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

2018-2020

CONTENIDO

1. INTRODUCCIÓN

Este plan pretende establecer mejores práticas y lineamientos de la 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, partiendo que la información es uin activo de gran valor que en la actualidad el estado reconoce como fuente de información para la interacción y toma de decisiones para la gestión. Adicional, que la política digital, se encuentra compuesta por dos componentes, TICS para el Estado y TICS para la Sociedad y uno de sus tres habilitadores es la Seguridad de la Información. Por ello es importante contar con un plan acerca plan de tratamiento de riesgos de seguridad y privacidad de la información.

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.

2. OBJETIVOS

2.1 Objetivo general

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

2.2 Objetivos específicos

- Concientizar a todos los 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.

3. ALCANCE

Esta guía, proporciona la metodología establecida por el HFPS 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.

4. ÁMBITO DE APLICACIÓN

Los lineamientos definidos en esta guía, aplica para la gestión de los riesgos de la información para el Hospital Francisco de Paula Santander ESE.

5. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder

a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal

- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.

- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).

- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).
- **Autorización**: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Ciberseguridad** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originen oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.

- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales:** Privados Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles. Datos Personales Sensibles Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3). Declaración de aplicabilidad Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los

procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000). Derecho a la Intimidad Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de

- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- **Materialización del riesgo:** ocurrencia del riesgo identificado
- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio

- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.

- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.

- **Proceso:** conjunto de entradas tangibles o intangibles, suministradas por un proveedor, a estas entradas se les asigna recursos y se aplican controles, obteniendo salidas tangibles o intangibles, destinadas a un usuario, generando un impacto en estos. Se clasifican en estratégicos, misionales, de apoyo y de evaluación.

- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.

- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen las siguientes características:

  - Los riesgos que han sido clasificados como estratégicos: en el paso de identificación deben haber sido marcados como de clase estratégica, es decir, se relacionan con el cumplimiento de objetivos institucionales, misión y visión.
  - Los riesgos que se encuentran en zona alta o extrema: después de valorar el riesgo (identificación y evaluación de controles), el riesgo residual se ubica en zonas de riesgo alta o extrema, indicando que el grado de exposición a la materialización del riesgo aún se encuentra poco controlado.
  - Los riesgos que tengan incidencia en usuario o destinatario final externo: en el caso de la materialización del riesgo la afectación del usuario externo se presenta de manera directa.

- Los riesgos de corrupción: todos los riesgos identificados que hagan referencia a situaciones de corrupción, serán considerados como riesgos de tipo institucional.

- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.

- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

6. 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:

- Gerente: aprueba las directrices para la administración del riesgo en el HFPS. Alineadas a la Dimensión 7 del Modelo Integrado de Planeación y Gestión.

- Proceso Planeación: Genera la metodología para la administración del riesgo del HFPS, coordina, lidera, capacita y asesora en su aplicación.

- Responsables de los procesos: Identifican, analizan, evalúan y valoran los riesgos del HFPS (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, contratistas y colaboradores: 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 de la ESE.

7. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

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

1. Conocer y cumplir las normas internas y externas relacionadas con la administración de los riesgos.
2. 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.
3. Someter los procesos y procedimientos permanentemente al análisis de riesgos con base en la aplicación de las metodologías adoptadas para el efecto.
4. Mantener un control permanente sobre los cambios en la calificación de los riesgos para realizar oportunamente los ajustes pertinentes.
5. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.
6. 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.
7. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades del HFPS para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado la Alta 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 el HFPS y que tienen como propósito evitar la materialización del riesgo.

8. 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 desplegarán 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.

9. 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 el hospital 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 institución; es la base para la identificación del riesgo, dado que de su análisis suministrará la información sobre las CAUSAS del riesgo.

10. Desarrollo práctico - Contexto Estratégico

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

- Cada responsable de proceso de Planeación, 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:

	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, cuál 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 de **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 articulará las ideas afines de la siguiente manera:

Figura 1. Articulación de ideas

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:

	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:

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

	insuficientes ● Equipos obsoletos		
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	● Najo 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 pertenecen cada idea:

Idea	Factores Externos
Nueva tecnología disponible	Tecnológico
Nuevas leyes	Legal
Demoras en la respuesta de comunicaciones enviadas por otras entidades	Interinstitucional
Incremento en el número de solicitudes por alta demanda de usuarios	Social
Cambio de Gobierno	Político
Poco conocimiento por parte de la ciudadanía	Social
Adaptación a normatividad internacional	Legal

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:

	CONTEXTO ESTRATÉGICO		
PROCESO:			
OBJETIVO:			
FECHA:			
FACTORES INTERNOS	**CAUSAS**	**FACTORES EXTERNO**	**CAUSAS**
Tecnología y sistemas de información	• Equipos insuficientes • Equipos obsoletos	Tecnológico	• Nueva tecnología 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	• Los indicadores no	Político	Cambio de

de control	miden nada		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 del hospital.
- 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.

11. 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.

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

Figura 2. Componentes de la identificación del riesgo

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.

11.1.1. Componentes de la identificación del riesgo

a) 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:

1. 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.
2. 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.
3. No se deben calificar las ideas como buenas o malas, son simplemente puntos de vista que capitalizados pueden brindar alternativas no consideradas.
4. 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.
5. El análisis de las ideas se debe realizar al final, por el moderador, quien las organizará y las expondrá a manera de resultado.
6. 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.

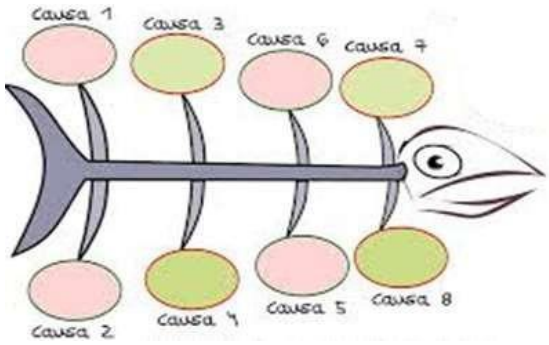

Figura 3. Análisis de causas – espina de pescado

b) 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 cuál podría ser el efecto menor que puede causar la materialización del riesgo hasta llegar al efecto mayor generado.

c) 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 riesgo mediante la definición de controles y planes de manejo:

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 del hospital por parte de la alta gerencia.
Operativo	Relacionados con el funcionamiento y operatividad de los sistemas de información del HFPS: definición de procesos,

	estructura del HFPS, articulación entre dependencias.
Financieros	Relacionados con el manejo de los recursos del HFPS: 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 del HFPS.

12. 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

Figura 4. Metalenguaje del riesgo

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.

12.1.1. 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).

	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

	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	Incumplimiento en la generación de respuesta a los usuarios	No se generan las respuestas dentro de los términos legales	• Sanciones • Demandas

obsoletos • Desconocimiento de la normatividad aplicable			
• 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 qué 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:

	IDENTIFICACIÓN DEL RIESGO
PROCESO:	
OBJETIVO:	

FECHA:			
CAUSAS	**RIESGO**	**DESCRIPCIÓN**	**CONSECUENCIAS POTENCIALES**

A continuación, se presenta un ejemplo de diligenciamiento del formato 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

13. 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:

13.1.1. Calificación 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:

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.

13.1.2. 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.

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.**

13.1.3. 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;

	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

	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

13.2. 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.

13.2.1. 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 del HFPS, en la medida en que los controles se identifican, documentan, 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:

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 el hospital 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.

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:

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**

Figura 5. Descripción de las clases de controles

13.2.2. 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.

13.2.3. 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:

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

riesgos	consecuencias	

Figura 6. Afectación de escalas según la probabilidad y/o el impacto

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.

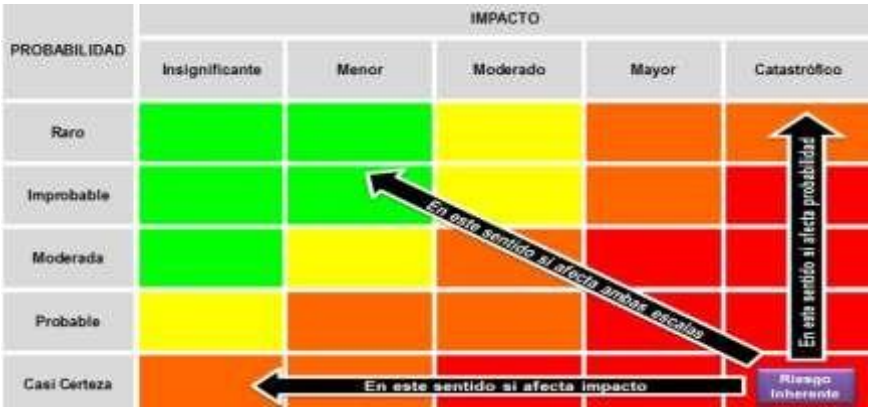

Figura 7. Afectación de escalas según la probabilidad y/o el impacto

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.

13.2.4. 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.

	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.

	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

13.3. 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

Figura 8. Definición adecuada de las acciones

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.

13.3.1. Desarrollo práctico - Manejo-

La información correspondiente al plan de manejo se debe registrar en el formato Manejo del riesgo.

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

13.4. 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.

14. 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,

	MAPA DE RIESGOS										
PROCESO:	ATENCIÓN 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	CALIFICACIÓN		Evaluación	Controles	Nueva Calificación		Eval	Medida Resp.	Acciones	Responsable	Indicador
	Proba.	Imp.	Zona Riesg.		Prob.	Imp.	Zon. Riesg				

Ejemplo de diligenciamiento de mapa de proceso

			MAPA DE RIESGOS								
PROCESO:			ATENCIÓN 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	CALIFICACIÓN		Evaluación	Controles	Nueva Calificación		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 - Área de tecnología	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		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.

15. CONTROL DE CAMBIOS

FECHA	VERSIÓN	CAMBIOS
Junio 2018	01	Documento inicial

Elaborado por	Revisado por	Aprobado por
Proceso: Dirección de TI	**Proceso:** Subgerencia Administrativa	**Proceso:** Subgerencia Administrativa
Fecha: Enero de 2020	**Fecha:** Enero de 2020	**Fecha:** Enero de 2020