2023

POLITICA DE ADMINISTRAACION DEL RIESGO

DIRECCION TERRITORIAL DE SALUD DE CALDAS

GCC ISO 9001 EMPRESA CERTIFICADA
Certificate No. LAT - 0915

+57 (606) 8801620 línea gratuita 018000968080
Cra 21 N° 29 - 29 Manizales - Caldas
informacion@saluddecaldas.gov.co
www.saluddecaldas.gov.co

Tabla de contenido

1. COMPROMISO 3
2. INTRODUCCIÓN 3
3. OBJETIVO 4
4. ALCANCE DE LA POLÍTICA 4
5. TÉRMINOS Y DEFINICIONES 4
6. RESPONSABILIDADES 9
7. ESCENARIOS DE PÉRDIDA DE CONTINUIDAD DEL NEGOCIO 14
8. CRITERIOS PARA LA EVALUACIÓN DE IMPACTO DE PÉRDIDA DE CONTINUIDAD DE NEGOCIO 15
9. ETAPAS PARA LA GESTIÓN DEL RIESGO 16
10. CONTEXTO 16
11. IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO 18
12. MEDICIÓN DE IMPACTO RIESGOS DE CORRUPCIÓN 21
13. VALORACIÓN DE IMPACTO DE RIESGOS SEGURIDAD DIGITAL 23
14. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS 25
15. APETITO DEL RIESGO 27
16. ESTRATEGIA DE SEGUIMIENTO AL PLAN DE ACCIÓN 28
17. HERRAMIENTA PARA LA GESTIÓN DEL RIESGO 29

1. COMPROMISO

La política de Administración del Riesgo de la Dirección Territorial de Salud de Caldas representa el compromiso institucional, en relación con la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos y escenarios de pérdida de continuidad de negocio que puedan afectar la planificación estratégica, en el marco del Modelo Integrado de Planeación y Gestión- MIPG.

2. INTRODUCCIÓN

La Dirección Territorial de Salud de Caldas en su compromiso para gestionar, identificar y tratar los riesgos de Gestión, de Corrupción y de Seguridad Digital, define su política de riesgos como un proceso dinámico, continuo y esencial**.** Por lo tanto, diseñamos herramientas que proporcionen la capacidad y la competencia para diagnosticar, priorizar, monitorear y tratar sus riesgos, teniendo en cuenta los cambios en el ambiente interno y externo, de tal forma que no sea sorprendida por riesgos desconocidos y no controlados.

El presente documento establece los lineamientos para la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos y escenarios de pérdida de continuidad de negocio que puedan afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos y planes institucionales, tomando como referencia las directrices del Modelo Integrado de Planeación y Gestión- MIPG, la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI, los requerimientos de la Guía para la administración del riesgo del DAFP y el Modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital.

3. OBJETIVO

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

4. ALCANCE DE LA POLÍTICA

La presente política de Administración de Riesgos Institucionales, **abarca el manejo de los riesgos asociados a los procesos, proyectos y acciones definidos por la entidad** y ejecutadas por el talento humano y todos aquellos actores que prestan servicios a través de las diferentes modalidades contractuales en el marco del Modelo Integrado de Planeación y Gestión que incluye: los riesgos de gestión, los riesgos de corrupción y los riesgos de seguridad digital, para los cuales se tendrán en cuenta los lineamientos y metodologías que se definan por parte de la entidad para su respectiva gestión.

5. TÉRMINOS Y DEFINICIONES

ACEPTACIÓN DEL RIESGO: Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

ACTIVO: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la institución para funcionar en el entorno digital.

ADMINISTRACIÓN DE RIESGOS: Conjunto de elementos de control que al interrelacionarse permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar con sus diferentes elementos le permite a la entidad pública, auto - controlar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.

AMENAZAS: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

ANÁLISIS DE RIESGO: Elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo.

APETITO DEL RIESGO: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

CAPACIDAD DE RIESGO: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta que no sería posible el logro de los objetivos de la Entidad.

CAUSA: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

CAUSA INMEDIATA: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

CAUSA RAÍZ: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

CIGD: Comité Institucional de Gestión y Desempeño.

CICCI: Comité Institucional de Coordinación de Control Interno.

COMPARTIR EL RIESGO: Se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.

CONFIDENCIALIDAD: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

CONSECUENCIA: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

CONTEXTO ESTRATÉGICO: Insumo básico para la identificación de los riesgos en los procesos y actividades, el análisis se realiza a partir del conocimiento de situaciones internas y externas de la institución.

CONTEXTO EXTERNO: Ambiente externo en el cual la Entidad busca alcanzar sus objetivos que puede ser: políticos, económicos y financieros, sociales y culturales, tecnológicos, ambientales, legales y reglamentarios.

CONTEXTO INTERNO: Ambiente interno en el cual la Entidad busca alcanzar sus objetivos, el cual puede ser: financieros, personal, procesos, tecnología, estratégicos, comunicación interna.

CONTINGENCIA: Posible evento futuro, condición o eventualidad.

CONTINUIDAD: Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.

CONTROL: Medida que permite reducir o mitigar un riesgo.

CONTROL CORRECTIVO: Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad detectada u otra situación no deseable.

CONTROL OPERACIONAL: Es el subsistema de control efectuado en el nivel de ejecución de las operaciones. Se trata de una forma de control realizada sobre la ejecución de las tareas y las operaciones desempeñadas por los trabajadores. En este sentido, el control operacional se refiere a los aspectos más específicos, como las tareas y operaciones.

CONTROL PREVENTIVO: Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad potencial u otra situación potencial no deseable.

CONTROL DETECTIVO: Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Atacan la probabilidad de ocurrencia del riesgo

CONTROL TÁCTICO: Control ejercido en el nivel intermedio de las organizaciones, también denominado control por departamentos o control gerencial. De manera general, el control táctico se refiere a los aspectos menos globales de la entidad. Su espacio de tiempo es el mediano plazo.

CRISIS (Emergencia): Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.

DISPONIBILIDAD: Propiedad de ser accesible y utilizable a demanda por una entidad.

FACTORES DE RIESGO: Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgos o tienden a aumentar la exposición, pueden ser internos o externos de la entidad.

GESTIÓN DEL RIESGO: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

IDENTIFICACIÓN DEL RIESGO: Elemento de control que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.

INTEGRIDAD: Propiedad de exactitud y completitud.

IMPACTO: Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

FACTORES DE RIESGO: Son las fuentes generadoras de riesgos.

NIVEL DE RIESGO: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

MAPA DE RIESGOS: Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.

MIPG: Modelo Integrado de Planeación y Gestión.

MECI: Modelo Estándar de Control Interno.

NIVEL DE ACEPTACIÓN DEL RIESGO: Son los criterios de aceptación de riesgos establecidos que se emplean durante la etapa de evaluación de riesgos.

PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

PROBABILIDAD: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

PROCESO DE ADMINISTRACIÓN DE RIESGO: Aplicación sistemática de políticas, procedimientos y prácticas de administración a las diferentes etapas de la administración del riesgo.

REDUCIR EL RIESGO: Aplicación de controles para reducir las probabilidades de ocurrencia de un evento.

RESTABLECIMIENTO: Capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.

RIESGO: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

RIESGO DE CORRUPCIÓN: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

RIESGO DE GESTIÓN: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

RIESGO DE SEGURIDAD DIGITAL: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, e incluye aspectos relacionados con el ambiente físico, digital y las personas.

RIESGO DE TECNOLOGÍA: Están relacionados con la capacidad tecnológica de la organización para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

RIESGO ESTRATÉGICO: Son las pérdidas ocasionadas por las definiciones estratégicas inadecuadas, errores en el diseño de planes, programas, estructura, integración del modelo de operación con el direccionamiento estratégico, asignación de recursos, estilo de dirección, ineficiencia en la adaptación a los cambios del sector, entre otros.

RIESGO INHERENTE: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

RIESGO FINANCIERO: Se relacionan con el manejo de los recursos de entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

RIESGO OPERACIONAL: Es la posibilidad de pérdidas ocasionadas en la ejecución de los procesos y funciones de la entidad por fallas en procesos, sistemas, procedimientos, modelos o personas que participan en dichos procesos.

RIESGO RESIDUAL: El resultado de aplicar la efectividad de los controles al riesgo inherente.

SGI: Sistema de Gestión Integrado.

TOLERANCIA AL RIESGO: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

TRATAMIENTO DEL RIESGO: Consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo, para evitar de este modo los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.

VALORACIÓN DEL RIESGO: Busca identificar y analizar los riesgos que enfrenta la entidad, tanto de fuentes internas como externas relevantes para la consecución de los objetivos, para administrarlos.

VULNERABILIDAD: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas

6. RESPONSABILIDADES

La responsabilidad de la gestión del riesgo, se encuentra definida a través de las Líneas de Defensa y la Dirección Territorial de Salud de Caldas las acoge según la siguiente tabla:

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
Línea Estratégica	Alta Dirección - Comité Institucional de Coordinación de Control Interno	Definir y aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la Dirección Territorial de Salud de Caldas y capacidades para prestar servicios. Definir y aprobar la política para la administración del riesgo. Garantizar el cumplimiento de los planes de la entidad Definición de líneas de reporte en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. Aprobar la política de administración de riesgos a través de acto administrativo.
Primera Línea	Subdirectores- Líderes de proceso- Equipos de trabajo	Conocer y apropiar las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo. Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso. Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. Revisar de acuerdo con su competencia y alcance la documentación de continuidad de negocio. Desarrollar ejercicios de autocontrol que corresponde a la actividad de primera línea, para ejecutar los controles establecidos en el día a día para mitigar los riesgos del proceso para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los planes de

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		preparación frente a la pérdida de continuidad de negocio. Informar a la Oficina asesora de planeación y Calidad (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. Reportar en el SIG los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. Formular planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados. Coordinar con sus equipos de trabajo las acciones establecidas en la planeación institucional, a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa. Realizar el seguimiento al mapa de riesgos de su proceso
Segunda Línea	Oficina Asesora de Planeación y Calidad	Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el CIGD. Actualizar la documentación que soporta la estrategia de continuidad de negocio. Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. Supervisar que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio. Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del CICCI. Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad.
Segunda Línea	Gestores de riesgos	Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles y las estrategias de continuidad de negocio asociadas a los escenarios de continuidad de negocio bajo su responsabilidad y los temas a su cargo. Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. Reportar en el módulo de riesgos del aplicativo SIG o delegar a un profesional de la dependencia o grupo a su cargo, el registro de los avances en la gestión del riesgo. Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad. Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.

LÍNEAS DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE AL RIESGO
		Participar en las pruebas del plan de continuidad de negocio y en la implementación. Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo.
Tercera Línea	Oficina de Control Interno	Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. . Asesorar a la primera línea de defensa de forma coordinada con la Oficina Asesora de Planeación y Calidad, en la identificación de los riesgos y diseño de controles. Llevar a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI. Recomendar mejoras a la política de operación para la administración del riesgo Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. Brinda un nivel de asesoría proactiva y estratégica, frente a la Alta Dirección y los líderes de proceso. Formar a la Alta Dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.

De igual manera, la Oficina Asesora de Planeación y Calidad lleva a cabo las siguientes acciones durante el acompañamiento para la identificación y administración del riesgo:

- Socializar anualmente la metodología de riesgos, los lineamientos de la primera línea de defensa frente al riesgo, objetivo del proceso, comunicación de los planes y proyectos del proceso asesorado.

- Capacitar al grupo de trabajo de cada dependencia en la herramienta SGI para la gestión del riesgo.

- Liderar las mesas de trabajo de identificación del riesgo.

- Verificar que las acciones de control se documenten conforme a los requerimientos de la metodología.

- Identificar claramente, junto con el equipo de trabajo, los responsables de las acciones y las fechas de realización, y registrarlas en el SGI.

- Elaborar el mapa de riesgos de proceso con toda la información respectiva, a partir de la información construida con los equipos de trabajo.

- Documentar los escenarios de pérdida de continuidad de negocio que se utilizan para el desarrollo y prueba del plan de continuidad de negocio.

- Revisar que el cargue de información en el SGI esté acorde con lo aprobado.

- Identificar, socializar y publicar el mapa de riesgos institucional a partir de los mapas de proceso

Por su parte, los líderes de proceso tienen la responsabilidad de:

- Asegurar que al interior de su grupo de trabajo se reconozca el concepto de "administración del riesgo", la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa.

- Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán de la identificación, monitoreo, reporte y socialización del riesgo asociados.

7. ESCENARIOS DE PÉRDIDA DE CONTINUIDAD DEL NEGOCIO

Cuando se presentan eventos que materializan uno o más de los escenarios de continuidad del negocio la Entidad evalúa las características de la emergencia para autorizar la activación del plan de continuidad, designar recursos y autorizar cualquier comunicación oficial hacia todos los grupos de valor, una vez declarada oficialmente la emergencia, se aplican las acciones de respuesta definidas en el plan de continuidad de negocio para dar respuesta a la misma.

La Dirección Territorial de Salud de Caldas adopta el siguiente conjunto de escenarios de riesgo estandarizados para el diseño de la estrategia de continuidad de negocio.

ESCENARIO	DESCRIPCIÓN

Emergencia Social	Imposibilidad de uso de las instalaciones debido a revueltas sociales, asonadas o pérdida del orden público que hace imposible la prestación del servicio o generación del producto.
Colapso de infraestructura física	Imposibilidad de acceso o abandono súbito de las instalaciones debido a un caso fortuito, fenómeno natural o fuerza mayor
Desastre Tecnológico	Pérdida total de la capacidad tecnológica o de los procesos institucionales para prestar los servicios o generar los productos
Crisis Financiera	Inexistencia de los bienes y servicios necesarios para el normal funcionamiento de la entidad que impacta la disponibilidad de recursos financieros, humanos, físicos y tecnológicos
Emergencia sanitaria	Crisis sanitaria que impide el funcionamiento de los procesos institucionales, incluye pandemias y epidemias declaradas por los organismos de salud del Estado.

8. CRITERIOS PARA LA EVALUACIÓN DE IMPACTO DE PÉRDIDA DE CONTINUIDAD DE NEGOCIO

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

CRITERIO	DESCRIPCIÓN
FINANCIERO	Nivel de pérdidas económicas
REPUTACIONAL	Nivel de pérdida de la confianza de los grupos de valor en la entidad
LEGAL/ REGULATORIO	Nivel de incumplimiento de normas y regulaciones a las que está sometida la entidad
CONTRACTUAL	Impactos asociados al incumplimiento de cláusulas en obligaciones contractuales
MISIONAL	Nivel de incumplimiento o impacto percibido por imposibilidad de cumplir los objetivos y obligaciones misionales

9. ETAPAS PARA LA GESTIÓN DEL RIESGO

La gestión de riesgos comprende las actividades de análisis del contexto interno y externo, identificación y análisis del riesgo, valoración, evaluación, definición de controles para el tratamiento y seguimiento:

- **Identificación y análisis de riesgos:**

En esta etapa, tratamos de averiguar cuáles son los elementos que pueden amenazar el éxito de la entidad. Se trata de reconocer todo aquello que puede provocar un mal funcionamiento en el desarrollo y ver la relación causa-efecto que puede tener.

Identificamos y priorizamos los riesgos teniendo en cuenta la probabilidad de que ocurran y el impacto en la entidad. El uso de herramientas como la matriz de riesgos nos pueden ayudar a visualizar de forma más clara todo el proceso.

- **Valoración de los riesgos:**

En función del impacto y la probabilidad de que ocurra, podemos atender al impacto que puede producir en el tiempo, la naturaleza, si podemos gestionarlos de forma interna o externa y priorizar los riesgos conocidos.

- **Evaluación de los riesgos:**

En esta fase, analizamos la probabilidad de que ocurra y el impacto que puede tener para obtener así el factor de riesgo. Esto nos permite saber si merece más atención que otro un determinado riesgo y priorizar los riesgos conocidos.

- **Control y reducción de riesgos:**

Planear una respuesta para los riesgos de alta prioridad, monitorizar nuevos riesgos que puedan presentarse y ejecutar un plan de acción que dé respuesta a la mitigación de estos.

10. CONTEXTO

A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar en cada vigencia, se analiza el entorno estratégico de La Dirección Territorial de Salud de Caldas a partir de los siguientes factores internos, externos y de proceso, para el adecuado análisis de las causas del riesgo y gestión del mismo.

CONTEXTO		
CONTEXTO EXTERNO	Económicos y Financieros	Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	Políticos	Cambios de gobierno, legislación, políticas públicas, regulación
	Sociales y culturales	Demografía, responsabilidad social, orden público
	Tecnológicos	Avances en tecnología, acceso a sistemas de información externos, gobierno en línea
	Ambientales	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible
	Legales y reglamentarios	Normatividad externa (Leyes, decretos, ordenanzas y acuerdos)
	Comunicación externa	Mecanismos utilizados Para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad
CONTEXTO INTERNO	Financieros	Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada
	Personal	Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional
	Procesos	Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento
	Tecnología	Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información
	Estratégicos	Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo
	Comunicación interna	Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones
	Diseño del proceso	Claridad en la descripción del alcance y objetivo del proceso

CONTEXTO		
CONTEXTO INTERNO DEL PROCESO	Interacciones con otros procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes
	Transversalidad	Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad
	Procedimientos asociados	Pertinencia en los procedimientos que desarrollan los procesos
	Responsables del proceso	Grado de autoridad y responsabilidad de los funcionarios frente al proceso
	Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos
	Activos de seguridad digital del proceso	Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano

11. IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO

La identificación del riesgo se realiza determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del Proceso.

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos. Se aplican las siguientes fases:

- **Análisis de objetivos estratégicos y de los procesos:**

Objetivos Estratégicos: La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que pueden ocasionar su éxito o su fracaso.

Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es

decir, que contengan las siguientes características mínimas: Especifico, medible, alcanzable, relevante y proyectado en el tiempo.

Objetivos de Procesos: Los objetivos de proceso deben ser analizados con base en las características de los objetivos estratégicos, además, se debe revisar que los mismos estén alineados con la Misión y la Visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos.

- **Identificación de los puntos de riesgo:**

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

- **Identificación de áreas de impacto:**

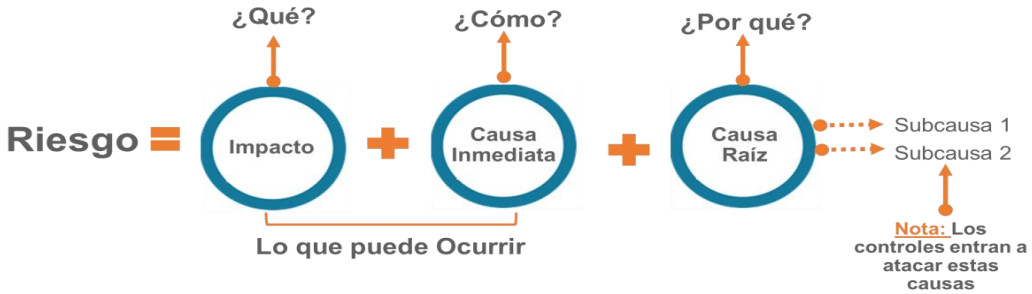
El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

- **Identificación de áreas de factores de riesgo:**

La identificación de riesgos es la etapa de la gestión en la que se concretan esos factores de incertidumbre. Esta etapa reviste especial importancia ya que, si no se consigue identificar aquellos riesgos más importantes, la gestión posterior resultaría poco eficaz.

- **Descripción del riesgo:**

la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:



Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Causa Inmediata: Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o subcausas que pueden ser analizadas.

PROBABILIDAD RIESGOS DE GESTIÓN, CORRUPCION Y SEGURIDAD DIGITAL

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

Nivel	Probabilidad	Descripción
100%	Muy Alta	La actividad se realiza más de 1500 veces al año.
80%	Alta	La actividad se realiza entre 366 a 1500 veces al año.
60%	Media	La actividad se realiza entre 13 a 365 veces al año.
40%	Baja	La actividad se realiza entre 5 a 12 veces al año.
20%	Muy Baja	La actividad se realiza máximo 4 veces al año.

IMPACTO RIESGOS DE GESTION

Se revisa el nivel de impacto de acuerdo con el tipo de impacto definido en la descripción del riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

Nivel	Impacto	Descripción Económica o Presupuestal	Descripción Reputacional
100%	Catastrófico	Pérdida económica superior a 1500 SMLV.	Deterioro de imagen con efecto publicitario sostenido a nivel internacional.
80%	Mayor	Pérdida económica de 319 hasta 1500 SMLV.	Deterioro de imagen con efecto publicitario sostenido a nivel Nacional o Territorial.
60%	Moderado	Pérdida económica de 21 hasta 318 SMLV.	Deterioro de imagen con efecto publicitario sostenido a nivel Local o Sectores Administrativos.
40%	Menor	Pérdida económica de 11 hasta 20 SMLV.	De conocimiento general de la entidad a nivel interno, Dirección General, Comités y Proveedores.
20%	Leve	Pérdida económica hasta 10 SMLV.	Solo de conocimiento de algunos funcionarios.

12. MEDICIÓN DE IMPACTO RIESGOS DE CORRUPCIÓN

La medición del impacto de los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración. Cada riesgo identificado es valorado de acuerdo con

las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

MEDICIÓN DE IMPACTO RIESGOS DE CORRUPCIÓN			
DESCRIPTOR	**DESCRIPCIÓN**	**NIVEL**	**RESPUESTAS AFIRMATIVAS**
Moderado	Afectación parcial al proceso y a la dependencia Genera mediana consecuencia para la entidad	5	1-5
Mayor	Impacto negativo en la entidad Genera altas consecuencias para la entidad	10	6-11
Catastrófico	Consecuencias desastrosas sobre el sector Genera consecuencias desastrosas para la entidad	20	12-19

NO	PREGUNTA	RESPUESTA	
	¿SI EL RIESGO SE MATERIALIZA PODRÍA?	**SI**	**NO**
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la Entidad?		
4	¿Afectar el cumplimiento de misión del sector al cual pertenece la Entidad?		
5	¿Generar pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
9	¿Generar perdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la fiscalía u otro ente?		

NO	PREGUNTA	RESPUESTA	
	¿SI EL RIESGO SE MATERIALIZA PODRÍA?	SI	NO
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fis cales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar les iones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

13. VALORACIÓN DE IMPACTO DE RIESGOS SEGURIDAD DIGITAL

CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL			
CATEGORÍA	**DESCRIPCIÓN CUANTITATIVA**	**DESCRIPCIÓN CUALITATIVA**	**NIVEL**
CATASTRÓFICO	Afectación en un valor igual o superior al 50%de la población. Afectación en un valor igual o superior al 50% del presupuesto de seguridad de la información en la entidad. Afectación muy grave del medio ambiente que requiere > 3 años de recuperación	Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad por más de cinco 5 días	**100%**
MAYOR	Afectación en un valor igual o mayor al 20% e inferior al 50% de la población.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros.	**80%**

CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL			
CATEGORÍA	**DESCRIPCIÓN CUANTITATIVA**	**DESCRIPCIÓN CUALITATIVA**	**NIVEL**
	Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto de seguridad de la información en la entidad. Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación	Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad entre 2 y 4 días	
MODERADO	Afectación en un valor igual o mayor al 10% y menor al 20% de la población. Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto de seguridad de la información en la entidad. Afectación leve del medio ambiente requiere de 3,1 a 1 año de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros. Interrupción de las operaciones de la Entidad por un (1) día.	**60%**
MENOR	Afectación en un valor igual o mayor al 1% y menor al 10%de la población. Afectación en un valor igual o mayor al 1% y menor al 10%del presupuesto de seguridad de la información en la entidad.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad. Interrupción de las operaciones de la Entidad hasta por 8 horas (1 jornada laboral)	**40%**

CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL			
CATEGORÍA	**DESCRIPCIÓN CUANTITATIVA**	**DESCRIPCIÓN CUALITATIVA**	**NIVEL**
	Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación		
LEVE	Afectación en un valor menor al 1% de la población. Afectación en un valor menor al 1% del presupuesto de seguridad de la información en la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad No hay interrupción de las operaciones de la entidad	**20%**

14. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

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

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	**Líder de Proceso**	Informar a la Oficina Asesora de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado y marcar en el SGI la alerta de posible materialización.
		Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario.
		Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento.
		Efectuar el análisis de causas y determinar acciones preventivas y de mejora.

		Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar.
		Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario.
		Informar a discreción los posibles actos de corrupción al ente de control.
Riesgos de Gestión y Seguridad digital	**Líder de Proceso**	Informar a la Oficina Asesora de Planeación como segunda línea de defensa, el evento o materialización de un riesgo.
		Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento.
		Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos.
		Dar cumplimiento al procedimiento plan de mejoramiento.
	Oficina de Control Interno	Informar al líder del proceso sobre el hecho encontrado
		Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.
		Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente.

		Si la materialización de los riesgos es el resultado de una auditoría realizada por la Jefatura de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento.
Riesgos de continuidad de negocio	**Comité institucional de Gestión y desempeño**	Activar el plan de continuidad de negocio

15. APETITO DEL RIESGO

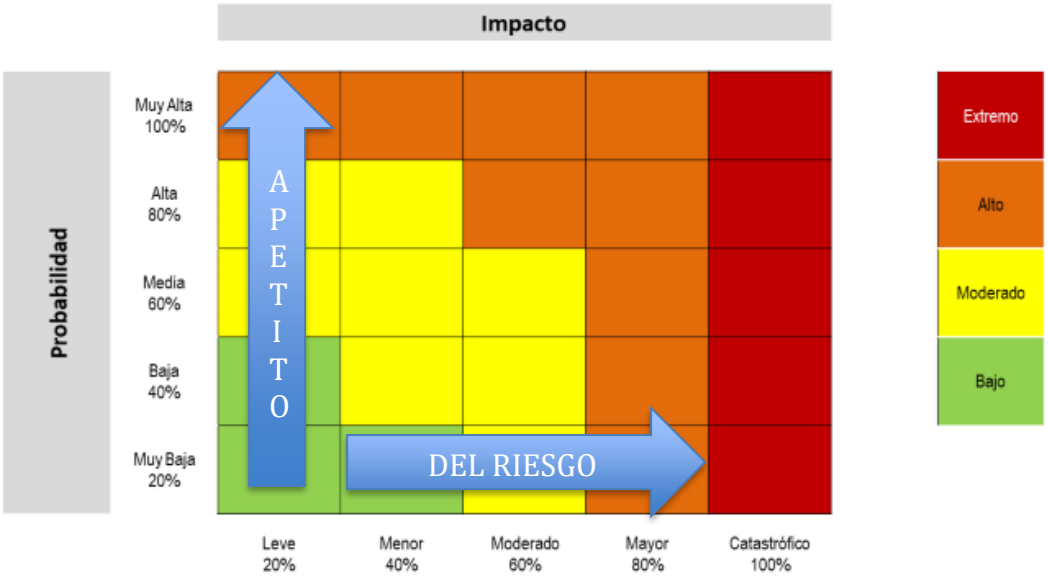
Acorde con los riesgos residuales aprobados por el Comité Institucional de Coordinación de Control Interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados, de la siguiente manera:

Decisión que se toma frente a un determinado nivel de riesgo, pueden ser aceptar, reducir y evitar. Se analiza frente al Riesgo Residual, esto para proceso en funcionamiento, cuando se trate de procesos nuevos se procederá a partir del riesgo inherente.

TIPO DE RIESGO	ZONA DE RIESGO RESIDUAL	ESTRATEGIA DE TRATAMIENTO
Riesgos de Gestión y Seguridad digital	Baja	Se realiza seguimiento CUATRIMESTRAL y se registran sus avances en el módulo de riesgos SGI.
	Moderada	Se realiza seguimiento CUATRIMESTRAL y se registran sus avances en el módulo de riesgos – SGI.
	Alta	Se realiza seguimiento CUATRIMESTRAL y se registran sus avances en el módulo de riesgos – SGI.
	Extrema	Se realiza seguimiento CUATRIMESTRAL y se registra en el módulo de riesgos - SGI.

Riesgos de Corrupción	Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento CUATRIMESTRAL y se registra en el módulo de riesgos – SGI.

ACEPTACION DEL RIESGO EN LA MATRIZ DE CALOR (NIVELES DE SEVERIDAD DEL RIESGO)



16. ESTRATEGIA DE SEGUIMIENTO AL PLAN DE ACCIÓN

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

		Después de haber implementado la acción debe realizar un seguimiento con el fin de evaluar la efectividad del plan de acción.

Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar periódicamente su Mapa de Riesgos y si es del caso ajustarlo. Igualmente registrar en el Modulo de Riesgos - SGI los avances y analizan con sus equipos de trabajo el estado de sus proyectos y procesos frente a los controles establecidos. Según el resultado de la administración del riesgo, el líder del proceso solicita ajuste a los riesgos o controles y elabora acciones de mejoramiento o correctivas en el Plan de Mejoramiento Institucional.

17. HERRAMIENTA PARA LA GESTIÓN DEL RIESGO

La Dirección Territorial de Salud de Caldas determina que el Módulo de Riesgos del SIG, es la herramienta para identificar, valorar, evaluar y administrar los riesgos, de corrupción y de seguridad digital, por tanto, toda información asociada con los riesgos es provista por dicha herramienta, para lo cual la Oficina Asesora de Planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento y cargue de información y dispone un manual de uso para el servicio de todos los procesos

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

Manual operativo MIPG Versión 3
Política de Riesgos de la Dirección Territorial de Salud de Caldas
Guía para la Administración del riesgo de DAFP Versión 5
Manual Metodología de riesgos Versión 7
Módulo de riesgos SGI