribuir al aseguramiento del cumplimiento de la misión, la visión y los objetivos institucionales y la erradicación de la posibilidad de lesionar los intereses de la entidad a causa de la obtención de beneficios particulares.

OBJETIVOS ESPECIFICOS

- Establecer, formalizar y poner en práctica una metodología integral para la gestión del riesgo.
- Definir y establecer el nivel aceptable de los riesgos.
- Contar con la aprobación explícita de los planes de mitigación de los riesgos.
- Realizar evaluaciones periódicas de los procedimientos en uso para el control de los riesgos.
- Mantener informadas a las partes involucradas sobre el estado y el perfil de riesgos de la Fundación.

RESPONSABLE

La política debe ser aplicada por toda la Fundación. Los lineamientos, principios y definiciones que se mencionan a continuación y el manual de gestión a usar que se explica más adelante, constituyen la base sobre la cual aplica la Política de Gestión de Riesgos.

POLITICA

Los riesgos surgen tanto de la amenaza de que algo no deseado ocurra, como de que algo bueno no ocurra. El riesgo es un aspecto inseparable y debe ser adecuadamente administrado y gestionado, siendo por ello necesario analizar y considerar la existencia de condiciones, situaciones o eventos que pueden desencadenarse y resultar en consecuencias negativas para la Fundación, sus empleados, el medio ambiente y la comunidad. Los principios mencionados aplican sobre todos los ámbitos del quehacer operativo, financiero, de proyectos, medioambiental, recursos humanos, salud y seguridad de empleados y contratistas, legal y regulatorio y en temas relacionados con la comunidad, de reputación y sociales. La Fundación debe contar con políticas de riesgo y con un sistema de gestión y control integral de ellos. Para estos efectos, deben establecer el análisis de alto nivel de los riesgos estratégicos que pueden afectarlos y la asignación de recursos para una adecuada ejecución de las acciones de mitigación según la naturaleza, complejidad, las operaciones y las actividades. La gerencia tiene la responsabilidad de desarrollar y aplicar las políticas y procedimientos necesarios para una adecuada gestión y el control de riesgos. Aplicar medidas de control o de mitigación que permiten mantener la exposición a un nivel aceptable. Tanto la metodología aplicada como el resultado de la evaluación de los riesgos deben ser conocidos y comunicados a los ejecutivos de la Fundación con el objeto de que ellos aporten en la identificación de los riesgos y en el desarrollo e implementación de planes de mitigación.

DEFINICIONES:

- Riesgo se define como la incertidumbre resultante de la posible ocurrencia de un evento que puede impactar en forma negativa al cumplimiento de los objetivos de la Fundación. Al ser una definición tan amplia, es necesario analizar la forma de identificarlos en su dimensión general, para posteriormente acotarlos según el tipo de negocio, de Fundación, de ambiente, de estructura y cultura organizacional.

Riesgo Operativo (RO): Se entiende por Riesgo Operativo, la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el Riesgo Legal y Reputacional, asociados a tales factores.

- Riesgo Legal: Es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales. El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

- Riesgo Reputacional: Es la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

- Perfil De Riesgo: Resultado consolidado de la medición permanente de los riesgos a los que se ve expuesta la entidad.

- Actores De Riesgo: Se entiende por factores de riesgo, las fuentes generadoras de riesgos

operativos que pueden o no generar pérdidas. Son factores de riesgo el recurso humano, los procesos, la tecnología, la infraestructura y los acontecimientos externos. Dichos factores se deben clasificar en internos o externos, según se indica a continuación.

Internos

• Recurso Humano: Es el conjunto de personas vinculadas directa o indirectamente con la ejecución de los procesos de la entidad. Se entiende por vinculación directa, aquella basada en un contrato de trabajo en los términos de la legislación vigente. La vinculación indirecta hace referencia a aquellas personas que tienen con la entidad una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo.

• Procesos: Es el conjunto interrelacionado de actividades para la transformación de elementos de entrada en productos o servicios, para satisfacer una necesidad.

• Tecnología: Es el conjunto de herramientas empleadas para soportar los procesos de la entidad. Incluye: hardware, software y telecomunicaciones.

• Infraestructura: Es el conjunto de elementos de apoyo para el funcionamiento de una Organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

Externos

Son situaciones asociadas a la fuerza de la naturaleza u ocasionadas por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

• Evento: Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.

• Eventos De Pérdida: Son aquellos incidentes que generan pérdidas por riesgo operativo a las entidades

CLASIFICACIÓN DE LOS RIESGOS OPERATIVOS

• Fraude Interno: Actos que de forma intencionada buscan defraudar o apropiarse indebidamente de activos de la entidad o incumplir normas o leyes, en los que está implicado, al menos, un empleado o administrador de la entidad.

• Fraude Externo: Actos realizados por una persona externa a la entidad, que buscan defraudar, apropiarse indebidamente de activos de esta o incumplir normas o leyes.

• Relaciones laborales: Actos que son incompatibles con la legislación laboral, con los acuerdos internos de trabajo y, en general, la legislación vigente sobre la materia.

• Clientes: Fallas negligentes o involuntarias de las obligaciones frente a los clientes y que

impiden satisfacer una obligación profesional frente a éstos.
• Daños a activos físicos: Pérdidas derivadas de daños o perjuicios a activos físicos de la entidad.

• Fallas tecnológicas: Pérdidas derivadas de incidentes por fallas tecnológicas

PROCEDIMIENTO- MANUAL PARA LA GESTIÓN DEL RIESGO OPERATIVO

Este Manual busca establecer los controles y las recomendaciones necesarias acerca del tratamiento del riesgo operativo y definir los criterios específicos para mitigar este tipo de riesgos teniendo en cuenta todos los aspectos de la Fundación.

Manual de Riesgo Operativo (MRO): Conjunto de elementos tales como políticas, procedimientos, documentación, estructura organizacional, registro de eventos de riesgo operativo, órganos de control, plataforma tecnológica, divulgación de información y capacitación, mediante los cuales la entidad identifica, mide, controla y monitorea el riesgo operativo.

Riesgo Inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Plan De Continuidad: Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

Plan De Contingencia (parte del Plan de Continuidad): Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso. INTEGRACION DEL

PERFIL DE RIESGO

Los principales elementos contenidos con respecto a Riesgo Operacional incluyen los siguientes aspectos:

• Establecer el contexto
• Identificar riesgos
• Analizar riesgos
• Evaluar los riesgos
• Tratar los riesgos
• Monitorear y revisar
• Comunicar y consultar

FUNDAMENTOS, MEDICION Y ADMINISTRACION DE RIESGOS OPERATIVOS

Etapa de Identificación de Riesgos Operativos: La Entidad clasifica, monitorea y administra los riesgos identificados en cada área.

A continuación, las principales áreas de medición:
• Identificación de Riesgos de Sistemas

- Identificación de Riesgos de Procesos
- Identificación de Riesgos de Recursos Humanos
- Identificación de Riesgos administrativos y financieros

Etapa de Medición de Riesgos Operativos: Para la medición cuantitativa de los riesgos operativos se realizará una evaluación basada en objetivos, modelo de riesgo específico y datos históricos de siniestros, teniendo como soporte una adecuada base de datos y personal capacitado.

Para realizar una eficiente medición cuantitativa de los riesgos, inicialmente se deben registrar los siniestros, bienes afectados, el daño ocasionado, la fecha, descripción del siniestro, el área donde se presentó y la persona que lo detectó. Toda esta información deberá estar registrada en una base de datos.

Monitoreo del Riesgo Operativo: Los riesgos de operaciones son responsabilidad de la Gerencia de Riesgos, y su responsable decide si los riesgos pueden ser afectados, registrados e informados a los Órganos directivos y Gerencia General, a través de los exámenes que realice la auditoría interna, auditoría externa y/o auditoria de sistemas.

NIVELES DE ACEPTACIÓN DEL RIESGO

La Fundación decide aceptar los riesgos cuando controlarlos implica mayores costos que asumir las consecuencias o impactos de la ocurrencia. La priorización para la gestión de los riesgos se definirá durante la fase de análisis; sí el análisis ubica los riesgos en nivel alto o extremo, el tratamiento deberá iniciarse obligatoriamente por parte del directo responsable. En los demás niveles la priorización es opcional.

NIVELES DE ACEPTACIÓN DEL RIESGO

La Fundación decide aceptar los riesgos cuando controlarlos implica mayores costos que asumir las consecuencias o impactos de la ocurrencia. La priorización para la gestión de los riesgos se definirá durante la fase de análisis; sí el análisis ubica los riesgos en nivel alto o extremo, el tratamiento deberá iniciarse obligatoriamente por parte del directo responsable. En los demás niveles la priorización es opcional.

ESTRATEGIAS PARA EL DESARROLLO DE LA POLÍTICA

Socialización, involucramiento por niveles, documentación, integración en los procesos naturales de planeación.

MATRIZ DE RIESGOS

La clasificación de cada riesgo corresponde a la combinación del impacto generado por la ocurrencia del evento con la probabilidad de ocurrencia definida. (Tabla en Excel)

RESUMEN DE LOS POSIBLES RIESGOS IDENTIFICADOS RIESGO DE SISTEMAS

• Guardar la información en los escritorios de los PC y no en el servidor y en la carpeta indicada para cada una de las áreas.
• Duplicar la información en discos externos y no actualizar la información en el servidor
• Jaqueo de la información
• Perdida de la información de interés y no posibilidad de recuperarla
• No hacer soporte externo (backup) de la información (disco, nube)
• Cada una de las personas servidoras de la empresa se crea dueña y propietaria de la información que produce.
• Que no se tengan establecidos controles para el manejo de la información, quién administra, modifica, guarda y respalda la información.
• Maquinas obsoletas, que además no se les hace mantenimiento.
• No renovación de equipos y licencias. RIESGO DE PROCESOS
• No se tienen procesos para el desarrollo de cada una de las actividades y acciones de la organización.
• Se tiene, pero nadie los conoce porque no son socializados a las personas que prestan los servicios en la organización.
• Se tiene, pero no son aplicados por las personas de la organización.
• Todos las hacen de la forma que creen es más conveniente, no hay control.
• No hay un administrador y controlador de los procesos.
• No existe sistema de gestión de la calidad

RIESGO DEL RECURSO HUMANO

• No existe un área que se encargue de la administración del recurso humano.
• No se tiene manual de funciones, o no es conocido por las personas que hacen parte de la organización.
• Que no se realicen contratos de acuerdo con la calidad en la que se contrate (laboral, servicios, suministros).

RIESGO FINANCIERO Y ADMINISTRATIVO

• Existe un manual o protocolo para la operación administrativa y financiera pero no aplica.
• No se aplican tiempos para realizar las labores administrativas.
• No se respalda la información contable y administrativa.
• No se hace control permanente a la administración y operación financiera.
• No se realiza revisoría fiscal de manera permanente.

PREVENCIÓN, MITIGACIÓN Y ELIMINACIÓN DE LOS POSIBLES RIEGOS IDENTIFICADOS RIESGOS DE SISTEMAS

• Realizar backup a toda la información de la organización, ya sea en discos externos o en la nube.

- Realizar soporte y mantenimiento permanente el servidor
- Tener los servicios técnicos de sistemas, ya sea externo o interno para el buen funcionamiento del área de sistemas.
- Renovación permanente de los equipos y licencias empresariales
- Implementación del proceso de sistemas de la información, para que todas las personas de la organización manejen de manera adecuada la información.
- Establecer los controles en el manejo de la información (quién o quiénes son administradores, operativos y controladores), así mismo el nivel de manejo de la información por parte de cada una de las personas, permisos para cambiar, modificar, eliminar y guardar la información.
- En caso de jaqueo tener la capacidad de reaccionar de manera inmediata. Pero, además, tener la información asegurada.

RIESGO DE PROCESOS

- Establecer un sistema de gestión de la calidad, en los que se identifiquen los procesos por cada una de las áreas.
- Socializar con todo el personal este manual y crear los comités de seguimiento y control, que permitan la adecuada implementación del sistema.
- Nombrar un administrador del sistema.

RIESGO DEL RECURSO HUMANO

- Tener un responsable del área para que administre, haga seguimiento y control.
- Tener manual de funciones, que sea, además, socializado con todas personas que laboran en la organización.
- Llevar control de los diferentes contratos que se desarrollan en la organización. Vigilando que se documenten de la debida manera.
- Guardar y custodia de la información de hojas de vida y contratos de la organización.

RIESGO FINANCIERO Y ADMINISTRATIVO

- Se tiene un manual de procedimientos y protocolos para la implementación de las tareas administrativas y financieras.
- Se tienen establecidos controles para la realización de las actividades administrativas y financieras.
- Se tiene un sistema contable, en el cual se registran todas las operaciones financieras de la organización.
- Se realizan de manera permanente balances para revisar y hacer seguimiento a las actividades administrativas y financieras.
- Se realiza revisión fiscal (administrativa, financiera, sistemas y recurso humano)
- Se realizan autorías internas por parte de los cooperantes (públicos o privados)
- Se realizan de manera oportuna todos los pagos de impuestos establecidos por la ley.

• Se realizan informes periodos que se presentan a la dirección general, para la toma de decisiones.

SOCIALIZACIÓN

La Fundación, socializa con el equipo de trabajo, los riegos potenciales identificados y revisa de manera conjunta la manera de prevenirlos, mitigarlos o eliminar su ocurrencia. De modo, que no se afecte la organización.

Estas socializaciones, permiten la implicación de todo el equipo de trabajo, no solo de la dirección de la organización.

La organización reconoce la importancia de la planeación, y en especial la planeación participativa, que involucra a cada una de las personas que hacen parte de la organización, trabajando con un enfoque diferencial y de género.

La Fundación, reconoce la importancia de tener una política de riesgos, por ello, la aplica y la socializa con las personas que hacen parte de ella.

POLÍTICA DE MANEJO DE ARCHIVO DE DOCUMENTOS

OBJETIVO

Controlar la gestión de documentos a lo largo de su ciclo de vida, asegurando el acceso, seguridad, disponibilidad, confidencialidad y conservación de la documentación recibida y producida por la Fundación Apego.

ROLES Y RESPONSABILIDADES

Dirección Ejecutiva: orienta y dirige la implementación de la política de archivo de la Fundación Apego.

Coordinación de Proyectos: se encarga de supervisar el proceso de gestión documental.

Coordinador de proyecto: organiza y entrega a la coordinación administrativa los documentos relacionados con el desarrollo técnico del proyecto a su cargo para su debida ubicación en el archivo.

Coordinación Administrativa: responde por el manejo operativo del archivo, recibe y ubica el documento en la carpeta correspondiente, asegura el acceso de los funcionarios a la información con criterios de seguridad y confidencialidad. Se preocupa por la conservación de la documentación.

PROCESO DE GESTIÓN DOCUMENTAL

Planeación: comprende el conjunto de actividades encaminadas a la planeación, generación y

valoración de los documentos de la entidad, en cumplimiento del contexto administrativo, funcional y técnico.

Producción: se refiere a las actividades destinadas a la producción de los documentos, su formato, estructura, finalidad y área de competencia.

Gestión: conjunto de actuaciones necesarias para el registro, la descripción, la disponibilidad, recuperación de los documentos y elementos del archivo.

Organización: conjunto de operaciones técnicas para declarar el documento en el sistema de gestión documental, clasificarlo, ubicarlo en el nivel adecuado, ordenarlo y describirlo adecuadamente.

MANEJO OPERATIVO DEL ARCHIVO

El manejo operativo del archivo se compone de las siguientes actividades:

- Recepción de documentos: la coordinación administrativa recibe los documentos bien sea por correspondencia urbana o a través de la Dirección Ejecutiva, o Coordinación de Proyectos. Así mismo lleva un control e inventario de documentos mediante un formato institucional. (Anexo 1. Formato de Control e Inventario de Documentos)

– Clasificación: la coordinación de proyectos y/o coordinación temática revisan la documentación recibida y orientan a la coordinación administrativa para ubicar la documentación según las categorías de valoración documental y archivo virtual.

- Organización de documentos en archivo físico o virtual: comprende la ubicación de documentos físicos o virtuales en el espacio establecido.

- Actualización y limpieza de documentos: cada seis meses la coordinadora administrativa con la supervisión de la coordinadora de proyectos revisará la documentación existente de uso frecuente y aquella que tenga terminada su vigencia para determinar si se conserva o se elimina.

- Reemplazo de carpetas: con la actualización y limpieza, la coordinadora administrativa identificará la necesidad de remplazar carpetas bien sea en su titulación o por desgaste de uso y solicitará en Comité administrativo el cambio o compra de nuevas capetas.

VALORACIÓN DOCUMENTAL

La valoración documental es orientada por la Directora Ejecutiva, Coordinación de Proyectos y Coordinadora Temática, teniendo en cuenta la selección de los documentos en cualquier etapa del archivo, con miras a su conservación temporal, permanente o a su eliminación, teniendo en cuenta que existen tres tipos de archivo:

Archivo de gestión: se refiere a la documentación activa como información administrativa, contable y de proyectos con vigencia anual.

Archivo central: comprende la documentación semi-activa o poco frecuentada, como documentos legales de constitución de la organización y datos de consulta de proyectos y/o información contable del año recientemente anterior.

Archivo Histórico: esta categoría se entiende como la documentación inactiva, es decir documentos legales, administrativos y contables de los últimos 5 años, publicaciones y otros productos de proyectos (videos, guías, manuales).

ORGANIZACIÓN DE ARCHIVO VIRTUAL

La fundación Mejorhabitat cuenta con un servidor en red y organiza el archivo digital de la siguiente manera:

Archivo financiero y contable: comprende documentación relacionada con la planeación financiera (presupuesto institucional anual, planes de adquisición por proyecto), declaración de impuestos, informes contables, y soportes. También incluye antecedentes disciplinarios del Revisor Fiscal y Contador, extractos bancarios, conciliaciones bancarias y certificaciones parafiscales.

Para efectos de organización de soportes contables como comprobantes de egreso y facturas Siigo cuenta con dos herramientas digitales: Word Office y Dropbrox, los cuales hacen parte de esta categoría.

El manejo de esta información es exclusiva de la Dirección Ejecutiva, Coordinación de Proyectos, Coordinación Administrativa y Contadora. Por tal razón la carpeta creada para este tipo de archivo tiene permisos especiales de acceso.

Archivo legal: contiene documentos relacionados con la constitución de la Fundación, Estatutos y enmienda a los estatutos, registró actualizado ante la cámara de comercio, resoluciones emitidas por entidades públicas para el reconocimiento de personería jurídica, registro único tributario, actas del Consejo Directivo, documento de miembros del Consejo Directivo y sus cartas recientes de aceptación de los cargos, documentos del representante legal y debidas certificaciones de antecedentes judiciales y disciplinaros.

Archivo administrativo: bajo esta nominación se organizan las políticas institucionales, manuales de procesos y procedimientos, directorio de proveedores y prestadores de servicios, términos de referencia para procesos de contratación contratos, cotizaciones, actas de comités administrativos, soportes de proveedores y consultores, correspondencia, certificados de cumplimiento de contratos y actas de liquidación. Certificaciones laborales e inventarios de activos.

Archivo de proyectos: en esta categoría se ubican documentos relacionados con la formulación, planificación, ejecución y evaluación de los proyectos. A su vez se organizan subcarpetas por proyecto que incluyen la propuesta, plan de trabajo o plan operativo, documentos técnicos para atención a la población participante, guías, presentaciones en power point, directorios de equipo

de trabajo, informes de proceso, informe técnico final y soportes de la ejecución.

Archivo de comunicaciones: comprende la organización de documentos para la visibilización y posicionamiento institucional y de las líneas de trabajo de la Fundación Mejorhabitat. Documentos técnicos, piezas digitales, directorios de comunicaciones, y de administración de las redes sociales.

Entre estos documentos se encuentran: manual de imagen corporativa, protocolo de convocatorias y de eventos, logos institucionales, piezas de comunicación como pendones, folletos, boletines, gorras, camisetas, banco de imágenes, bases de contactos corporativos, informes de gestión, invitaciones, tarjetas, rutas de acceso y algoritmos para la administración de página web y redes sociales.

Archivo de aliados: agrupa información relacionada con instituciones aliadas que facilitan procesos de incidencia social y de política pública en temas relacionados con la misión institucional. Bajo esta clasificación se organizan convenios, soportes legales de aliados, logos institucionales, propuestas conjuntas, documentos técnicos de incidencia, certificaciones de participación en eventos.

CHRISTIAN GIANI JIMÉNEZ BECERRA
Representante Legal
FUNDACIÓN MEJORHABITAT
NIT. 805.016.076-1
gerencia@fundacionmejorhabitat.org