RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

El Gerente del Hospital Departamental San Rafael de Zarzal E.S.E., en uso de sus atribuciones legales, en especial de las conferidas en el Artículo 4º del Decreto Ley 0139 de 1996 y demás normas concordantes, y

CONSIDERANDO:

1. Que el Artículo 209 de la Constitución Política, establece que "La Administración Pública, en todos sus órdenes tendrá un Control Interno que se ejercerá en los términos que señale la Ley"

2. Que el Artículo 269 de la Carta Política, estipula que "En las Entidades Públicas, las autoridades correspondientes están obligadas a diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de Control Interno, de conformidad con lo que disponga la Ley.

3. Que el Artículo 5 de la Ley 87 de 1.993, "Por la cual se establecen normas para el ejercicio del Control Interno de las Entidades y organismos del Estado y se dictan otras disposiciones", dispuso que el establecimiento y desarrollo del Sistema de Control Interno en los Organismos y Entidades Públicas, será responsabilidad del Representante Legal o máximo directivo correspondiente. No obstante, la aplicación de los métodos y procedimientos al igual que la calidad, eficiencia y eficacia del Control Interno, también será responsabilidad de los jefes de cada una de las distintas dependencias de las Entidades y Organismos.

4. Que el Literal 1 del Artículo 2 de la Ley 87 de 1.993, establece como uno de los objetivos del Sistema de Control Interno. definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de sus objetivos.

5. Que el Decreto 1537 de 2001, por medio del Cual se reglamenta parcialmente la Ley 87 de 1.993, en su artículo 4, define la Administración de Riesgos como parte integral del fortalecimiento de los Sistemas de Control Interno en las Entidades Públicas, para lo cual se establecerán y aplicarán Políticas de Administración del Riesgo.

6. Que en el ARTÍCULO 2.2.9.1.2.1. Componentes. Los fundamentos de la Estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea.

7. Que el Hospital Departamental San Rafael de Zarzal E.S.E., en aras de propender por el mejoramiento continuo de los procesos, y teniendo en cuenta los constantes cambios que se han presentado, ha observado la necesidad de adoptar el Manual de Administración del Riesgo de la Entidad, pretendiendo con ello aumentar la probabilidad de alcanzar las metas y objetivos institucionales.

8. Que el Departamento Administrativo de la Función Pública, publicó "Guía para la Administración del Riesgo de Gestión, Corrupción y Seguridad Digital y, Diseño de Controles en Entidades Públicas." De mayo del 2018 la cual obedece a la armonización entre el Modelo Estándar de Control Interno y la norma técnica de

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

calidad (NTCGP1000:2009) y el Modelo Integrado de Planeación y Gestión, con el fin de facilitar a las entidades el ejercicio de la administración del Riesgo.

9. Que el decreto 1008 de 2018, actualizó la estructura de la Estrategia Gobierno en Línea a la nueva Política de Gobierno Digital así:

9.1 Componentes de la Política de Gobierno Digital: Son las líneas de acción que orientan el desarrollo y la implementación de la Política de Gobierno Digital, a fin de lograr sus propósitos. Los componentes son:

- TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones.
- TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común.
- Habilitadores Transversales de la Política de Gobierno Digital: Son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital; y
- Lineamientos y estándares de la Política de Gobierno Digital: Son los requerimientos mínimos que todos los sujetos obligados deberán cumplir para el desarrollo de los componentes y habilitadores que permitirán lograr los propósitos de la Política de Gobierno Digital.

RESUELVE

ARTÍCULO PRIMERO: ADOPCIÓN. ADOPTAR el "**MANUAL DE ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL" Y "LOS MAPAS DE RIESGOS" PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."**, con los cuales se conducirá a la minimización de la ocurrencia de riesgos negativos y que puedan afectar la gestión administrativa de la entidad, acciones que se encaminarán como resultado de la calificación y evaluación obtenida en el análisis, medición y valoración de los riesgos, plasmados en los Mapas de Riesgos del Hospital Departamental San Rafael de Zarzal E.S.E. y que serán adelantados por los integrantes del Comité de Control interno de la Entidad, conforme al documento e instrumentos que hacen parte integral del presente acto administrativo.

PARÁGRAFO: El Manual de Administración del Riesgo de gestión, corrupción y seguridad digital, contiene la metodología de la Administración de Riesgos y establece las guías de acción para que todos los servidores públicos del Hospital Departamental San Rafael de Zarzal E.S.E., coordinen y administren los eventos que pueden impedir el logro de los objetivos de la entidad, orientándolas y habilitándolas para ello. El manual establece las políticas que identifican las opciones para tratar y manejar los Riesgos con base en su

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

valoración, y permiten tomar decisiones adecuadas para evitar, reducir, compartir, transferir o asumir el riesgo.

ARTÍCULO SEGUNDO: ALCANCE. La Administración de Riesgos en la entidad, tendrá carácter prioritario y estratégico, fundamentado en el Modelo de Operación por procesos. En virtud de lo anterior, la identificación, análisis y valoración de los Riesgos se circunscribirá a los objetivos estratégicos de cada proceso.

ARTÍCULO TERCERO: RESPONSABLE. La Responsabilidad de la elaboración del Mapa de Riesgos estará a cargo de los responsables de cada uno de los procesos. Ellos serán los encargados de implementar los controles, verificar su efectividad, proponer cambios, velar por su adecuada documentación y por su actualización y aplicarlos al interior de su proceso. El Comité Coordinador de Control Interno es el encargado de aprobar y adoptar las modificaciones a los Mapas de Riesgos

ARTICULO CUARTO: ESTRUCTURA DE LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, MANUAL DE OPERACIÓN Y MAPAS DE RIESGOS DEL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.

¿QUÉ ESTABLECE MIPG?

El Numeral 2.2.1 "Política de Planeación institucional" de la dimensión "Direccionamiento Estratégico y Planeación" menciona que, para responder a la pregunta ¿Cuáles son las prioridades identificadas por la entidad y señaladas en los planes de desarrollo nacionales y territoriales?, se deben formular las metas de largo plazo, tangibles, medibles, audaces y coherentes con los problemas y necesidades que deben atender o satisfacer, evitando proposiciones genéricas que no permitan su cuantificación y definiendo los posibles riesgos asociados al cumplimiento de las prioridades.

De igual forma, se menciona en esta dimensión que, para llevar a cabo el ejercicio de planeación, la entidad debe documentar dicho ejercicio en donde se describa la parte conceptual u orientación estratégica; y la parte operativa en la que se señale de forma precisa los objetivos, las metas y resultados a lograr, las trayectorias de implantación o cursos de acción a seguir, cronogramas, responsables, indicadores para monitorear y evaluar su cumplimiento y los riesgos que pueden afectar tal cumplimiento y los controles para su mitigación

1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Teniendo en cuenta que el Decreto 1537 de 2001 en su artículo 4 establece que la Administración del riesgo es parte integral del fortalecimiento de los Sistemas de Control Interno en las entidades públicas y determina que las autoridades correspondientes deberán establecer y aplicar políticas para su gestión, el Hospital Departamental San Rafael de Zarzal E.S.E. a continuación establece los lineamientos para la gestión del riesgo aplicable en todos los niveles de la entidad.

Dicha política se asienta sobre las siguientes bases:

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

1.1 Objetivo:

Establecer el marco general de actuación para la gestión de los riesgos a los que puede enfrentarse el Hospital Departamental San Rafael de Zarzal E.S.E. Valle, en el marco de sus actuaciones, garantizando de forma razonable que se alcanzarán los objetivos institucionales y por ende será posible cumplir con su misión y visión.

1.2 Alcance:

Los lineamientos acá presentados serán de aplicación obligatoria para todos los procesos y áreas del Hospital Departamental San Rafael de Zarzal E.S.E., así mismo se deberán extender para los proyectos especiales que desarrolle la entidad.

1.3. Términos y Definiciones:

ADMINISTRACIÓN DEL RIESGO**:** Un 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. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de Planeación.

ANÁLISIS CUALITATIVO: Se refiere a la utilización de formas descriptivas para presentar la magnitud de consecuencias potenciales y la posibilidad de ocurrencia.

ANÁLISIS CUANTITATIVO: Este análisis contempla valores numéricos; la calidad depende de lo exactas y completas que estén las cifras utilizadas. Básicamente se refiere a la construcción de indicadores que reflejen tanto la probabilidad de ocurrencia como el impacto que pueden causar. La forma en la cual la probabilidad y el impacto son expresados y las formas por las cuales ellos se combinan para proveer el nivel de riesgo puede variar de acuerdo al tipo de riesgo.

CONSECUENCIA: Resultado de un evento

ESTABLECIMIENTO DEL CONTEXTO: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.

IDENTIFICACIÓN DEL RIESGO: Proceso para encontrar, reconocer y describir el riesgo.

LÍDER O RESPONSABLE DEL PROCESO: Persona con la responsabilidad y autoridad para gestionar un riesgo.

PROBABILIDAD: Oportunidad de que algo suceda

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

Nota: El riesgo en su tendencia más común es valorado como una amenaza, en este sentido, los esfuerzos institucionales se dirigen a reducirlo, evitarlo, transferirlo o mitigarlo;

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

sin embargo, el riesgo puede ser analizado como una oportunidad, lo cual implica que su gestión sea dirigida a maximizar los resultados que éstos generan.

RIESGO DE CORRUPCIÓN: La 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 en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

RIESGO RESIDUAL: Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.

1.4 POLÍTICA GENERAL DE ADMINISTRACIÓN DEL RIESGO

El Hospital Departamental San Rafael de Zarzal E.S.E., declara que en el desarrollo de sus actividades ocurren riesgos, por lo cual se compromete a adoptar mecanismos y acciones necesarias para la gestión integral de los mismos que prevengan o minimicen su impacto.

Para ello adoptará mecanismos que permitan la identificación, análisis, valoración, seguimiento y control de los riesgos propios de su actividad, acogiendo una autorregulación prudencial. La entidad determinará su nivel de exposición concreta a los impactos de cada uno de los riesgos para priorizar su tratamiento, y estructurará criterios orientadores en la toma de decisiones respecto de los efectos de los mismos basados en los lineamientos para administración del riesgo dados por el departamento administrativo de la función pública.

1.5 Estructura para la gestión del Riesgo

La estructura para el análisis de contexto, la identificación y valoración del riesgo que deberá ser aplicada por los procesos está determinada por la metodología para la Administración del Riesgo emitida por el Departamento Administrativo de la Función Pública v4.

A partir de dichos lineamientos, específicamente para el análisis de probabilidad e impacto de los riesgos, se establecen las siguientes tablas generales basadas en la Guía Para La Administración del Riesgo v4 la cual será la base de trabajo para todo el componente de administración del Riesgo para el Hospital Departamental San Rafael de Zarzal E.S.E.

2. IDENTIFICACIÓN DEL RIESGO

ANÁLISIS Y DEFINICIÓN DE OBJETIVOS. Le corresponde a la Segunda Línea de Defensa, el análisis de los objetivos de la entidad tanto del orden estratégico como de procesos.

- **Análisis de objetivos estratégicos.** La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

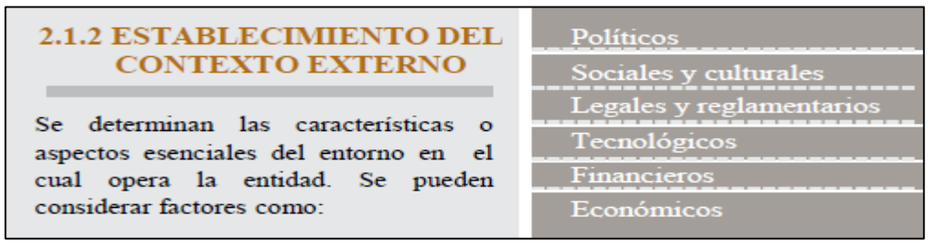
Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en inglés).

- **Análisis de los objetivos de proceso.** Los objetivos de proceso deben ser analizados con base en las características mínimas, pero, 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.

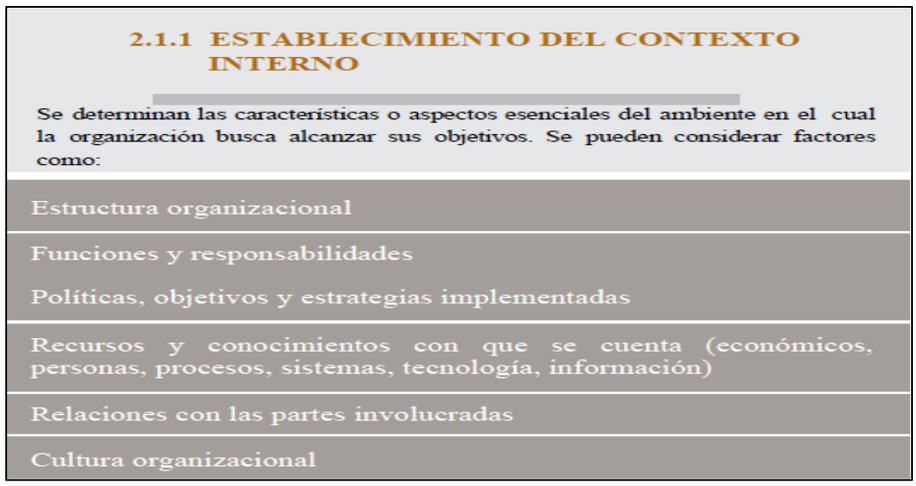
2.1 ESTABLECIMIENTO DEL CONTEXTO

Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo a partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

- **ESTABLECIMIENTO DEL CONTEXTO EXTERNO**
  Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad.



- **ESTABLECIMIENTO DEL CONTEXTO INTERNO**
  Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos.

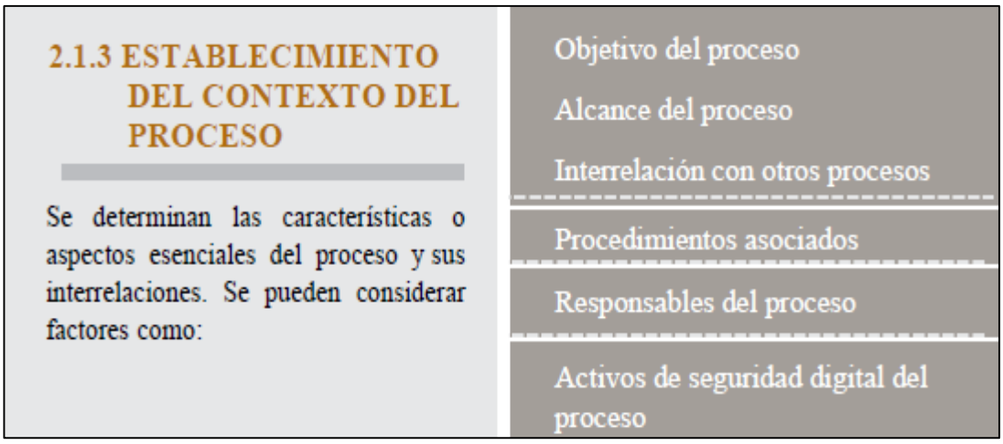


RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

- **ESTABLECIMIENTO DEL CONTEXTO DEL PROCESO**

  Se determinan las características o aspectos esenciales del proceso y sus interrelaciones.



Contexto Externo	**ECONÓMICOS**: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación.
	SOCIALES: Demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	MEDIOAMBIENTALES: Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	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.
Contexto del Proceso	**DISEÑO DEL PROCESO:** Claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

	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.

IDENTIFICACIÓN DE ACTIVOS – RIESGOS DE SEGURIDAD DIGITAL

IDENTIFICACIÓN DE LOS ACTIVOS
Le corresponde a la Primera línea de Defensa, realizar la identificación de activos en cada proceso.

¿QUÉ SON LOS ACTIVOS?
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 organización para funcionar en el entorno digital.

¿POR QUÉ IDENTIFICAR ACTIVOS?
De esta manera se puede determinar qué es lo más importante que cada entidad y sus procesos poseen (Sean bases de datos, unos archivos, servidores web o aplicaciones claves para que la entidad pueda prestar sus servicios). Así la entidad puede saber qué es lo que debe proteger para garantizar su funcionamiento tanto interno como de cara al **ciudadano**, aumentando así su confianza en el uso del entorno digital para interactuar con el estado.

IMPORTANTE: Todo lo que no está plenamente identificado, no está debidamente asegurado.

¿COMO IDENTIFICAR LOS ACTIVOS?:

Paso 1. Listar los activos por cada proceso
Paso 2. Identificar el dueño de los activos
Paso 3. Clasificar los activos.
Paso 4. Clasificar la información
Paso 5. Determinar la criticidad del activo

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

IDENTIFICACIÓN DE RIESGOS

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. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo.

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 o estratégicos.

Preguntas claves para la identificación del riesgo.

¿Qué puede suceder?
¿Cómo puede suceder?
¿Cuándo puede suceder?
¿Qué consecuencias tendría su materialización?

Las preguntas claves para la identificación del riesgo permiten determinar:

¿QUÉ PUEDE SUCEDER? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.

¿CÓMO PUEDE SUCEDER? Establecer las causas a partir de los factores determinados en el contexto

¿CUÁNDO PUEDE SUCEDER? Determinar de acuerdo al desarrollo del proceso

¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN? Determinar los posibles efectos por la materialización del riesgo

IDENTIFICACIÓN DE RIESGOS -TÉCNICAS PARA LA IDENTIFICACIÓN DE RIESGOS

RIESGOS DE CORRUPCIÓN

Definición 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.

"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos". (Conpes N° 167 de 2013)

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

Los riesgos de corrupción se establecen sobre ***procesos***.

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la **matriz de definición de riesgo de corrupción**, que incorpora cada uno de los componentes de su definición.

Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente, se trata de un riesgo de corrupción, así:

Matriz definición del riesgo de corrupción				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato	X	X	X	X

GENERALIDADES RIESGOS DE CORRUPCIÓN

- Entidades encargadas de gestionar el riesgo: lo deben adelantar las entidades públicas del orden nacional, departamental y municipal.

- Se elabora anualmente por cada responsable de los procesos al interior de las entidades, junto con su equipo.

- Consolidación: la oficina de planeación o quien haga sus veces, o al área encargada de gestionar el riesgo le corresponde liderar el proceso de administración de estos. Adicionalmente, esta misma oficina será la encargada de consolidar el mapa de riesgos de corrupción.

- Publicación del mapa de riesgos de corrupción: se debe publicar en la página web de la entidad, en la sección particular de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

La publicación será parcial, y fundamentada en la elaboración del Índice de Información Clasificada y Reservada. En dicho instrumento la entidad debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014)

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

En este caso, se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora no se hace visible en la publicación.

Se debe recordar que las excepciones solo pueden estar establecidas en una la ley, un decreto con fuerza de ley, o un tratado internacional ratificado por el Congreso o en la Constitución.

- **Socialización:** Los servidores públicos y contratistas de la entidad deben conocer su contenido antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces o la de gestión del riesgo, deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del Mapa de Riesgos de Corrupción.

Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos de corrupción. Deberá dejarse la evidencia del proceso de socialización y publicarse sus resultados.

- **Ajustes y modificaciones:** después de su publicación y durante el respectivo año de vigencia, se podrán realizar los ajustes y las modificaciones necesarias orientadas a mejorar el Mapa de Riesgos de Corrupción. En este caso deberá dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

- **Monitoreo**: en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción.

- **Seguimiento**: el jefe de control interno o quien haga sus veces, debe adelantar seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción.

TIPOLOGÍA DE RIESGOS

Estratégicos: Son los Asociados a la administración de la Entidad y se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la Administración.

De imagen: Relacionado con la percepción y la confianza por parte de la ciudadanía hacia la Institución.

Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, la estructura de la entidad y la articulación entre las áreas.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

Financieros: Relacionado con el manejo de recursos que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Tecnológicos: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

De corrupción: Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.

De información: Se asocia a la calidad, seguridad, oportunidad, pertinencia y confiabilidad de la información agregada y desagregada.

Riesgos de Seguridad Digital: Posibilidad Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

FORMATO DE DESCRIPCIÓN DEL RIESGO DE GESTIÓN Y CORRUPCIÓN

RIESGO	DESCRIPCIÓN	TIPO	CAUSAS	CONSECUENCIAS
		Operativo/ Corrupción		

FORMATO DE DESCRIPCIÓN DEL RIESGO DE SEGURIDAD DIGITAL

Los riesgos de seguridad digital se basan en la afectación de 3 criterios en un activo o un grupo de activos dentro del proceso: **"Integridad, confidencialidad o disponibilidad"**

Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización

ACTIVO	RIESGO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/VULNERABILIDADES	CONSECUENCIAS
				Seguridad Digital		

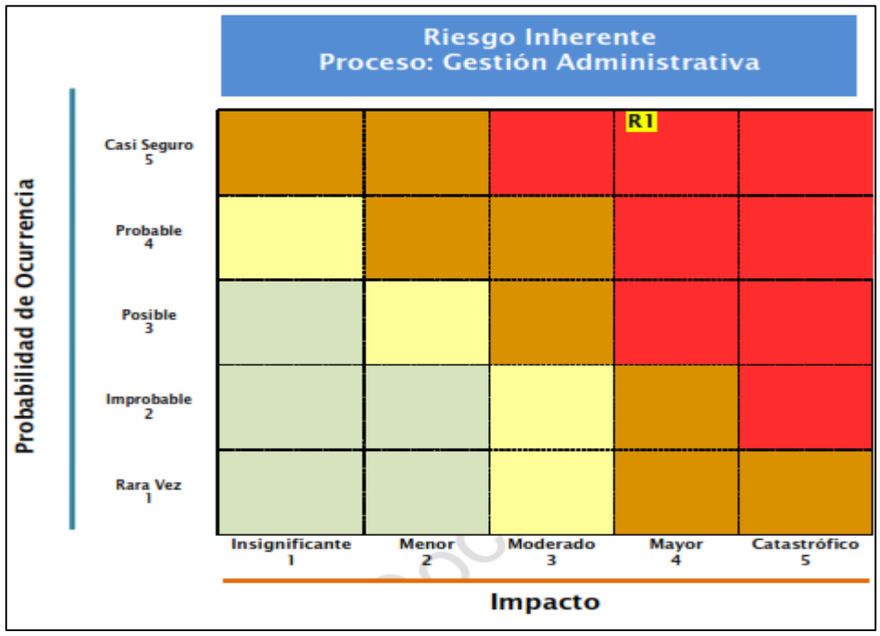
3. VALORACIÓN DEL RIESGO

3.1 ANÁLISIS DEL RIESGO

Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."



ZONA RIESGO EXTREMA	ZONA RIESGO ALTA	ZONA RIESGO MODERADA	ZONA RIESGO BAJA

Análisis de la Probabilidad

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.

Criterios parar calificar la probabilidad

Nivel	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

En este paso los integrantes del equipo de trabajo, a menos que posean datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, deben calificar en privado, (para no generar polémica o influencia en el criterio de los otros), el nivel de probabilidad en términos de factibilidad, de forma similar a la priorización de causas, para definir el nivel de probabilidad de cada riesgo, de acuerdo con la tabla de criterios establecida.

Matriz de priorización probabilidad

Nro	RIESGO	P1	P2	P3	P4	P5	P6	Tot	Prom
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	5	4	3	5	3	4	24	4 PROBABLE
2	Otros riesgos identificados								
3	Otros riesgos identificados								

Convenciones:
Nro: Número consecutivo del riesgo - P1: Participante 1 P… - Tot: Total puntaje -
Prom.: Promedio

CRITERIOS PARA CALIFICAR EL IMPACTO

Niveles para calificar el Impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

Niveles para calificar el Impacto	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
MODERADO	- Impacto que afecte la ejecución presupuestal en un valor ≥5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
Menor	- Impacto que afecte la ejecución presupuestal en un valor ≤1% - Pérdida de cobertura en la prestación de los servicios de la entidad ≤5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≤1% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≤1%del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
Insignificante	- Impacto que afecte la ejecución presupuestal en un valor ≤0,5% - Pérdida de cobertura en la prestación de los servicios de la entidad ≤1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≤0,5% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≤0,5%del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

VALORACIÓN DEL RIESGO

Criterios para calificar el Impacto – Riesgos de Seguridad Digital

Nivel asignado	Valor del impacto	Criterios de impacto para seguridad digital					
		Integridad (I)	Disponibilidad (D)	Confidencialidad (C)	Social (S)	Económica (E)	Ambiental (A)
INSIGNIFICANTE	1	Sin afectación de la integridad	Sin afectación de la disponibilidad	Sin afectación de la confidencialidad	Afectación del X % de la población o menos	Afectación del X % del presupuesto anual de la entidad o menos	Sin Afectación medioambiental
MENOR	2	Afectación muy leve de la integridad	Afectación muy leve de la disponibilidad	Afectación muy leve de la confidencialidad	Afectación del X % de la población	Afectación del X % del presupuesto anual de la entidad	Afectación leve del MA requiere de X meses de recuperación
MODERADO	3	Afectación leve de la integridad de la información debido al interés particular de los empleados y terceros	Afectación leve de la disponibilidad de la información debido al interés particular de los empleados y terceros	Afectación leve de la confidencialidad de la información debido al interés particular de los empleados y terceros	Afectación del X % de la población	Afectación del X % del presupuesto anual de la entidad	Afectación leve del MA requiere de X años de recuperación
MAYOR	4	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros	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	Afectación del X % de la población	Afectación del X % del presupuesto anual de la entidad	Afectación importante del MA que requiere de X años De recuperación
CATASTRÓFICO	5	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 confidencialidad de la información debido al interés particular de los empleados y terceros	Afectación del X % de la población	Afectación del X % del presupuesto anual de la entidad	Afectación muy grave del MA que requiere de X años de recuperación

Las variables de confidencialidad, integridad y disponibilidad se definen de acuerdo con el Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital (GD).

La variable población (social) se define teniendo en cuenta el establecimiento del contexto externo de la entidad. Esto significa que, para la variable social, la consideración

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites a través del entorno digital, y que de una forma u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto

La variable económica, la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental, estará también alineada con la afectación del entorno por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

Riesgo	Amenaza	Vulnerabilidad	Probabilidad	Impactos: Social	Económico	Ambiental	Confidencialidad	Integridad	Disponibilidad	Impacto del riesgo	Zona de riesgo
Pérdida de la Confidencialidad	Modificación no autorizada	Ausencia de políticas de control de acceso Contraseñas sin protección Ausencia de mecanismos de identificación y autenticación de usuarios Ausencia de bloqueo de sesión	3-posible	1-insignificante	3-moderado	N/A	2- menor	2- menor	N/A	2- menor	(6) Zona de riesgo Moderado

EJEMPLO

Promedio de las 4 Variables escogidas

NIVELES DE ACEPTACIÓN DEL RIESGO.

La medición de los riesgos de los procesos se hará teniendo en cuenta la siguiente tabla de probabilidad e impacto así:

	Probabilidad		Zona de Riesgos (Procesos)				
PROBABILIDAD	Casi seguro	5	Alto	Alto	Extremo	Extremo	Extremo
	Probable	4	Moderado	Alto	Alto	Extremo	Extremo
	Posible	3	Bajo	Moderado	Alto	Extremo	Extremo
	Improbable	2	Bajo	Bajo	Moderado	Alto	Extremo
	Rara vez	1	Bajo	Bajo	Moderado	Alto	Alto
	Impacto		1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrófico

IMPACTO

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

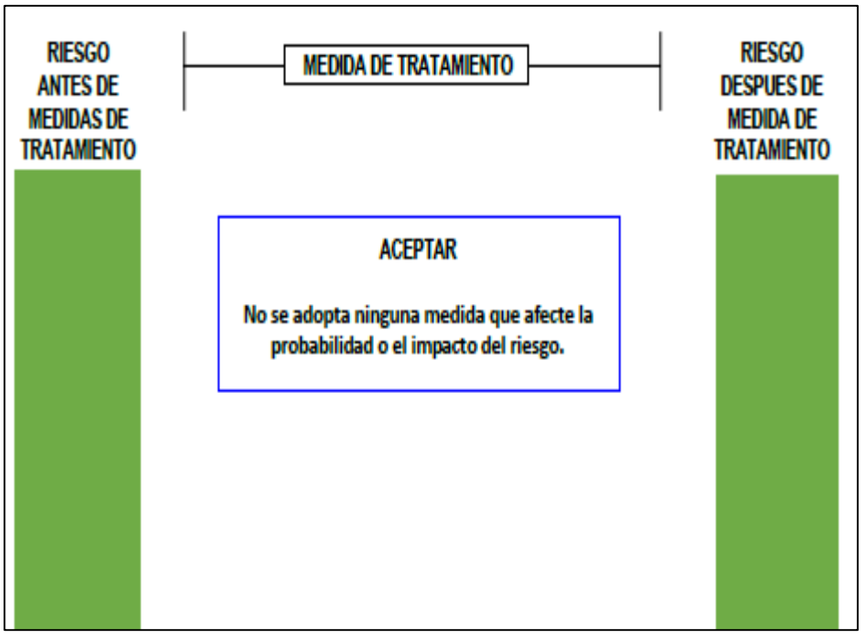
TRATAMIENTO DEL RIESGO

Es la respuesta establecida por la Primer Línea de Defensa para la mitigación de los diferentes riesgos, incluyendo los riesgos de Corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto del riesgo, y la relación costo beneficio de las medidas de tratamiento. Pero en caso de que una respuesta ante el riesgo, derive en un riesgo residual que supere los niveles aceptables para la dirección, se deberá volver a analizar y revisar dicho tratamiento. En todos los casos para los riesgos de corrupción, la respuesta será evitar, compartir o reducir el riesgo. **Ningún riesgo de corrupción podrá ser aceptado.**

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- **Aceptar el Riesgo.** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

Si el nivel de riesgo cumple con los criterios de aceptación de riesgo, no es necesario poner controles y el riesgo puede ser aceptado. Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo.



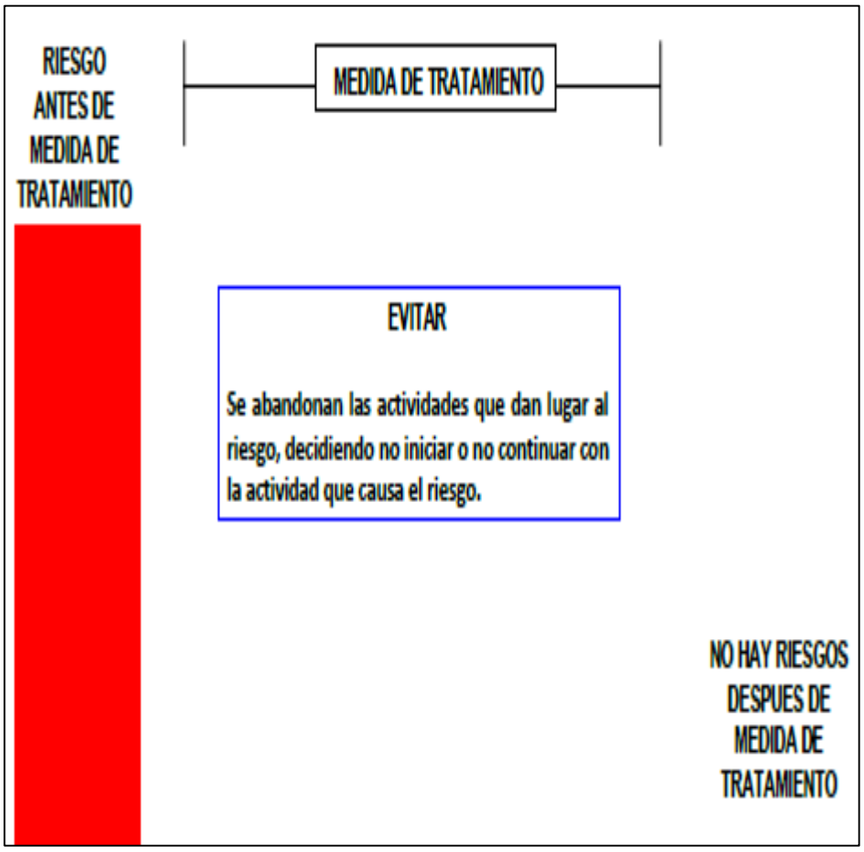
La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

- **Evitar el Riesgo.** Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.

Cuando los escenarios de riesgo identificado se consideran demasiados extremos, se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o conjunto de actividades.



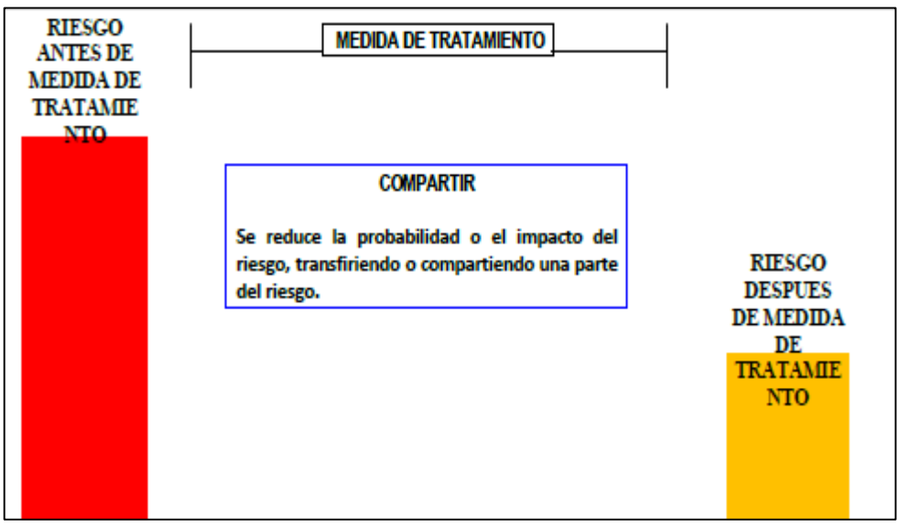
Desde el punto de vista de los responsables de la toma de decisiones, este tratamiento es simple, la menos arriesgada y menos costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y por lo tanto hay situaciones donde no es una opción.

- **Compartir el Riesgo.** Se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo.

Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable, o se carece de conocimientos necesarios para gestionarlo, el riesgo puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

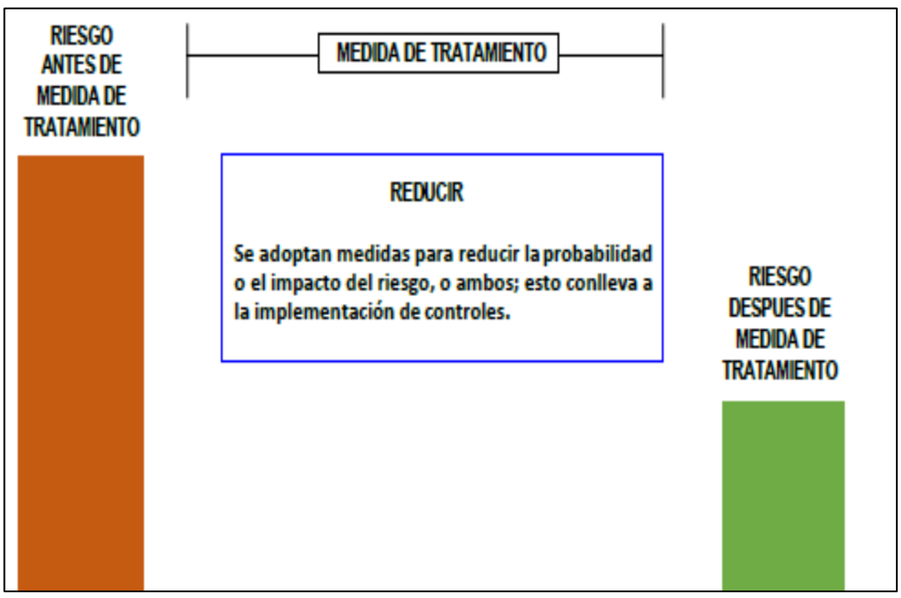
"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."



Los dos principales métodos de compartir o transferir parte del riesgo son, por ejemplo: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual.

- **Reducir el Riesgo.** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo.



RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

Deberían seleccionarse controles apropiados y con una adecuada segregación de funciones, permitiendo que el tratamiento al riesgo adoptado, logre la reducción prevista sobre el riesgo.

TRATAMIENTO DEL RIESGO – ROL DE LA PRIMERA LÍNEA DE DEFENSA

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.

Las actividades de control son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Estas actividades están documentadas en:

- **Políticas:** las políticas establecen las líneas generales del control interno
- **Procedimientos:** los procedimientos son los que llevan dichas políticas a la práctica

3.2 VALORACIÓN DEL RIESGO

Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

3.3 ANÁLISIS Y EVALUACIÓN DE CONTROLES

La valoración del riesgo requiere de una evaluación de los controles existentes, lo cual implica:

DETERMINAR SU NATURALEZA: Si se trata de un control preventivo, detectivo o correctivo, para este análisis tenga en cuenta.

CONTROLES PREVENTIVOS:

Evitan que un evento suceda. Por ejemplo, el requerimiento de un login y password en un sistema de información es un control preventivo. Éste previene (teóricamente) que personas no autorizadas puedan ingresar al sistema. Dentro de esta categoría pueden existir controles de tipo detectivo, los cuales permiten registrar un evento después de que ha sucedido, por ejemplo, registro de las entradas de todas las actividades llevadas a cabo en el sistema de información, traza de los registros realizados, de las personas que ingresaron, entre otros.

CONTROLES DETECTIVOS:

Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

VALORACIÓN DE LOS CONTROLES – DISEÑO DE CONTROLES

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo, se debe considerar desde la redacción del mismo, las siguientes variables

PASO 1	Debe tener definido el responsable de realizar la actividad de control.
PASO 2	Debe tener una periodicidad definida para su ejecución.
PASO 3	Debe indicar cuál es el propósito del control.
PASO 4	Debe establecer el cómo se realiza la actividad de control.
PASO 5	Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
PASO 6	Debe dejar evidencia de la ejecución del control.

1. **RESPONSABLE:** Persona asignada de ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si ese responsable quisiera hacer algo indebido, por sí solo, no lo podría hacer. Si la respuesta es que cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de su ejecución.

2. **PERIODICIDAD:** El control debe tener una periodicidad específica para su realización, (diario, mensual, trimestral, anual) etc. y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la periodicidad se debe evaluar si este previene o detecta de manera oportuna el riesgo. Una vez definido el paso 1 - Responsable del control, debe establecerse la periodicidad de su ejecución.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

Cada vez que se releva un control, debemos preguntarnos si la periodicidad en que se ejecuta el control ayuda a prevenir o detectar el riesgo de manera oportuna. Si la respuesta es SÍ, entonces la periodicidad del control está bien diseñada.

3. **PROPÓSITO:** El control debe tener un propósito que indique para qué se realiza el control, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar), o detectar la materialización del riesgo, y conlleve a que se realicen los ajustes y correctivos en el diseño del control o en su ejecución. El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas. Siguiendo las variables a considerar en la evaluación del diseño de control revisadas, veamos algunos ejemplos de cómo se deben redactar los controles, incluyendo el propósito de lo que busca el control.

4. **¿COMO SE REALIZA?:** El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control, es confiable para la mitigación del riesgo.
Cuando estemos evaluando el control, debemos preguntarnos, si la fuente de información utilizada ¿es información confiable?, imaginémonos, que la validación de que, si el proveedor cumple con los requisitos de contratación, no la estemos realizando con una lista de chequeo, si no de memoria, porque los requisitos no los sabemos de memoria, o que la conciliación la realicemos con un extracto de Bancos que fue suministrado por la misma área de cartera o a través de un archivo en Excel.

5. **OBSERVACIONES O DESVIACIONES:** El control debe indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control. Al momento de evaluar si un control está bien diseñado para mitigar el riesgo, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumple, la actividad no debería continuarse hasta que se subsane la situación o si es un control que detecta una posible materialización de un riesgo, debería gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas u observaciones. Sigamos con nuestros ejemplos prácticos de ayuda, para la interiorización de estos conceptos.

6. **EVIDENCIA:** El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control, y se pueda evaluar que el control realmente fue ejecutado de acuerdo a los parámetros establecidos y descriptos anteriormente:

1. Fue realizado por el responsable que se definió.
2. Se realizó de acuerdo a la periodicidad definida.
3. Se cumplió con el propósito del control.
4. Se dejó la fuente de información que sirvió de base para su ejecución.
5. Hay explicación a las observaciones o desviaciones resultantes de ejecutar el control.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

ANÁLISIS Y EVALUACIÓN DE LOS CONTROLES PARA LA MITIGACIÓN DE LOS RIESGOS.

Criterio de evaluación	Aspecto a Evaluar en el Diseño del Control	Opciones de respuesta	
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	Inoportuna
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.?	Prevenir o detectar	No es un control
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?.	Confiable	No confiable
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	No se investigan y resuelven oportunamente.
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?.	Completa	Incompleta / no existe

PESO O PARTICIPACIÓN DE CADA VARIABLE EN EL DISEÑO DEL CONTROL PARA LA MITIGACIÓN DEL RIESGO

Criterio de evaluación.	Opción de respuesta al criterio de evaluación	Peso en la evaluación del diseño del control
1.1 Asignación del responsable	Asignado	15
	No Asignado	0
1.2 Segregación y autoridad del responsable.	Adecuado	15
	Inadecuado	0
2. Periodicidad	Oportuna	15
	Inoportuna	0
3. Propósito	Prevenir	15
	Detectar	10
	No es un control	0
4. Cómo se realiza la actividad de control.	Confiable	15
	No confiable	0
5. Qué pasa con las observaciones o desviaciones	Se investigan y resuelven oportunamente	15
	No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control.	Completa	10
	Incompleta	5
	No existe	0

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

Resultados de la evaluación del diseño del control

El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables, para que un control se evalué como bien diseñado.

Rango de calificación del diseño	Resultado - peso en la evaluación del diseño del control
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Resultados de la evaluación de la ejecución del control

Aunque un control este bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurare por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación realizadas por auditoría interna o control interno.

Rango de calificación de la ejecución	Resultado - peso de la ejecución del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Análisis y evaluación de los controles para la mitigación de los riesgos

Dado que la calificación de riesgos inherentes y residuales se realiza al riesgo y no a cada causa, hay que consolidar el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto si ayudan al tratamiento de los riesgos, considerando tanto el diseño y ejecución individual y promedio de los controles.

En la evaluación del diseño y ejecución de los controles, las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que siempre la calificación de la solidez de cada control, asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, tal como se detalla en la siguiente tabla:

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

Peso del diseño individual o promedio de los controles. (DISEÑO)	El control se ejecuta de manera consistente por los responsables. (EJECUCIÓN)	Solidez individual de cada control fuerte:100 moderado:50 debil:0	Aplica plan de acción para fortalecer el control Sí / NO
fuerte calificación entre 96 y 100	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
moderado calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
débil entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sii

Nivel de riesgo (riesgo residual)

Desplazamiento del riesgo inherente para calcular el riesgo residual.

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual, se realizará de acuerdo a la siguiente tabla:

Tabla ilustrativa 8. Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos.

Solidez del conjunto de los controles.	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje de impacto
fuerte	directamente	directamente	2	2
fuerte	directamente	indirectamente	2	1
fuerte	directamente	no disminuye	2	0
fuerte	no disminuye	directamente	0	2
moderado	directamente	directamente	1	1
moderado	directamente	Indirectamente	1	0
moderado	directamente	no disminuye	1	0
moderado	no disminuye	directamente	0	1

4. MONITOREO Y REVISIÓN

El monitoreo y revisión debe asegurar que las acciones establecidas en los mapas de riesgo se están llevando a cabo y evaluar la eficacia en su implementación, adelantando revisiones sobre la marcha para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de acciones preventivas.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

El monitoreo debe estar a cargo de:

RESPONSABLES DE LOS PROCESOS:

El monitoreo y revisión de la gestión de riesgos, está alineado con la dimensión del MIPG de "Control Interno", que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad como sigue:

LÍNEA ESTRATÉGICA: Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.

1ª. Línea de defensa. Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.
Rol principal: diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad.
Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.

2ª. Línea de defensa. Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende

A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros.
Rol principal: monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

3ª. Línea de defensa. Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa

A cargo de la oficina de control interno, auditoría interna o quien haga sus veces.
El rol principal: proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I.
El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I.

REPORTE PLAN DE TRATAMIENTO DE RIESGOS

CONSOLIDAR INFORMACIÓN PARA LA GESTIÓN DEL RIESGO

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

- Una vez analizado el nivel de riesgo residual y definido el tratamiento a implementar con el establecimiento de controles preventivos y detectivos, es necesario generar un reporte que consolide la información clave del proceso de gestión del riesgo.

- En el formato de Mapa y Plan de Tratamiento de Riesgos, se inicia con el registro del riesgo identificado, luego se especifica la clase de riesgo, se transcriben las causas raíz o causas priorizadas, así como la probabilidad e impacto que quedaron después de valorar los controles para determinar el riesgo residual

- A partir de allí se deben analizar las estrategias DO y FA o estrategias de supervivencia formuladas en la etapa de establecimiento del contexto, que contrarresten las causas raíz, para colocarlas en las actividades de control del formato y con base en su contenido se establezca la opción de tratamiento a la que corresponden

- Luego se relaciona el soporte con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad o la periodicidad de ejecución.

- Al final de todas las actividades de control establecidas para atacar las causas del riesgo, se debe relacionar la acción de contingencia a implementar una vez el riesgo se materialice, para ello se deben analizar las estrategias DA o estrategias de fuga provenientes de la Matriz DOFA, seleccionando la(s) más apropiada(s) para el riesgo identificado.

- No olvidar colocar el soporte, responsable y tiempo de ejecución, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso o la estrategia.

- Por último, se formulan los indicadores clave de riesgo (KRI por sus siglas en ingles) que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control, siempre y cuando conduzcan a la toma de decisiones (Por riesgo identificado en los procesos)

INDICADORES -GESTIÓN DEL RIESGO DE SEGURIDAD DIGITAL

Igualmente, en el caso de los riesgos de seguridad digital, se deben generar indicadores, para medir la gestión realizada, en esencia la eficacia y la efectividad de los planes de tratamiento implementados.

La entidad debería definir como mínimo 2 indicadores POR PROCESO de la siguiente manera:

- 1 indicador de eficacia, que indique el cumplimiento de las actividades para la gestión del riesgo de seguridad digital en cada PROCESO de la entidad.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

- 1 indicador de efectividad, para cada riesgo o la suma de todos los riesgos de seguridad digital (pérdida de confidencialidad, de integridad, de disponibilidad).

EFICACIA:

Porcentaje de controles implementados = (#controles implementados / #controles definidos) x 100

EFECTIVIDAD:

Riesgos materializados de confidencialidad = (# de incidentes que afectaron la confidencialidad de algún activo del proceso)

Variación de incidentes de confidencialidad (para entidades con mediciones anteriores) =
((# de Incidentes de Confidencialidad Periodo Actual - # de Incidentes de Confidencialidad Periodo Previo) / Incidentes de Confidencialidad Periodo Previo) * 100%

SEGUIMIENTO RIESGOS DE CORRUPCIÓN

GESTIÓN RIESGOS DE CORRUPCIÓN

• **Seguimiento:** El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento a los Mapas de Riesgos. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

• ***Primer seguimiento:*** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

• ***Segundo seguimiento:*** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

• ***Tercer seguimiento:*** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la Entidad o en lugar de fácil acceso al ciudadano.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación de los Mapas de Riesgos en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

RESOLUCION No.1756 DE 2019
(Diciembre 05)

"POR LA CUAL SE ADOPTA LA POLÍTICA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL, Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS Y LOS MAPAS DE RIESGOS, PARA EL HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E."

5. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes involucradas tanto internas como externas debería tener lugar durante todas las etapas del proceso para la gestión del riesgo.
Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios.

Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

ARTÍCULO QUINTO: La presente resolución rige a partir de la fecha de su publicación y modifica la que le sean anteriores o contrarias.

COMUNIQUESE Y CUMPLASE:

Dada en Zarzal, Valle del Cauca, el quince (15) de enero de dos mil diecinueve (2019).

Jorge Luis de Jesús Bedoya Hincapie
Gerente E.S.E.

Proyectó: *Luz Marina Mayor Castaño, Asesor Control Interno.*
Revisó: *José Jair Gutierrez Corrales, Asesor Jurídico Externo.*
Transcribió: *Elizabeth Valencia A, Secretaria.*
Archivado en: *Carpeta Resoluciones.*