PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN AÑO 2019
FONDO DE VIVIENDA DE INTERÉS SOCIAL Y REFORMA URBANA DISTRITAL- CORVIVIENDA

Dir: Manga 3ª Avenida, Calle 28 #21-62
Email: info@corvivienda.gov.co
wwww.corvivienda.gov.co
Tel: 6445429 - 6445074

DIRECTIVOS CORVIVIENDA

ÉRICA BARRIOS BLANQUICETH	Gerente
JOSE UTRIA MONSALVE	Director Administrativo
MIGUEL RAMÓN MÉNDEZ PAREDES	Director Técnico
NATACHA GONZALEZ VALLEJO	Jefe Oficina Asesora de Planeación
ISABEL DIAZ MARTINEZ	Jefe Oficina Asesora de Jurídica
JAVIER ERNESTO CAMACHO DIAZ	Jefe Oficina de Control Interno

_____

Aprobó: ÉRICA BARRIOS BLANQUICETH **Gerente**
Revisó: NATACHA GONZALEZ VALLEJO **Jefe Oficina Asesora Planeación**
Elaboró: ISSI TUÑON ARROYO **Contratista**
.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

1. INTRODUCCIÓN

Con el avance de las nuevas tecnologías nos encontramos frente a nuevos retos y desafíos, los cuales deben ser afrontados por las empresas que se encuentran inmersas en la denominada revolución digital, es necesario que se reconozca el protagonismo de la información en los procesos productivos, por tanto la importancia de tener la información adecuadamente identificada y protegida, como también la proporcionada por las partes interesadas, enmarcada bajo las relaciones de cumplimiento, comerciales y contractuales como los son acuerdos de confidencialidad y demás compromisos, que obligan a dar un tratamiento, manejo y clasificación a la información bajo una correcta administración y custodia.

La Seguridad de la Información en las empresas tiene como objetivo la protección de los activos de información en cualquiera de sus estados ante una serie de amenazas o brechas que atenten contra sus principios fundamentales de confidencialidad, integridad y su disponibilidad, a través de la implementación de medidas de control de seguridad de la información, que permitan gestionar y reducir los riesgos e impactos a que está expuesta y se logre alcanzar el máximo retorno de las inversiones en las oportunidades de negocio.

Administración de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

Los principios de protección de la información se enmarcan en:

- **Confidencialidad**: Propiedad que la información sea concedida únicamente a quien esté autorizado.
- **Integridad**: Propiedad que la información se mantenga exacta y completa.

- **Disponibilidad**: Propiedad que la información sea accesible y utilizable en el momento que se requiera.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

1.2. OBJETIVOS ESPECÍFICOS

- Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas de seguridad de la información que estén acordes al entorno operativo de la Entidad.
- Proteger el valor de los activos de información mediante el control de implementación de acciones de mitigación frente al riesgo y potencializar las oportunidades asociadas.
- Lograr y mantener a través de la implementación de medidas de control el nivel de probabilidad e impacto residual de los riesgos a el nivel aceptable por parte de la Alta Gerencia.
- Concientizar a todos los trabajadores y/o colaboradores, áreas, procesos, proveedores, externos en general sobre la necesidad e importancia de gestionar de manera adecuada, los riesgos inherentes a la gestión.
- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

2. ALCANCE

Esta guía, proporciona la metodología establecida por la Entidad para la administración y gestión de los riesgos a nivel de procesos; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

La gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la Entidad, a cualquier sistema de información o aspecto particular de control de ésta, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación.

3. TÉRMINOS Y DEFINICIONES

A continuación, se presentan algunos términos y definiciones de términos que se utilizarán durante el desarrollo de la gestión de riesgos de seguridad de la información.

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento de valor para los procesos de la Organización.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Causa: Son todo aquello que se pueda considerar fuente generadora de eventos (riesgos). Las fuentes generadoras o agentes generadores son las personas, los métodos, las herramientas, el entorno, lo económico, los insumos o materiales entre otros.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.
Criterios del riesgo: Términos de referencia frente a los cuales la importancia de un riesgo se evaluada.

Control: Medida que modifica el riesgo.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo, se compone de la evaluación y el tratamiento de riesgos.

Identificación del riesgo. Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de las consecuencias y su posibilidad.

Matriz de riesgos: Instrumento utilizado para ubicar los riesgos en una determinada zona de riesgo según la calificación cualitativa de la probabilidad de ocurrencia y del impacto de un riesgo.

Monitoreo: Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de con trol o las diferentes auditorías de los sistemas integrados de gestión.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Proceso: Conjunto de actividades interrelacionadas o que interactúan para transformar una entrada en salida.

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

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo en la seguridad de la información. Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación n de los controles de seguridad de la información sobre cada uno de los procesos.

Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información.

4. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

Dirección: Aprueban las directrices para la administración del riesgo en la Entidad. La Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

Proceso Administración del Sistema Integrado de Gestión: Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año. Si bien los Líderes SIG apoyan la ejecución de las etapas de gestión del riesgo a nivel de los procesos, esto no quiere decir que el proceso de administración de riesgos este solo bajo su responsabilidad. Al contrario, cada responsable de proceso se encarga de garantizar que en el proceso a su cargo se definan los riesgos que le competen, se establezcan las estrategias y responsabilidades para tratarlos y, sobre todo, que se llegue a cada funcionario que trabaja en dicho proceso. No se debe olvidar que son las personas que trabajan en cada uno de los procesos los que mejor conocen los riesgos existentes en el desarrollo de sus actividades.

Servidores públicos y contratistas: Ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

Control Interno: Debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

5. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

CORVIVIENDA adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo, y para ello todos los servidores de la entidad se comprometen a:

- Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.
- Fortalecer la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.
- Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.
- Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
- Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.
- Desarrollar e implementar planes de contingencia para asegurar la continuidad de los procesos, en los eventos de materialización de los riesgos que afecten a los objetivos institucionales previstos y los intereses de los usuarios y partes interesadas.
- Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Dirección asignará los recursos tanto humanos, presupuestales y tecnológicos necesarios que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, la presente guía forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del riesgo en la entidad y que tienen como propósito evitar la materialización del riesgo.

6. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegaran los aspectos conceptuales y operativos que se deben tener en cuenta.

Contexto estratégico: Determinar los factores externos e internos del riesgo.

Identificación: identificación de causas, riesgo, consecuencias y clasificación del riesgo.

Análisis: Calificación y evaluación del riesgo inherente.

Valoración: identificación y evaluación de controles; incluye la determinación del riesgo residual.

Manejo: Determinar, si es necesario, acciones para el fortalecimiento de los controles.

Seguimiento: Evaluación integral de los riesgos.

7. ANÁLISIS CONTEXTO ESTRATÉGICO

Definir el contexto estratégico contribuye al control de la entidad frente a la exposición al riesgo, ya que permite conocer las situaciones generadoras de riesgos, impidiendo con ello que la entidad actúe en dirección contraria a sus propósitos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión, de manera que se perciba la administración del riesgo como una herramienta gerencial y no como algo aislado del accionar administrativo. Por lo tanto, el diseño de esta primera etapa, se fundamenta en la identificación de los factores internos (debilidades) y externos (amenazas) que puedan generar riesgos que afecten el cumplimiento de los objetivos institucionales.

Esta etapa es orientadora, se centra en determinar las amenazas y debilidades de la entidad; es la base para la identificación del riesgo, dado que de su análisis suministrará la información sobre las CAUSAS del riesgo.

8. DESARROLLO PRÁCTICO – CONTEXTO ESTRATÉGICO

Tomando como referente lo anterior, se debe atender y seguir las siguientes orientaciones:

- Cada responsable de proceso del Sistema Integrado de Gestión, deberá identificar a los funcionarios que por su competencia pueden ser considerados claves dentro de cada una de las dependencias que participan en el proceso, serán factores de selección de estos, el conocimiento y nivel de toma de decisiones sobre el proceso.

- Los funcionarios seleccionados deberán ser convocados a una reunión inicial, en donde se presentará el propósito de esta actividad .

- Se establecerán los factores internos y externos que afectan el proceso, para esto, se debe diligenciar el formato Matriz DOFA para identificación de riesgos:

1.1.1.1 Tabla 1. Matriz DOFA para identificación de riesgos

	MATRIZ DOFA PARA IDENTIFICACIÓN DE RIESGOS		
PROCESO:			
OBJETIVO:			
FECHA:			
DEBILIDADES	**FUENTE**	**AMENAZAS**	**FUENTE**

Para diligenciar la matriz anterior, y como parte introductoria se deberá informar a los asistentes: la dependencia a la cual corresponde el proceso y el objetivo (se debe presentar indicando que se hace, cual es el mediante y la finalidad). Con esta información, se identificarán las posibles debilidades como:

- La administración, la estructura organizacional, las funciones y las responsabilidades.
- Las políticas, los objetivos y las estrategias que existen para su realización.

- Las capacidades, entendidas en términos de recursos y de conocimiento (humanos, de capital, tiempo, personas, infraestructura, procesos, sistemas y tecnologías).

- Los sistemas de información y comunicación, flujos de información formales e informales y toma de decisiones.

- Las normas, directrices y modelos adoptados por la organización.

- La forma y el alcance de las relaciones contractuales.

Las debilidades deberán ser expresadas con términos similares a estos

- Ausencia de….
- ... obsoletos
- Falta….
- ….insuficientes
- Disminución de…
- Fallas de….

Este tipo de palabras no necesariamente deben aparecer al inicio de la idea, ejemplo: número equipos de cómputo **obsoletos.**

Nota: Se recomienda que las ideas, en lo posible, se soporten de experiencias, registros y demás, por eso en el cuadro relacionado se establece una columna denominada “Fuente”, en caso que la idea cuente con una fuente se colocará tal y como aparece a continuación, en caso contrario se dejará no aplica (N/A).

Debilidad	**Fuente**
Falta de respeto entre compañeros	Estudio de Clima Laboral

Posteriormente, se articularán las ideas afines de la siguiente manera:

Es importante destacar que no todas las ideas tendrán afinidad y se conservarán como fueron establecidas en la lluvia de ideas; después de articular y organizar las ideas, se debe identificar a que factor corresponde cada idea, como se muestra en el siguiente ejemplo:

Ideas	**Factores internos**
Número de equipos insuficiente	Tecnología y sistemas de información
Desconocimiento de la normatividad aplicada	Talento Humano
Proceso manual	Modelo de Operación
Desmotivación	Talento Humano
Fallas en el seguimiento a los procedimientos del proceso	Modelo de Operación
Equipos obsoletos	Talento Humano
Resistencia al cambio	Talento Humano
Bajo presupuesto de inversión	Financiero

Se consideran factores internos:

- Dirección
- Estructura organizacional
- Comunicación Interna
- Normativo
- Tecnología y sistemas de Información
- Talento humano
- Ético
- Clima Organizacional
- Infraestructura
- Financiero
- Operativo

- Insumos e información
- Modelo de operación
- Mecanismos de Control

Una vez se tengan identificados los factores internos, se debe diligenciar el formato Contexto Estratégico:

1.1.1.2

1.1.1.3 Tabla 2. Contexto Estratégico

	CONTEXTO ESTRATÉGICO		
PROCESO:			
OBJETIVO:			
FECHA:			
FACTORES INTERNOS	**CAUSAS**	**FACTORES EXTERNO**	**CAUSAS**

En la primera parte, se diligenciarán los factores internos a los cuales se les vincularán las causas, estas corresponderán a las ideas que salieron del análisis y agrupación por afinidad de las debilidades y que dieron origen a los factores. A continuación presentamos un ejemplo:

1.1.1.4 Tabla 3. Contexto Estatégico - Causas

	CONTEXTO ESTRATÉGICO		
PROCESO:			
OBJETIVO:			
FECHA:			
FACTORES INTERNOS	**CAUSAS**	**FACTORES EXTERNO**	**CAUSAS**
Tecnología	• Equipos insuficientes • Equipos obsoletos		

	CONTEXTO ESTRATÉGICO		
Procesos	• Ausencia de políticas de operación • Proceso manual • Fallas en el seguimiento a los procedimientos del proceso		
Talento Humano	• Desconocimiento de la normatividad aplicada • Desmotivación • Resistencia al cambio		
Sistemas de información	• Información desactualizada		
Medición	• Los indicadores no miden nada		
Financiero	• Bajo presupuesto de inversión		

Definidos los factores internos, se procede a identificar los factores externos, para ello deben ser identificadas las amenazas. Mediante lluvia de ideas se identifican los aspectos del entorno, para este caso puntual, no existe una regla específica de redacción, sin embargo tendrán el mismo tratamiento de las debilidades, es decir afinidad por agrupación, generando como resultado un listado como:

- Nueva tecnología disponible
- Nuevas leyes
- Demoras en la respuesta de comunicaciones enviadas por otras entidades
- Incremento en el número de solicitudes por alta demanda de usuarios
- Cambio de Gobierno
- Poco conocimiento por parte de la ciudadanía

- Adaptación a normatividad internacional

Con el listado de estas ideas, se debe identificar el factor externo al cual perteneces cada idea:

Se consideran factores externos:

- Interinstitucional
- Político
- Económico
- Ambiental
- Social
- Tecnológico
- Cultural
- Legal
- Imagen
- Entre otros

Con esta información, se procede a complementar el formato Contexto Estratégico, en lo correspondiente a factores externos:

1.1.1.5 Tabla 4. Contexto Estratégico – Factores Externos

	CONTEXTO ESTRATÉGICO		
PROCESO:			
OBJETIVO:			
FECHA:			
FACTORES INTERNOS	**CAUSAS**	**FACTORES EXTERNO**	**CAUSAS**
Tecnología y sistemas de información	• Equipos insuficientes	Tecnológico	• Nuevo tecnología

Corvivienda	**CONTEXTO ESTRATÉGICO**		
	• Equipos obsoletos		disponible.
Modelo de operación	• Ausencia de políticas de operación • Proceso manual • Fallas en el seguimiento a los procedimientos del proceso	Legal	• Nuevas leyes • Adaptación a normatividad internacional
Talento Humano	• Desconocimiento de la normatividad aplicada • Desmotivación • Resistencia al cambio	Interinstitucional	Demoras en la respuesta de comunicaciones enviadas por otras entidades
Tecnología y sistemas de información	• Información desactualizada	Social	Incremento en el número de solicitudes para alta demanda de usuarios
Mecanismos de control	• Los indicadores no miden nada	Político	Cambio de gobierno

En conclusión, los resultados de esta etapa son:

- Identificar los factores internos que pueden ocasionar la presencia de riesgos.
- Identificar los factores externos que pueden ocasionar la presencia de riesgos, con base en el análisis de la información externa y los planes y programas de la entidad.
- Aportar información que facilite y enriquezca las demás etapas de la Administración del Riesgo.

Conocidos los factores generadores de riesgo y dado por entendido que la Administración del Riesgo es un trabajo en equipo liderado y motivado constantemente por la Alta Dirección, se continúa con la identificación del riesgo.

9. IDENTIFICACIÓN DE RIESGOS

Es la etapa que permite conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo las causas y los efectos de su ocurrencia". Adicionalmente, en esta etapa también se realiza la clasificación del riesgo.

1.1.1.6 Tabla 5. Identificación de Riesgos

Causas Son los medios o circunstancias	**+**	**Riesgos Evento que tendrá un impacto**	**+**	Consecuencia Efecto que se puede presentar	+	Clasificación De acuerdo a las características	**=**	Identificación del Riesgo
Descripción a adecuada de los Riesgos								Resultado esperado

En este paso se identifican los riesgos institucionales y por procesos que la organización debe gestionar. Esta identificación se realiza con base en el Contexto Estratégico, definido en el paso anterior.

9.1. COMPONENTES DE LA IDENTIFICACIÓN DEL RIESGO

9.1.1. Causas del riesgo. Son las causas, uno de los aspectos a eliminar o mitigar para que el riesgo no se materialice; esto se logra mediante la definición de controles efectivos. Para realizar el análisis de las causas existen varias técnicas que serán analizadas a continuación.

Lluvia de ideas: Usualmente se utiliza la técnica de lluvia de ideas para identificar todo aquello que puede ser considerado dentro del análisis de riesgos y para que esta sea eficaz, se debe considerar que:

- Debe haber un moderador que tome nota y que organice las exposiciones de todos los participantes, indicando el tiempo que cada cual tiene para presentar sus ideas.
- Es más importante la cantidad de ideas que la calidad de las mismas. Todas las ideas son valiosas para el proceso de recopilación de información.
- No se deben calificar las ideas como buenas o malas, son simplemente puntos de vista que capitalizados pueden brindar alternativas no consideradas.
- Es importante soportarse en las ideas de los otros. Es decir, agregar valor a las apreciaciones de otros o considerar situaciones a partir de las mismas.

- El análisis de las ideas se debe realizar al final, por el moderador, quien las organizará y las expondrá a manera de resultado.
- Todos deben participar de manera equitativa, es importante no fijar la atención en pocos participantes, ni mantenerse en la palabra sin dar la oportunidad a otro de expresar sus ideas.

Diagrama Causa-efecto (Espina de pescado): Es un método que permite visualizar de manera estructurada todas las causas posibles del riesgo mediante el análisis desde los factores generadores de riesgo.

9.1.2. **Consecuencias.** Son los efectos que se generan o pueden generarse con la materialización del riesgo sobre los objetivos de los procesos y de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Se deben determinar las consecuencias del riesgo en escala ascendente; definiendo cual podría ser el efecto menor que puede causar la materialización del riesgo hasta llegar al efecto mayor generado.

9.1.3. **Clasificación de los Riesgos.** Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riego mediante la definición de controles y planes de manejo:

1.1.1.7 Tabla 6. Clasificación de los riesgos.

Clases de riesgo	**Definición**
Estratégico	Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Operativo	Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias.
Financieros	Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes.
Cumplimiento	Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad.
Tecnología	Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión.
Imagen	Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad.

10. ESTRUCTURA ADECUADA DE LA IDENTIFICACIÓN DEL RIESGO

La identificación del riesgo no se puede realizar de manera fragmentada; debe existir una relación total entre las causas identificadas, el riesgo y las consecuencias que podrían presentarse producto de la materialización; para evitar confusiones y definir articuladamente todos los componentes de la identificación del riesgo se establece un método apropiado que consiste en el uso del metalenguaje del riesgo para una identificación estructurada en tres partes:

Debido a	**Podría ocurrir**	**Lo que podría generar**
Una o más causa	Riesgo	Uno o más consecuencia
		

El metalenguaje pretende asegurar que se identifiquen correctamente causas, riesgos y consecuencias, sin confundir unas con otras; de no ser así, los pasos posteriores quedan viciados de error.

Ejemplo:

Debido a	**Podría ocurrir**	**Lo que podría generar**
Manejar con excesiva velocidad	Un accidente	Lesiones personales.

10.1. DESARROLLO PRÁCTICO – IDENTIFICACIÓN

De acuerdo con la etapa de Contexto Estratégico, se retomarán las ideas establecidas para cada uno de los factores internos y externos, las cuales se utilizarán para determinar las causas del riesgo identificado; posteriormente, se debe describir el riesgo y las posibles consecuencias de su materialización.

Esta información, se debe registrar en el formato Metalenguaje del riesgo (Cuando se estén construyendo los componentes de identificación) y posteriormente, diligenciar el formato de identificación de riesgos (Cuando se tenga toda la información depurada).

1.1.1.8 Tabla 7. Metalenguaje del riesgo

	METALENGUAJE DEL RIESGO		
PROCESO:			
OBJETIVO:			
FECHA:			
DEBIDO A (una o más causas)	**PUEDE OCURRIR QUE (riesgo)**	**DESCRIPCIÓN**	**LO QUE PODRÍA GENERAR (uno o más efectos)**

A continuación se presenta un ejemplo de diligenciamiento del formato Metalenguaje del riesgo

1.1.1.9 Tabla 8. Diligenciamiento metalenguaje del riesgo

	METALENGUAJE DEL RIESGO		
PROCESO:			
OBJETIVO:			
FECHA:			
DEBIDO A (una o más causas)	**PUEDE OCURRIR QUE (riesgo)**	**DESCRIPCIÓN**	**LO QUE PODRÍA GENERAR (uno o más efectos)**
• Equipos insuficientes • Equipos obsoletos • Desconocimiento de la normatividad aplicable	Incumplimiento en la generación de respuesta a los usuarios	No se generan las respuestas dentro de los términos legales	• Sanciones • Demandas
• Desmotivación • Resistencia al cambio • Información desactualizada	Generación de respuestas inadecuadas o errores a los usuarios	Respuestas sin la competencia técnica o no acorde a lo requerido	• Pérdida de imagen • Alto nivel de quejas por parte de los usuarios

Notas:

- Debido a (una o más causas): Documente las causas asociadas al riesgo identificado
- Puede ocurrir que (riesgo): Indique el nombre del riesgo
- Descripción: Utilice este espacio para describir en que consiste el riesgo identificado
- Lo que podría generar (uno o más efectos): Documente las consecuencias asociadas al riesgo

De acuerdo con la información anterior, se diligencia el formato Identificación del riesgo:

1.1.1.10 Tabla 9. Identificación del riesgo

	IDENTIFICACIÓN DEL RIESGO		
PROCESO:			
OBJETIVO:			
FECHA:			
CAUSAS	**RIESGO**	**DESCRIPCIÓN**	**CONSECUENCIAS POTENCIALES**

A continuación se presenta un ejemplo de diligenciamiento del formato Identificación del riesgo

1.1.1.11 Tabla 10. Diligenciamiento identificación del riesgo

	IDENTIFICACIÓN DEL RIESGO		
PROCESO:			
OBJETIVO:			
FECHA:			
CAUSAS	**RIESGO**	**DESCRIPCIÓN**	**CONSECUENCIAS POTENCIASLES**
• Equipos insuficientes • Equipos obsoletos • Desconocimiento de la normatividad aplicable	Incumplimiento en la generación de respuesta a los usuarios	No se generan las respuestas dentro de los términos legales	• Sanciones • Demandas
• Desmotivación • Resistencia al cambio • Información desactualizada	Generación de respuestas inadecuadas o errores a los usuarios	Respuestas sin la competencia técnica o no acorde a lo requerido	• Pérdida de imagen • Alto nivel de quejas por parte de los usuarios

11. ANÁLISIS DE RIESGOS

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado, o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por Impacto se entiende las consecuencias que puede ocasionar a la Entidad la materialización del riesgo. La etapa de análisis de los riesgos se divide en:

11.1. CLASIFICACIÓN DEL RIESGO

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda se refiere a la magnitud de sus efectos. Para la determinación de la calificación del riesgo, con base en la probabilidad y el impacto se debe tener en cuenta las siguientes tablas:

1.1.1.12 Tabla 11. Escala para clasificar la probabilidad del riesgo

Escala para calificar la probabilidad del riesgo		
Nivel	Concepto	Frecuencia
Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
Improbable	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
Moderado	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
Casi certeza	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Escala para calificar el impacto del riesgo							
Tipos de efecto o impacto		**a) Estratégico**	**b) Operativo**	**c) Financieros**	**d) Cumplimiento**	**e) Tecnología**	**f) Imagen**
INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la institución	Afecta el cumplimiento de algunas actividades	Genera ajustes a una actividad concreta	La pérdida financiera no afecta la operación normal de la institución	Genera un requerimiento	Afecta a una persona o una actividad del proceso	Afecta a un grupo de servidores del proceso
MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la institución	Afecta el cumplimiento de las metas del proceso	Genera ajustes en los procedimientos	La pérdida financiera afecta algunos servicios administrativos de la institución	Genera investigaciones disciplinarias, y/o fiscales y/o penales	Afecta el proceso	Afecta a los servidores del proceso
MODERADO	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la Institución	Afecta el cumplimiento de las metas de un grupo de procesos	Genera ajustes o cambios en los procesos	La pérdida financiera afecta considerablemente la prestación del servicio	Genera interrupciones en la prestación del bien o servicio	Afecta varios procesos de la institución	Afecta a todos los servidores de la institución
MAYOR	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas de la institución	Genera intermitencia en el servicio	La pérdida financiera afecta considerablemente el presupuesto de la institución	Genera sanciones	Afecta a toda la entidad	Afecta el sector
CATASTRÓFICO	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas del sector y del gobierno	Genera paro total de la institución	Afecta al presupuesto de otras entidades o a de la del departamento	Genera cierre definitivo de la institución	Afecta al Departamento	Afecta al Departamento, Gobierno, Todos los usuarios de la institución

Para la definición del impacto se debe tener en cuenta la clasificación del riesgo (Estratégico, operativo, financieros, cumplimiento, tecnología, imagen) de acuerdo con la clase del riesgo y la magnitud del impacto se debe determinar el nivel en el que se encuentra.

11.2. EVALUACIÓN DEL RIESGO

Permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo; de esta forma, se define la zona de ubicación del riesgo inherente (antes de la definición de controles). La evaluación del riesgo se calcula con base en variables cuantitativas y cualitativas.

1.1.1.13 Tabla 12. Evaluación del riesgo

PROBABILIDAD	**IMPACTO**				
	Insignificante	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Raro	B	B	B	M	M
Improbable	B	M	M	A	A
Moderado	B	M	A	A	E
Probable	M	A	A	E	E
Casi certeza	M	A	E	E	E

Color	**Zona de riesgo**
B	Zona de riesgo baja
M	Zona de riesgo moderada
A	Zona de riesgo alta
E	Zona de riesgo extrema

Con la evaluación del riesgo, previa a la formulación de controles se obtiene la ubicación del riesgo en la matriz de evaluación; esto se denomina **evaluación del riesgo inherente.**

11.3. DESARROLLO PRÁCTICO – ANÁLISIS

Formato de Análisis de riesgos, el cual hace parte del proceso Administración del Sistema Integrado de Gestión, donde se debe relacionar la siguiente información:

- **Riesgo:** Relacionar el riesgo redactado en el formato Identificación de riesgos
- **Calificación de probabilidad:** de acuerdo con la información cuantitativa y cualitativa
- **Calificación de impacto:** de acuerdo con la información cuantitativa y cualitativa que

- **Clasificación del riesgo:** Ver componentes de la identificación del riesgo, en el apartado de clasificación de los riesgos.
- **Evaluación:** surge del cruce de los resultados cuantitativos de la calificación para probabilidad e impacto;

1.1.1.14 Tabla 13. Análisis del riesgo

	ANÁLISIS DEL RIESGO			
PROCESO:				
OBJETIVO:				
FECHA:				
Riesgo	**Calificación**		**Clasificación del riesgo**	**Evaluación**
	Probabilidad	**Impacto**		

A continuación se presenta un ejemplo de diligenciamiento del formato Análisis del riesgo:

1.1.1.15 Tabla 14. Diligenciamiento Análisis del riesgo

	ANÁLISIS DEL RIESGO			
PROCESO:				
OBJETIVO:				
FECHA:				
Riesgo	**Calificación**		**Clasificación del riesgo**	**Evaluación**
	Probabilidad	**Impacto**		
Incumplimiento en la generación de respuesta a los usuarios	3	5	Cumplimiento	Zona de riesgo extrema
Generación de respuestas inadecuadas o errores a los usuarios	5	5	Operativo	Zona de riesgo extrema

11.4. VALORACIÓN DE LOS RIESGOS

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos Identificación y evaluación de controles y Valoración del riesgo.

11.4.1. **Identificación de controles.** Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

A continuación, se presentan las características mínimas que se deben tener en cuenta para la definición de los controles:

1.1.1.16 Tabla 15. Características para la definición de controles

Característica	**Descripción**
Objetivos	No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener
Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo
Realizables	Se deben definir controles que la entidad o el proceso esté en capacidad de llevar a cabo
Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad
Periódicos	Tienen frecuencia de aplicación en el tiempo
Efectivos	Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo
Asignables	tienen responsables definidos para su ejecución

En el siguiente ejemplo se presenta una forma de redacción de un control.

1.1.1.17 Tabla 16. Redacción de un control

Causa	**Riesgo**	**Efecto/Consecuencia**	**Control**
Uso de un calendario tributario obsoleto	Declaración de impuestos extemporánea	Sanciones pecuniarias para la entidad o disciplinaria para un(os) funcionario(s)	El contador y/o el Subdirector Administrativo y Financiero debe realizar la actualización u divulgación, en enero de cada año, de los calendarios tributarios nacionales y departamentales, en

			la página web, intranet, físicos, etc.

En esta etapa se deben describir todos los controles, existentes y por definir, deben estar orientados a atacar las causas y/o consecuencias (mitigar y/o eliminar) del riesgo. Una vez se hayan identificado y descrito los controles se debe determinar la clase del control; un control puede ser de tipo preventivo o correctivo como se presenta a continuación:

1.1.1.18 Tabla 17. Clases de controles

Clases de controles	
PREVENTIVO	CORRECTIVO
Acción o Conjunto de acciones que elimina o mitiga las causas del riesgo	Acción o conjunto de acciones que eliminan o mitigan las consecuencias
Orientación a disminuir la probabilidad de ocurrencia del riesgo	**Orienta a disminuir el nivel de impacto del riesgo**

11.4.2. **Evaluación de los controles.** Permite determinar en qué medida los controles identificados están aportando para disminuir los niveles de probabilidad e impacto del riesgo. Se evalúan verificando su documentación, aplicación y efectividad de la siguiente manera:

¿El control está documentado, incluye el responsable y la frecuencia de aplicación?	¿El control se está aplicando?	¿El control es efectivo (sirve o cumple su función?

- Si la pregunta relacionada con documentación se está cumpliendo, se deben asignar 25 puntos; en caso contrario marque 0.
- Si la pregunta relacionada con aplicación se está cumpliendo, se deben asignar 25 puntos; en caso contrario marque 0.
- Si la pregunta relacionada con efectividad se está cumpliendo, se deben asignar 50 puntos; en caso contrario marque 0.

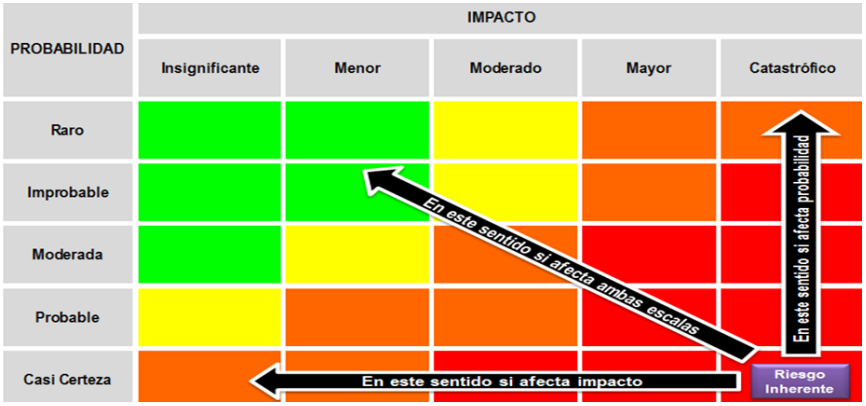
La evaluación se debe aplicar a cada control definido para el riesgo, determinando si se cumple o no el factor, según corresponda.

11.4.3. **Riesgo residual y definición de opciones de manejo.** Previo a la definición del riesgo residual se debe determinar qué escala (probabilidad, impacto o ambas) se afecta positivamente con la aplicación del control teniendo en cuenta las siguientes indicaciones:

1.1.1.19 Tabla 18. Escala de afectación

Escala de afectación		
PROBABILIDAD	IMPACTO	AMBAS
Cuando el control está orientado a eliminar o mitigar las causas del riesgos	Cuando el control está orientado a eliminar o mitigar las consecuencias	Cuando el control elimina o mitiga causas y consecuencias del riesgo

La evaluación de los controles (documentación, aplicación y efectividad) definirá la ubicación del riesgo en la matriz de evaluación; este paso se denomina “evaluación del riesgo residual”; los riesgos se pueden desplazar de la siguiente manera según la calificación de los controles y la definición de la escala que afecta cada riesgo.



Cuando se ha determinado el riesgo residual se debe asociar la opción de manejo mediante la cual se dará tratamiento al riesgo residual. Las opciones de manejo se determinan teniendo en cuenta la ubicación del riesgo según las zonas definidas así:

Color	**Zona de riesgo**	**Opciones de manejo**
B	Zona de riesgo baja	Asumir el riesgo
M	Zona de riesgo moderada	Asumir el riesgo Reducir el riesgo
A	Zona de riesgo alta	Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo
E	Zona de riesgo extrema	Reducir el riesgo Evitar el riesgo Compartir o transferir el riesgo

- **Asumir el riesgo:** aceptar la pérdida residual probable y elaborar los planes de contingencia para su manejo.

- **Reducir el riesgo:** implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). Ej.: optimización de procesos, definición de nuevos controles, entre otros.

- **Evitar el riesgo:** tomar las medidas encaminadas a prevenir su materialización. Ej.: cambios a la infraestructura, cambios en software.

- **Compartir o transferir el riesgo:** reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o mediante otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Ej.: seguros, sitios alternos, contratos de riesgos compartidos, etc.

11.4.4. **Desarrollo práctico – Valoración.** En el formato Identificación y evaluación de controles, se deben identificar y documentar los controles asociados al riesgo y calificar de acuerdo con las preguntas descritas en el formato; finalmente, se debe hacer la sumatoria de los resultados de calificación por control.

1.1.1.20 Tabla 19. Identificación y evaluación de controles

	IDENTIFICACIÓN Y EVALUACIÓN DE CONTROLES					
PROCESO:						
OBJETIVO:						
FECHA:						
RIESGO:						
Controles	Tipo de control		Evaluación del control			Total
	Probabilidad	Impacto	¿El control está documentado, incluye el responsable y la frecuencia de aplicación?	¿El control se está aplicando?	¿El control es efectivo (sirve o cumple su función)?	

Posterior a la identificación y evaluación de los controles, se debe diligenciar el formato Valoración del riesgo; en este formato se debe registrar la valoración final del riesgo de acuerdo con la calificación de cada control.

1.1.1.21 Tabla 20. Valoración de riesgos

	VALORACIÓN DE RIESGOS								
PROCESO:									
OBJETIVO:									
FECHA:									
RIESGO	CALIFICACIÓN		CONTROLES	VALORACIÓN				NUEVA VALORACIÓN	
	Probabilidad	Impacto		Tipo de control o impacto	Puntaje final probabilidad	Puntaje final impacto	Puntaje final	Probabilidad	Impacto

11.5. MANEJO DE RIESGOS

Una vez determinada la zona donde está ubicado el riesgo, y dependiendo de las opciones de manejo, se deben formular las acciones orientadas al mejoramiento y fortalecimiento de los controles identificados. Las acciones que se definan para el manejo del riesgo deben contemplar:

- Corregir las fallas identificadas en los controles según la evaluación realizada a cada uno.
- Reforzar o fortalecer los controles existentes.

Acción a Desarrollar	**+**	**Definición de responsables**	**+**	Definición de Plazo	**=**	Definición Adecuada de Acciones
Resolución adecuada de los Riesgos						Resultado esperado

Si la evaluación del riesgo residual, lo ubica en la zona baja no se deben formular acciones de manejo, el manejo estará únicamente enfocado en garantizar que los controles previamente establecidos operan de manera adecuada. Los riesgos ubicados en las zonas moderada, alta o extrema, exigen realizar acciones que fortalezcan los puntos débiles identificados en la evaluación de los controles.

11.5.1. **Desarrollo práctico – Manejo.** La información correspondiente al plan de manejo se debe registrar en el formato Manejo del riesgo.

1.1.1.22 Tabla 21. Manejo del riesgo

	MANEJO DEL RIESGO				
RIESGO:					
OBJETIVO:					
FECHA:					
RIESGO	**ZONA DE RIESGO RESIDUAL**	**ACCIONES**	**CRONOGRAMA**		**RESPONSABLE**
			Desde	**Hasta**	

11.6. SEGUIMIENTO DE RIESGOS

Cada cuatro meses Control Interno realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

- Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de Administración del Riesgo (diseño y funcionamiento).
- Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Los resultados de la evaluación y las observaciones de la persona que haga las veces de Control Interno deben ser presentados a la Alta Dirección, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.

12. MAPA DE RIESGOS

Una vez se tenga toda la información relacionada en los numerales anteriores, se documentará la información en el formato Mapa de riesgos de la Institución,

1.1.1.23 Tabla 22. Mapa de riesgos

Corvivienda www.corvivienda.gov.co			MAPA DE RIESGOS								
PROCESO:			ATENCION AL USUARIO								
OBJETIVO			Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.								
Fecha											
RIESGOS	CALIFICACION		Evalua Cion	Controles	Nueva Calificación		Eval	Medida Resp.	Acciones	Responsable	Indicador
	Proba.	Imp.	Zona Riesg.		Prob.	Imp.	Zon. Riesg				

Ejemplo de diligenciamiento de mapa de proceso

Corvivienda www.corvivienda.gov.co			MAPA DE RIESGOS							
PROCESO:			ATENCION AL USUARIO							
OBJETIVO			Dar trámite oportuno a las solicitudes provenientes de las diferentes partes interesadas, permitiendo atender las necesidades y expectativas de los usuarios, todo dentro de una cultura de servicio y de acuerdo a las disposiciones legales vigentes.							
Fecha										
RIESGOS	CALIFICACION		Evalua Cion	Controles	Nueva Calificacion		Eval	Medida Resp	Acciones	Responsable	Indicador
	Probabilidad	Impacto	Zona Riesgo.		Prob	Imp	Zona Riesgo				
Cambio en los datos de contacto de los usuarios	3	4	Extrema	Procedimientos establecidos para la asignación de Roles y Perfiles dentro del sistema	3	4	Alta	Reducir el Riesgo Evitar Compartir o Transferir	Capacitación al nuevo personal que asigna usuarios sobre el sistema.	Áreas responsables del manejo del sistema -	Nuevo personal vinculado VS Usuarios formados y conocedores de los procedimientos.

				Herramienta que permita el registro y monitoreo de acciones de los usuarios sobre sistema					Inclusión de alarmas ante anomalías	Área de tecnología	Número de solicitudes de usuario vs Cantidad de alarmas sobre el sistema

Los responsables de procesos y sus equipos de trabajo, deben garantizar que la información de los riesgos sea adecuada, coherente, pertinente y vigente. Cualquier ajuste que se deba realizar de esta información, debe ser informado.

13. CONTROL DE CAMBIOS

1.1.1.24 Tabla 23. Control de cambios

FECHA	VERSIÓN	CAMBIOS
Enero 2019	00	Documento inicial