





**MANUAL DE ADMINISTRACIÓN DEL RIESGO
SANATORIO DE CONTRATACIÓN ESE**


	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

CONTENIDO

1.	OBJETIVOS	5
1.1.	OBJETIVO GENERAL.....	5
1.2.	OBJETIVOS ESPECÍFICOS	5
2.	ALCANCE	6
3.	TÉRMINOS Y DEFINICIONES	6
4.	ESTRUCTURA PARA LA GESTIÓN DEL RIESGO	7
4.1.	METODOLOGÍA	8
5.	GESTIÓN DEL RIESGO	9
5.1.	DEFINICIÓN POLÍTICA ADMINISTRACIÓN DEL RIESGO	9
5.2.	IDENTIFICACIÓN DEL RIESGO	10
5.3.	VALORACIÓN DEL RIESGO	14
5.3.1.	Análisis de riesgos.....	14
5.3.1.1.	Determinar la probabilidad.....	14
5.3.1.2.	Determinar el impacto.....	15
5.3.2.	Evaluación de riesgos.....	16
5.3.2.1.	Análisis preliminar (riesgo inherente)	16
5.3.2.2.	Valoración de controles	16
5.3.3.	Opciones de tratamiento riesgo	19
5.3.4.	Herramientas para la gestión del riesgo	20
5.3.4.1.	Gestión de eventos	20
5.3.4.2.	Indicadores clave de riesgo	21
5.3.5.	Monitoreo y revisión	21
5.3.5.1.	Línea estratégica	21
5.3.5.2.	Primera Línea de Defensa	21
5.3.5.3.	Segunda Línea de Defensa	22
5.3.5.4.	Tercera Línea de Defensa	22
5.4.	LINEAMIENTOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN	22
5.4.1.	Definición de riesgo de corrupción.....	23

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

5.4.2.	Generalidades acerca de los riesgos de corrupción.....	24
5.4.3.	Valoración de riesgos	25
5.4.3.1.	Análisis de la probabilidad	25
5.4.3.2.	Análisis del impacto.....	25
5.4.3.3.	Valoración de los controles – diseño de controles.....	27
5.4.3.4.	Nivel del riesgo (riesgo residual)	27
5.4.3.5.	Tratamiento del riesgo	27
5.4.3.6.	Monitoreo de riesgos de corrupción	28
5.4.3.7.	Reporte de la gestión del riesgo de corrupción	29
5.4.3.8.	Seguimiento de riesgos de corrupción.....	29
5.4.3.9.	Acciones en caso de materialización de riesgos de corrupción.....	29
5.5.	LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	30
5.5.1.	Identificación de los activos de seguridad de la información.....	30
5.5.2.	Identificación del riesgo	31
5.5.3.	Valoración del riesgo.....	32
5.5.4.	Controles asociados a la seguridad de la información	34
6.	CONTROL DE CAMBIOS	35
	REFERENCIAS	36


 Sanatorio de Contratación E.S.E.	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

INTRODUCCIÓN

La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales, tanto pública como privada, la cual cobra mayor importancia dado el dinamismo y los constantes cambios que el mundo globalizado de hoy exige. Estos cambios hacen que las entidades se enfrenten a factores internos y/o externos que pueden crear incertidumbre sobre el logro de los objetivos planteados.

El Sanatorio de Contratación E.S.E, comprometido con la calidad en la prestación del servicio de salud integral a los enfermos de Hansen y sus convivientes, así como a la población sana del Municipio de Contratación y su área de influencia, implementará una Política de Administración del Riesgo que permita controlar aquellos que puedan impedir el logro de los objetivos institucionales y de procesos, identificándolos, evaluándolos y estableciendo las acciones a llevar a cabo para su prevención, contando para ello con personal comprometido con el mejoramiento continuo de sus procesos, quienes evaluarán la efectividad de las acciones y controles establecidos.

La Política de Administración del Riesgo del Sanatorio de Contratación E.S.E., se basó en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 5 expedida por el Departamento Administrativo de la Función Pública (DAFP) en 2020, la cual tiene como fin unificar los lineamientos en los aspectos comunes de las metodologías para la administración de todo tipo de riesgos y fortalecer el enfoque preventivo con el fin de facilitar a las entidades, la identificación y tratamiento de cada uno de ellos.

 Sanatorio de Contratación E.S.E.	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01


1. OBJETIVOS

1.1. OBJETIVO GENERAL

Establecer los elementos y marco general para el control y la gestión del riesgo del Sanatorio de Contratación E.S.E, que permita a los funcionarios identificar, analizar y valorar los riesgos, que crean incertidumbre en el logro de los objetivos propuestos en cada proceso, en los objetivos estratégicos, incluyendo los riesgos de corrupción y los de seguridad de la información; a su vez dar las directrices para la gestión de los riesgos identificados y las pautas para definir las alternativas de acción encaminadas a reducirlos, mitigarlos o eliminarlos, dando un adecuado tratamiento, a fin de garantizar el cumplimiento de la misión, visión y los objetivos institucionales.

1.2. OBJETIVOS ESPECÍFICOS

- Generar una visión sistémica acerca de la administración y evaluación de los riesgos.
- Aumentar la probabilidad de alcanzar los objetivos y proporcionar un aseguramiento razonable con respecto al logro de estos.
- Proteger los recursos del Sanatorio de Contratación E.S.E., resguardándolos contra la materialización de los riesgos.
- Concientizar la necesidad de identificar y tratar los riesgos en todos los niveles de la entidad.
- Involucrar y comprometer a todos los servidores del Sanatorio de Contratación E.S.E., en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.
- Mejorar la eficacia y eficiencia operativa de la institución.
- Asegurar el cumplimiento normas, leyes y regulaciones.
- Identificar situaciones que, por sus características, pueden originar prácticas corruptas.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

2. ALCANCE


La Política de Administración del Riesgo del Sanatorio de Contratación E.S.E., aplica para todas los procesos y dependencias de la entidad y deben ser conocidas, aplicadas y cumplidas tanto por los servidores públicos como por los contratistas que apoyan la gestión y demás partes implicadas.

3. TÉRMINOS Y DEFINICIONES

- **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.


- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo
- **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.
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **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 Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente. Control: Medida que permite reducir o mitigar 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. Factores de Riesgo: Son las fuentes generadoras de riesgos.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

- **Integridad:** Propiedad de exactitud y completitud. Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
- **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.
- **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.
- **Apetito de 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 y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
- **Tolerancia del 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.
- **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 Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **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 Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **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.

4. ESTRUCTURA PARA LA GESTIÓN DEL RIESGO

Con el fin de ejercer una correcta Administración del Riesgo, el Sanatorio de Contratación E.S.E, adoptará la metodología propuesta por el Departamento Administrativo de la Función

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

Pública DAFP, para la presente política, el marco de referencia será la “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 2020”.

Para establecer los riesgos de corrupción se tendrá como referente el documento “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano Versión 2, contemplado en el Decreto 2641 de 2012 y la “Guía para la Gestión del Riesgo de Corrupción”, también los lineamientos que emita la Dirección de Control Interno y Racionalización de Trámites del Departamento Administrativo de la Función Pública DAFP.

Para los riesgos de corrupción, en particular se deben dar reportes de los siguientes documentos establecidos por la Oficina de Control Interno del Sanatorio de Contratación E.S.E.

1. Cronograma del Plan Anticorrupción y de Atención al Ciudadano, el cual comprende un tiempo máximo para las acciones que se deben ejecutar en cada vigencia por componente e indica quienes son los responsables de cada acción.
2. Mapa de riesgos de corrupción por procesos el cual es establecido para cada vigencia, con el fin de cumplir unas acciones para mitigar los riesgos.

En lo referente a los riesgos del proceso de adquisición de bienes y servicios y en general a los riesgos en materia de contratación, se tomará como referente metodológico el Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación de “Colombia Compra Eficiente”.

En el caso de los riesgos de seguridad digital, estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de privacidad y seguridad de la información.

El resultado de aplicar la metodología propuesta será el *Mapa de Riesgos por proceso y mapa de riesgo institucional* el cual será el registro que consolidará los riesgos identificados, los recursos y acciones que se establecieron para mitigar los mismos y los responsables para ejecutarlas.

4.1. METODOLOGÍA

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos:


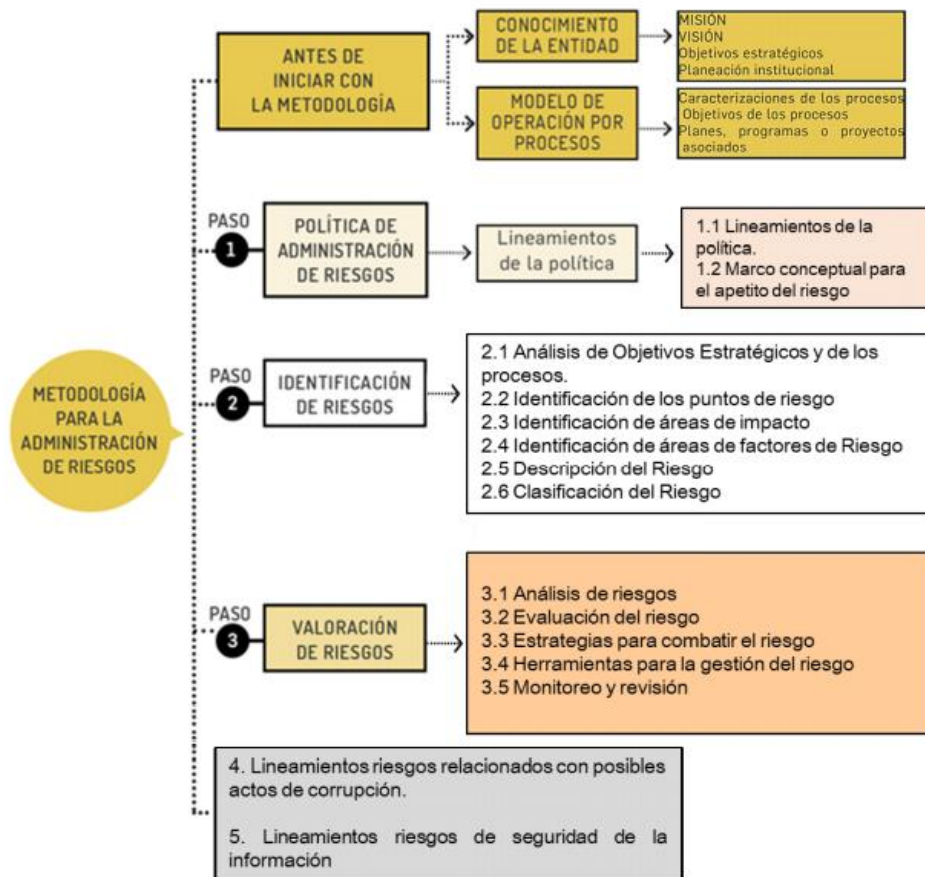
	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

Figura Metodología para la administración del riesgo




Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

5. GESTIÓN DEL RIESGO

5.1. DEFINICIÓN POLÍTICA ADMINISTRACIÓN DEL RIESGO


“El Sanatorio de Contratación Empresa Social del Estado, comprometido con el cumplimiento de su misión, visión y objetivos, implementará un Sistema de Administración de Riesgos estableciendo lineamientos precisos acerca del tratamiento, manejo, seguimiento y control a los riesgos que puedan impedir el logro de las metas institucionales y de sus procesos, contando para ello con una metodología de gestión del riesgo y personal comprometido con el mejoramiento continuo de sus procesos, quienes evaluarán la efectividad de las acciones y controles establecidos”.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01




5.2. IDENTIFICACIÓN DEL RIESGO

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:

- 1) **Análisis de objetivos estratégicos y de los procesos:** este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.
- 2) **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.
- 3) **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**.
- 4) **Identificación de áreas de factores de riesgo:** son las fuentes generadoras de riesgos. En la siguiente Tabla encontrará un listado con ejemplo de factores de riesgo que puede tener una entidad.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

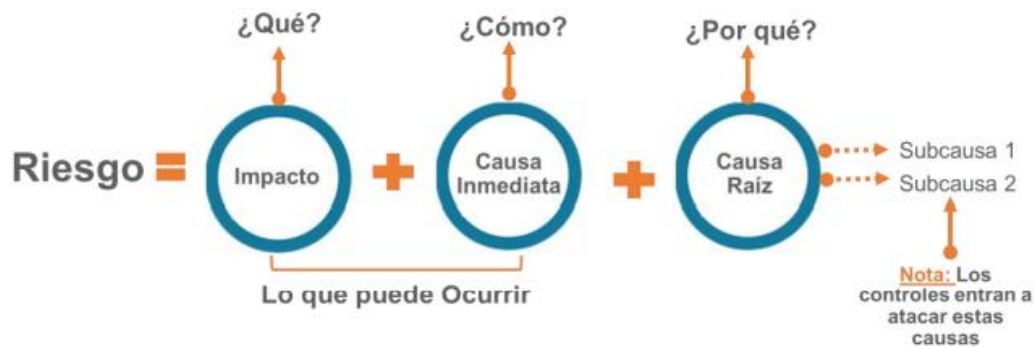
Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de aplicaciones
			Caída de redes
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos

Factor	Definición		Descripción
Evento externo	Situaciones externas que afectan la entidad.		Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

Fuente: Adaptado del curso de riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de la Función Pública. 2020

5) **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:


Figura Estructura propuesta para la redacción del riesgo



Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

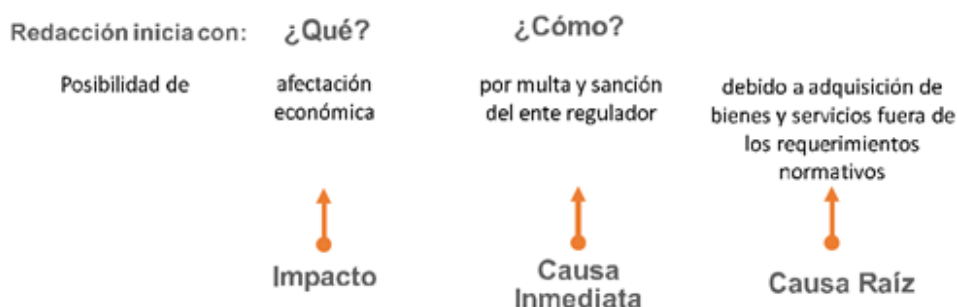
La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo. Desglosando la estructura propuesta tenemos:

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

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

- 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: es la causa principal o básica, corresponden 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 n existir más de una causa o subcausas que pueden ser analizadas.

Figura Ejemplo aplicado bajo la estructura propuesta para la redacción del riesgo




Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

- 6) Clasificación del riesgo:** permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla Clasificación de los riesgos

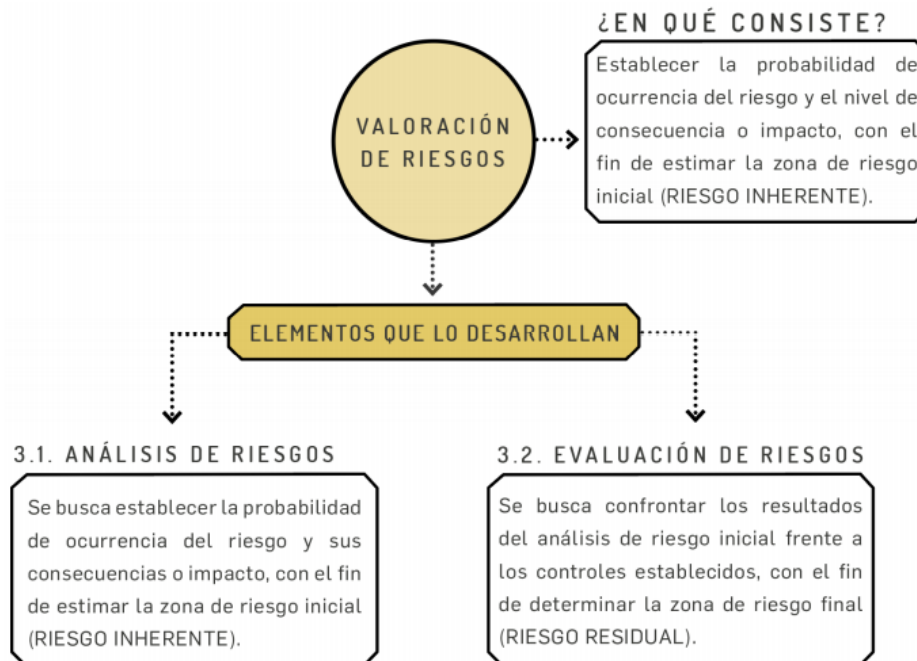
TIPO	DESCRIPCIÓN
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

5.3. VALORACIÓN DEL RIESGO

El proceso de valoración del riesgo se resume en la siguiente figura:



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.


5.3.1. Análisis de riesgos

En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

5.3.1.1. Determinar la probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

En la siguiente tabla se establecen los criterios para definir el nivel de probabilidad:

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.


5.3.1.2. Determinar el impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

En la siguiente tabla se establecen los criterios para definir el nivel de impacto.

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

IMPORTANTE: Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo.

5.3.2. Evaluación de riesgos

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

5.3.2.1. Análisis preliminar (riesgo inherente)

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor (ver figura Matriz de Calor).

Figura Matriz de calor (niveles de severidad del riesgo)


		TABLA DE SEVERIDAD				
		Impacto				
		Insignificante 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
Probabilidad	Muy Alto 100%	Alto	Alto	Alto	Alto	Extremo
	Alta 80%	Moderado	Moderado	Alto	Alto	Extremo
	Media 60%	Moderado	Moderado	Moderado	Alto	Extremo
	Baja 40%	Bajo	Moderado	Moderado	Alto	Extremo
	Muy Baja 20%	Bajo	Bajo	Moderado	Alto	Extremo

Fuente: Adaptado del Curso Riesgo Operativo. Universidad del Rosario.2020.

5.3.2.2. Valoración de controles

En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.

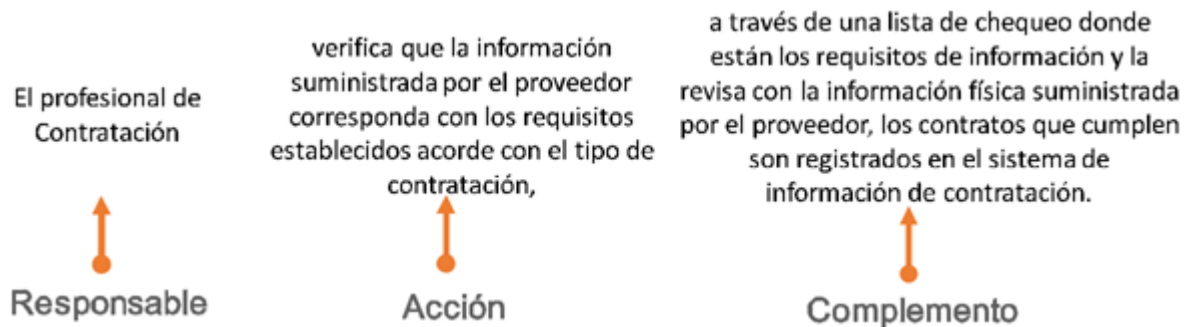
	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control: para una adecuada redacción del control, se establece la siguiente estructura que facilitará más adelante entender su tipología y otros atributos para su valoración:

- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

Ejemplo aplicado bajo la estructura propuesta para la redacción del control




Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Tipología de controles y los procesos: a través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión.

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- Control preventivo: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- Control detectivo: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- Control correctivo: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

- Control manual: controles que son ejecutados por personas.
- Control automático: son ejecutados por un sistema.

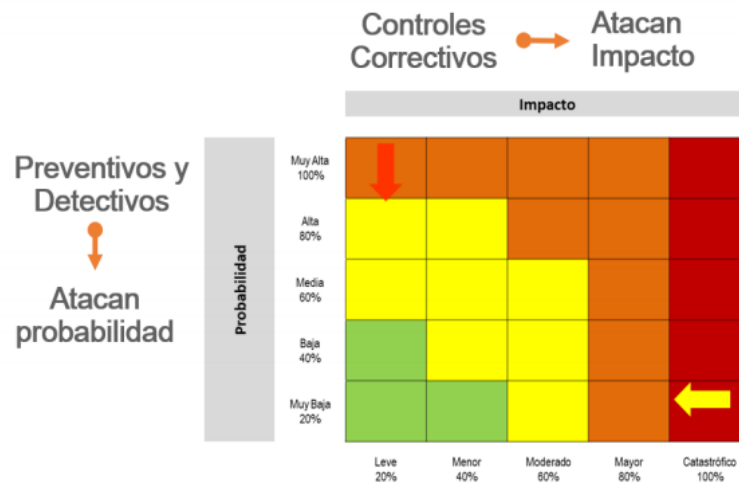
Análisis y evaluación de los controles – Atributos: A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así:

Características		Descripción	Peso	
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
*Atributos de Formalización	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	Con Registro	Corresponde a la evidencia de la ejecución del control Ejemplo: correos electrónicos, vistos buenos y documentos electrónicos seguridad, cartas con firma mecánica, firmas digitales, actas de Juan o Comités, firma de asistencia a capacitaciones, entre otros.	-
		Sin registro	Son aquellos controles que se ejecutan, pero al validar algún tipo de evidencia de su ejecución no es posible determinarla.	-

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Nota: Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles, tal y como se muestra en la siguiente figura:



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.


Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

El Sanatorio de Contratación Empresa Social del Estado ha establecido el formato “**PL-FO-04 Mapa de Riesgos**” para el registro de los mapas de riesgo.

5.3.3. Opciones de tratamiento riesgo

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

En la siguiente figura se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio¹ y se consideraría un control correctivo.


5.3.4. Herramientas para la gestión del riesgo

Como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes:

5.3.4.1. Gestión de eventos

Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología. Algunas fuentes para establecer una base histórica de eventos pueden ser:

¹ De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

- Mesa de ayuda
- Las PQRD (peticiones, quejas, reclamos, denuncias)
- Oficina jurídica
- Líneas internas de denuncia

Este mecanismo genera información para que el evento no se vuelva a presentar, así mismo, es posible establecer el desempeño de los controles así:

Desempeño del control = # eventos / frecuencia del riesgo (# veces que se hace la actividad)

5.3.4.2. Indicadores clave de riesgo

Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

5.3.5. Monitoreo y revisión

El modelo integrado de plantación y gestión (MIPG) desarrolla en la dimensión 7 control interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad.

5.3.5.1. 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.

5.3.5.2. Primera 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 programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la organización).

Rol principal: Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

5.3.5.3. Segunda 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: Jefe de Planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de contratación, entre otros.

Rol principal: Monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.

5.3.5.4. Tercera Línea de Defensa

Proporciona la información sobre la efectividad del Sistema de Control Interno - SCI, a través de un enfoque basado en riesgos, incluida la operación de la primera y la segunda línea de defensa.


A cargo de la oficina de Control Interno o quien haga sus veces.

Rol principal: Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del SCI.

El alcance de este aseguramiento, a través de auditoría interna cubre todos los componentes del SCI.

5.4. LINEAMIENTOS RIESGOS RELACIONADOS CON POSIBLES ACTOS DE CORRUPCIÓN

Para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018. Por lo anterior es necesario que, para formular el mapa de riesgos de corrupción, se remita a dicho documento. Para mayor facilidad, A continuación, se transcriben algunos de las pautas señaladas en la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

5.4.1. Definición de riesgo de corrupción

Es la 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 concurren los componentes de su definición, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO

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.

De acuerdo con la siguiente matriz, si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción:

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 dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

5.4.2. Generalidades acerca de los riesgos de corrupción


- Se elabora anualmente por cada responsable de proceso junto con su equipo.
- Consolidación: le corresponde a la oficina de planeación, liderar el proceso de administración de los riesgos de corrupción. 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 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 un 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.

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.

Las excepciones solo pueden estar establecidas en 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 el mapa de riesgos de corrupción antes de su publicación. Para lograr este propósito la oficina de planeación 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: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción después de su publicación y durante el respectivo año de vigencia. En este caso deberán 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.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

- 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.

5.4.3. Valoración de riesgos

5.4.3.1. 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.

Tabla criterios de probabilidad riesgos corrupción


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.

Fuente: DAFP

5.4.3.2. Análisis del impacto

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

Tabla criterios para calificar el impacto en riesgos de corrupción

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01


N.º	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA	
		SÍ	NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		
CATASTRÓFICO :	Genera consecuencias desastrosas para la entidad		

Nivel de impacto MAYOR

Fuente: Secretaría de Transparencia de la Presidencia de la República

IMPORTANTE: Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico.

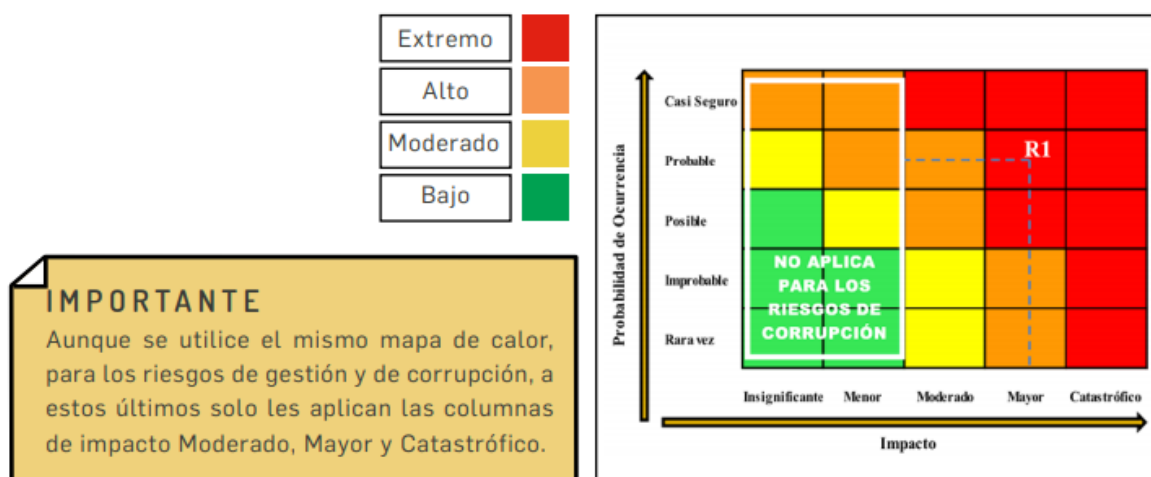
Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.

Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.

Tabla mapa de calor riesgos de corrupción



Fuente: Secretaría de Transparencia de la Presidencia de la República

5.4.3.3. Valoración de los controles – diseño de controles


Para el diseño de controles, los parámetros señalados en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de 2018, continúan vigentes, por lo tanto, es necesario remitirse a dicho documento.

5.4.3.4. Nivel del riesgo (riesgo residual)

IMPORTANTE: Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

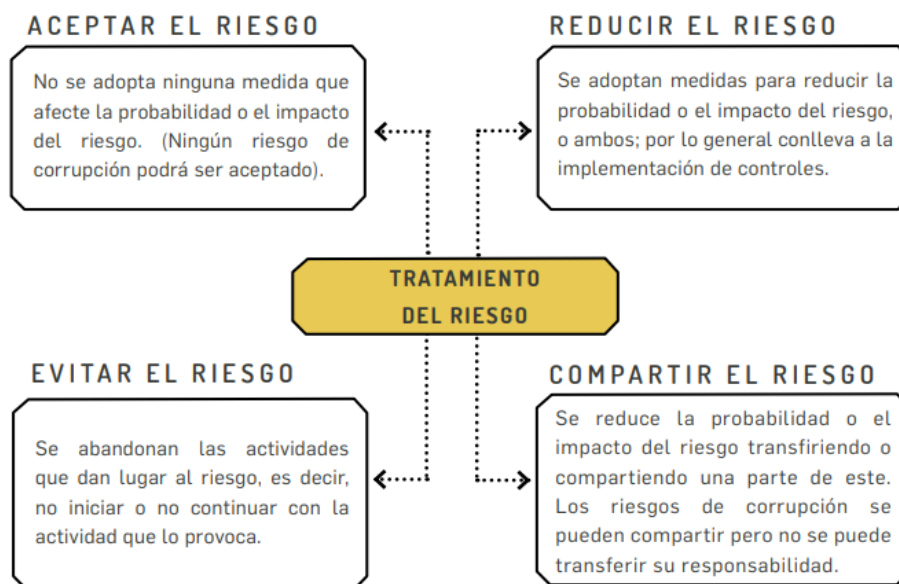
5.4.3.5. Tratamiento del riesgo

Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la 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 de este y la relación costo-beneficio de las medidas de

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

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

Tabla tratamiento riesgo de corrupción



Fuente: DAFP


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.

5.4.3.6. Monitoreo de riesgos de corrupción

El gerente del Sanatorio de Contratación E.S.E., y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa).

Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

5.4.3.7. Reporte de la gestión del riesgo de corrupción

De igual forma, se debe reportar en el mapa y plan de tratamiento de riesgos los riesgos de corrupción, de tal manera que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.


5.4.3.8. Seguimiento de riesgos de corrupción

- Seguimiento: El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. 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 un lugar de fácil acceso para el ciudadano.
- Verificar la publicación del Mapa de Riesgos de Corrupción 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.

5.4.3.9. Acciones en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

- 1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
- 2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- 3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- 4) Llevar a cabo un monitoreo permanente.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva. Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

5.5. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

5.5.1. Identificación de los activos de seguridad de la información


Como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

¿Qué son los activos de la información? Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización.

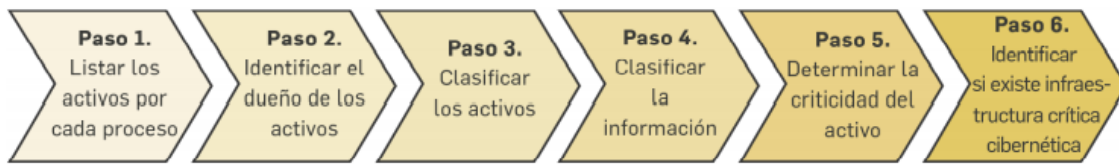
¿Por qué identificar los activos? Permite determinar qué es lo más importante que la entidad y sus procesos poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).

¿Qué son los activos? Servicios web, Redes, Información física o digital, Tecnologías de información TI, Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital.

¿Por qué identificar los activos de la información? La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digital.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

Pasos para la identificación de activos



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

Nota: para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas”.

Tabla ejemplo identificación activos del proceso

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el <i>front office</i> de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA


Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

5.5.2. Identificación del riesgo

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo 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. Para este efecto, es necesario consultar el Anexo 4 Modelo nacional de

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis:

- Tabla 5. Tabla de amenazas comunes
- Tabla 6. Tabla de amenazas dirigida por el hombre
- Tabla 7. Tabla de vulnerabilidades comunes

Nota: La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

Tabla de amenazas y vulnerabilidades de acuerdo con el tipo de activo

Tipo de activo	Ejemplos de vulnerabilidades	Ejemplos de vulnerabilidades
Hardware	Almacenamiento de medios sin protección	Hurto de medios o documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información
Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

5.5.3. Valoración del riesgo

Para esta etapa se utilizarán las tablas de probabilidad e impacto definidas en los numerales 5.3.1.1. y 5.3.1.2. del presente manual.

Para el análisis preliminar (riesgo inherente), en esta etapa se define el nivel de severidad para el riesgo de seguridad de la información identificado, para ello, se aplica la matriz de calor establecida en el numeral 5.3.2.1. del presente manual.

IMPORTANTE

Cada entidad deberá adaptar los criterios a su realidad.
El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Las variables 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) del Ministerio de Tecnologías de la Información y Las Comunicaciones.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una 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 presupuesto es 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 medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

Figura Valoración del riesgo en seguridad de la información


RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confidencialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

Extremo	
Alto	
Moderado	
Bajo	

IMPORTANTE:

La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

5.5.4. Controles asociados a la seguridad de la información

Se podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en el documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Tabla Controles para riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la pérdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del software y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.


	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

Figura Formato mapa riesgos seguridad de la información


N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	Pérdida de la integridad	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	Probable	Menor	Moderado	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	EFICACIA: Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100 EFFECTIVIDAD: Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
				Contraseñas sin protección	Reducir				A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018		
				Ausencia de mecanismos de identificación y autenticación de usuarios	Reducir				A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018		
				"Ausencia de bloqueo	Reducir				A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018		

*En este ejemplo el responsable de las actividades de control fue La Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

6. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ELABORADO POR	REVISADO POR	APROBADO POR	OBSERVACIONES
1		Alvaro Gamboa Rojas Encargado de Calidad	Comité Coordinador de Control Interno	Comité Institucional de Gestión y Desempeño	Creación del documento.

	MANUAL DE ADMINISTRACIÓN DEL RIESGO	Código: PL-MA-01
	PROCESO PLANEACIÓN INSTITUCIONAL	Versión: 01

REFERENCIAS

Guía para la administración del riesgo y el diseño de controles en entidades públicas.
Versión 5. Dirección de Gestión y Desempeño Institucional. Diciembre de 2020.