Función Pública

Instructivo Metodología de Riesgos - Usuarios

Oficina Asesora de Planeación
Septiembre 2024
Versión 08

Control de cambios

Versión	Fecha	Observaciones
1		Cambio de imagen del documento por cambio de gobierno
2		Actualización metodología de acuerdo a nueva guía de administración de riesgos versión 2018
3		Cambio de imagen del documento de acuerdo a plantilla emitida por el Proceso de Comunicaciones
4		Cambio de imagen del documento de acuerdo a plantilla emitida por el Proceso de Comunicaciones, se incluye estructura de redacción riesgo de corrupción, tabla impacto seguridad digital
5		Cambio de imagen del documento por cambio de gobierno
6		Actualización metodología de acuerdo a nueva guía de administración de riesgos versión 2020 - Se incluye el tema asociado al Plan de Continuidad del Negocio
7	2022-08-11	Cambio de imagen institucional debido a los lineamientos del nuevo gobierno Nacional
8	2024-09-25	Cambio de imagen institucional debido a los lineamientos del nuevo gobierno Nacional

Contenido

01

Glosario

Glosario

Concepto	Definición
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.
Amenazas	Situación potencial de un incidente no deseado , el cual puede ocasionar daño a un sistema o a una organización.
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.
Capacidad del 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 seria posible el logro de los objetivos de la entidad.
Causa	Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
Causa inmediata	Circunstancias bajo las cuales se presenta el riesgo, pero no constituye la causa principal o base para que se presente el riesgo
Causa Raíz	Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.

Glosario

Concepto	Definición
Confidencialidad	Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
Consecuencia	Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
Contingencia	Posible evento futuro, condición o eventualidad.
Continuidad del negocio	Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
Control	Medida que permite reducir o mitigar un riesgo.
Crisis	Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
Disponibilidad	Propiedad de ser accesible y utilizable a demanda por una entidad.
Factores de riesgo	Son las fuentes generadoras de riesgos.
Fraude	Acción de engaño intencional, que un servidor público o particular con funciones, públicas, realiza con el propósito de conseguir un beneficio o ventaja ilegal para si mismo o para un tercero

Glosario

Concepto	Definición
Gestión del riesgo	Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos
Impacto	Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
Integridad	Propiedad de exactitud y completitud
Mapa de riesgos	Documento que resume los resultados de las actividades de gestión de riesgos, incluye una presentación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos
Probabilidad	Se entiende la posibilidad de ocurrencia del riesgo, estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
Restablecimiento	Capacidad dela entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis
Riesgo	Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales

Glosario

Concepto	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.
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 Operativo	Posibilidad de incurrir en pérdidas por errores, fallas o deficiencias en el talento humano, procesos, tecnologías, infraestructura y eventos externos.
Riesgo Residual	El resultado de aplicar la efectividad de los controles al riesgo inherente.
Riego de seguridad digital	Efecto que se causa sobre los objetivos de las entidades, debido a amenazas y vulnerabilidades en el entorno digital.
Riesgo de seguridad de la información	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. ISO 27000
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.
Vulnerabilidad	Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Beneficios de la Gestión del Riesgo

1. Apoyo a la toma de decisiones
2. Garantizar la operación normal de la organización.
3. Minimizar la probabilidad e impacto de los riesgos.
4. Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos)
5. Fortalecimiento de la cultura de control de la organización.

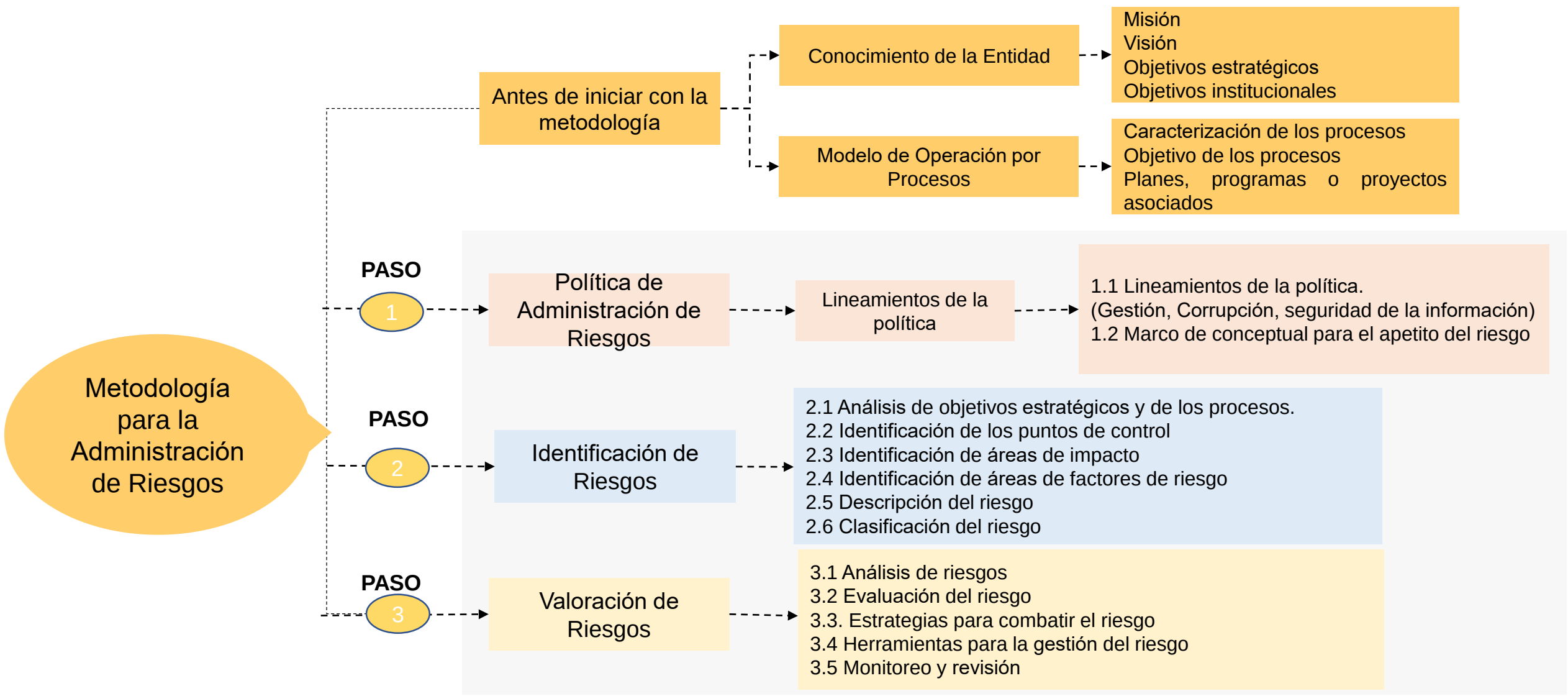
mipg | modelo integrado de planeación y gestión

Resultados que generen Valor Público

02

Metodología General

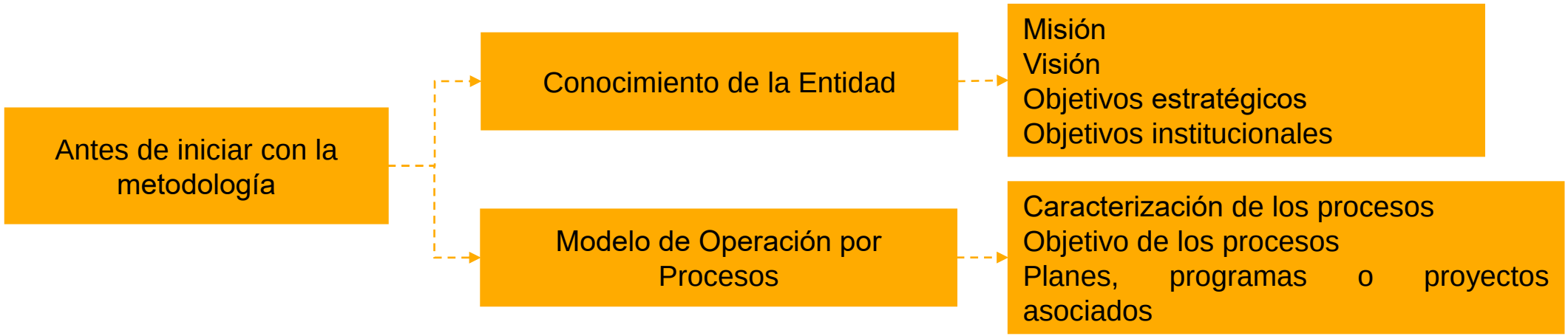
Metodología General



COMUNICACIÓN Y CONSULTA

Antes de iniciar la metodología

Es preciso analizar el contexto general de la Entidad, para establecer su complejidad, procesos, planeación institucional, permitiendo conocer y entender la Entidad y su entorno, lo que determinará el análisis de riesgos y la aplicación de la Metodología en general.



Consulta aquí:

SIPG

Plataforma Estratégica (Misión, visión, objetivos estratégicos)

Caracterizaciones del proceso

Planeación institucional

Planes, programas y proyectos

03

Política de administración de riesgos

Política de administración de riesgos

Qué es?

- La política de riesgos establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos. Es aplicable a todos los procesos, proyectos, planes de la entidad y a las actividades ejecutadas por los servidores durante el ejercicio de sus funciones.

Quién la establece?

- La establece la alta dirección de la entidad, en el marco del Comité Institucional de Coordinación de Control Interno.

Qué se debe tener en cuenta?

- Los objetivos estratégicos de la entidad.
- Nivel de responsabilidad frente al manejo de los riesgos.
- Mecanismos de comunicación para darla a conocer a todos los niveles de la entidad .

Qué debe contener?

- Objetivo
- Alcance
- Niveles de aceptación del riesgo
- Niveles para calificar el impacto
- Tratamiento de riesgos
- Periodicidad para el seguimiento de acuerdo con el nivel de riesgo residual
- Responsables del seguimiento

Consulta aquí Politica de Administración de Riesgos de Función Pública:

04

Identificación de riesgos

Contexto estratégico de Función Pública

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

CONTEXTO EXTERNO FUNCIÓN PÚBLICA	Políticos	Cambios de gobierno, legislación, políticas públicas, regulación
	Económicos y Financieros	Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia
	Sociales y culturales	Demografía, responsabilidad social, orden público
	Tecnológicos	Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	Ambientales	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible
	Legales y reglamentarios	Normatividad externa (leyes, decretos, ordenanzas y acuerdos)
	Comunicación externa	Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad

CONTEXTO INTERNO FUNCIÓN PÚBLICA	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 INTERNO 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
	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

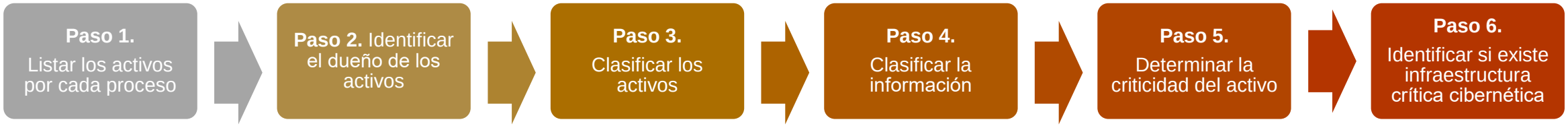
Consulta aquí Contexto Estratégico de Función Pública:

Identificación de activos

Solo existen tres (3) tipos de riesgos: pérdida de confidencialidad, pérdida de la integridad y pérdida de la disponibilidad de los activos de información. Para cada tipo de riesgo se podrán seleccionar las amenazas y las vulnerabilidades que puedan causar que dicho riesgo se materialice.

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

¿Cómo identificar los activos?



Identificación del riesgo

Esta etapa tiene como objetivo identificar los riesgos operativos que estén o no bajo el control de la entidad, teniendo en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance, y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Paso 1. Identificación del objetivo proceso

Todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo.

Paso 2. Identificación puntos de riesgo

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

Paso 3. Identificación áreas de impacto

Es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo

Paso 4. Identificación factores de riesgos

- Recurso Humano
- Procesos
- Infraestructura
- Tecnología
- Eventos Externos

Paso 5. Descripción del riesgo

Debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento para personas ajenas al proceso

No describir como riesgos omisiones ni desviaciones del control

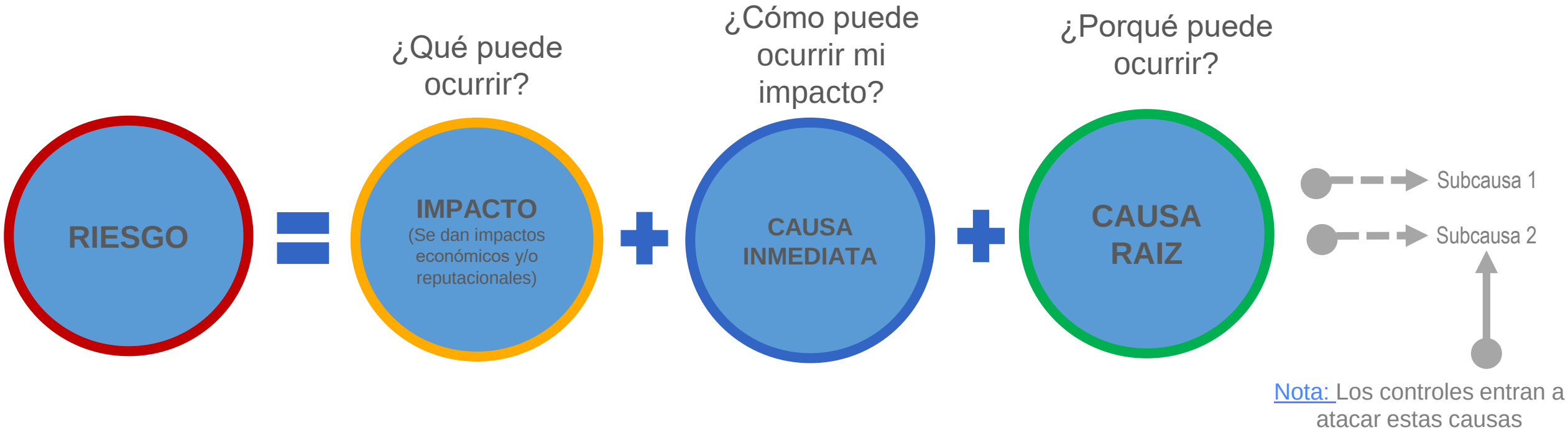
No describir causas como riesgos operativos

No describir riesgos como la negación de un control.

Tipología, factores y clasificación de riesgos

Tipología	Factores de Riesgo		Clasificación				
Riesgo operativo	Talento humano	Fraude interno	Pérdidas debido a actos de fraude, actuaciones irregulares, comisiones de hechos delictivos, infidelidades, abuso de confianza apropiación indebida o incumplimiento de regulaciones, legales o interna de la Entidad	Seguridad digital Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de los objetivos económicos y sociales, así como 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.	Continuidad del negocio Relacionado a la interrupción no deseada o escenarios que afecten la vida delas personas o bienes de la entidad, interrumpiendo sus funciones críticas parcial o totalmente	Grupos de valor, productos o servicios y practicas de la entidad Fallas negligentes o involuntarias de las obligaciones frente a los grupos de valor y que impiden satisfacer una obligaciones profesional frente a estos	Relaciones laborales Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleos, salud o seguridad del pago de demandas por daños personales o de discriminación
		Daño antijurídico	Falencia administrativa que ocasiona litigiosidad y puede ser tanto una acción como una omisión de la Entidad en desarrollo de sus actividades				
		Corrupción	Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado				
	Eventos externos	Fraude externo	Pérdidas derivadas de errores en la ejecución y administración de los procesos				
		Proveedores	Originado por las carencias del servicio prestado por proveedores y empresas subcontratadas				
	Procesos	Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de los procesos				
	Tecnología	Fallas tecnológicas	Pérdidas derivadas por fallas en hardware software, telecomunicaciones o interrupción en los servicios básicos				
	Infraestructura	Daños a activos físicos	Pérdidas por daños o extravíos de los activos físicos por desastres naturales y otros eventos				

Descripción del riesgo de gestión, seguridad digital y fiscal



Ejemplo: Posibilidad de incurrir en pérdidas económicas por multa o sanción del ente regulador debido a transmitir tarde el balance.

Descripción del 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 No 167 de 2013).

Componentes de su definición

Ejemplo:

Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.

05

Valoración del riesgo

Valoración del riesgo inherente

Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (riesgo inherente)

Riesgos Inherente
Nivel de riesgo propio de la actividad.
Resultado de combinar la probabilidad con el impacto, permite determinar el nivel de riesgo inherente dentro de unas escalas de severidad.

No es una operación matemática, sino una combinación de estos factores

Análisis de Riesgo de gestión y seguridad digital

En este punto se busca establecer la probabilidad de acuerdo a la exposición del riesgo y sus consecuencias o impactos.

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

La probabilidad inherente se basa en el número de veces en que se pasa por el punto de riesgo en el período de un año o exposición al riesgo.

Tabla de Impacto

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

El impacto es la consecuencia económica y/o reputacional que se genera por la materialización de un riesgo.

Impacto riesgos de corrupción

El impacto se mide según el efecto que puede causar el hecho de corrupción al cumplimiento de los fines de la Entidad. Para facilitar la asignación del puntaje es aconsejable diligenciar el siguiente formato:

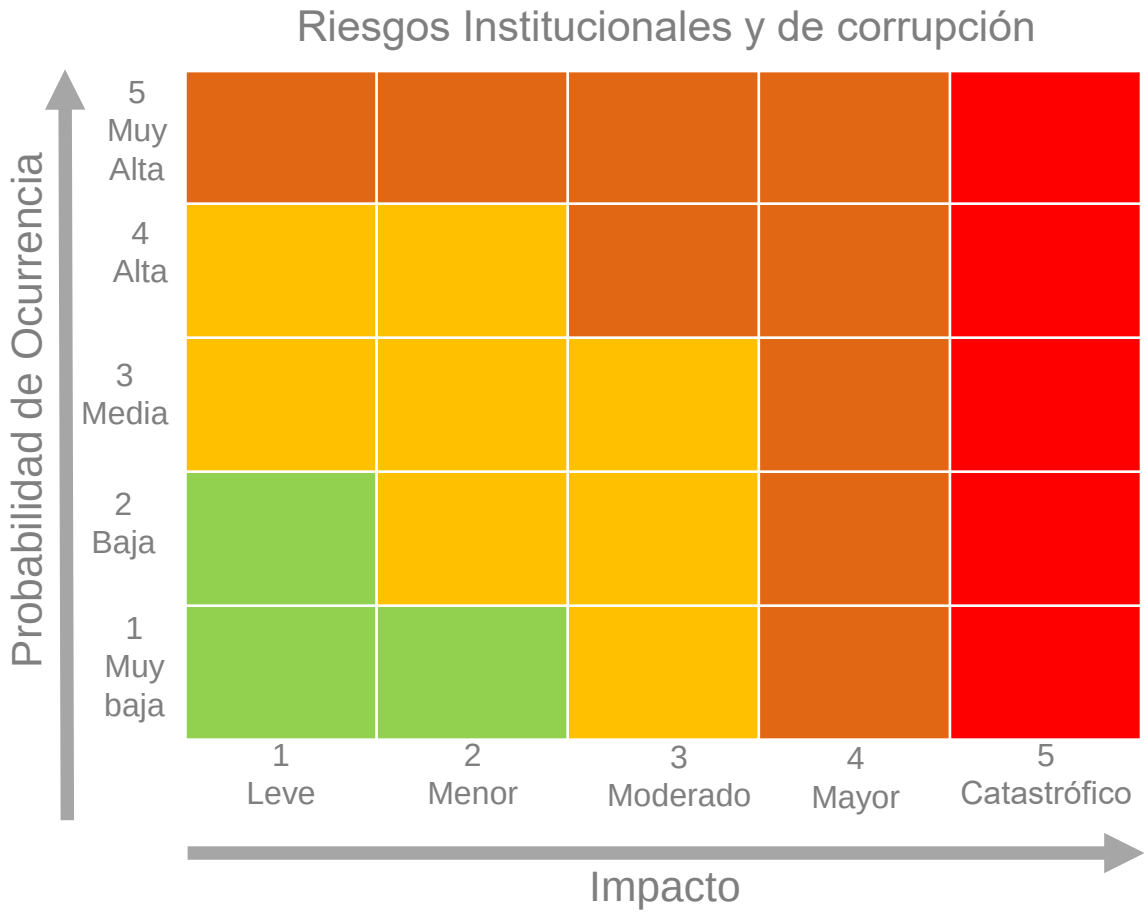
Medición Impacto Riesgo de Corrupción

NIVEL	DESCRIPTOR	DESCRIPCIÓN	RESPUESTAS AFIRMATIVAS
1	MODERADO	Genera medianas consecuencias sobre la entidad.	1 a 5
2	MAYOR	Genera altas consecuencias sobre la entidad.	6 a 11
3	CATASTRÓFICO	Genera consecuencias desastrosas para la entidad.	12 a 19

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PRODÍA…	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Evaluación del riesgo inherente

Se trata de determinar los niveles de severidad, cruzando los datos de probabilidad e impacto definidos, para obtener la **Zona de severidad.** Función Pública define 4 zonas de severidad en la siguiente matriz de calor.



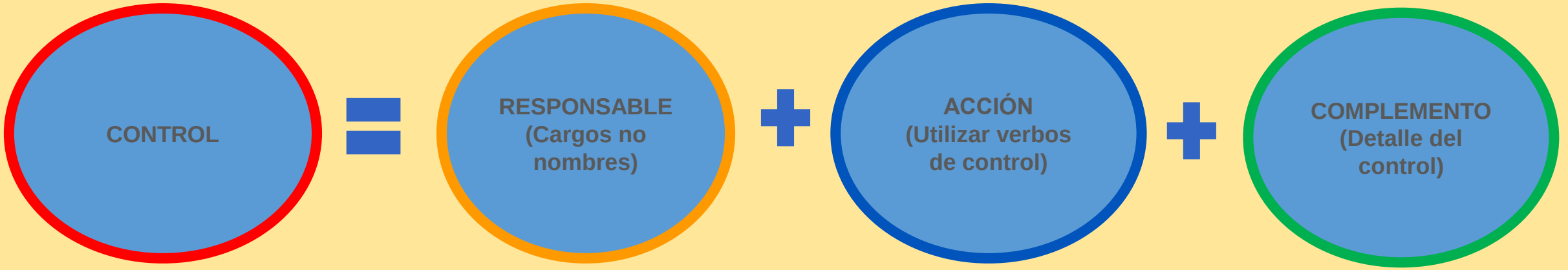
Zona de riesgo Extrema	Es responsabilidad del líder revisar y aprobar el riesgo y realiza seguimiento mensual.
Zona de riesgo Alta	Es responsabilidad del líder revisar y aprobar el riesgo y realiza seguimiento bimestral.
Zona de riesgo Moderada	Es responsabilidad del líder revisar y aprobar el riesgo y realiza seguimiento trimestral
Zona de riesgo Baja	Es responsabilidad del líder revisar y aprobar el riesgo y realiza seguimiento semestral

Identificación de controles

Un control se define como la medida que permite reducir o mitigar el riesgo, la identificación de controles se debe realizar para cada riesgo a través de las entrevistas con los funcionarios expertos.

Los responsables de implementar y monitorear los controles son los lideres de proceso.

La descripción del control debe contener los siguientes elementos:



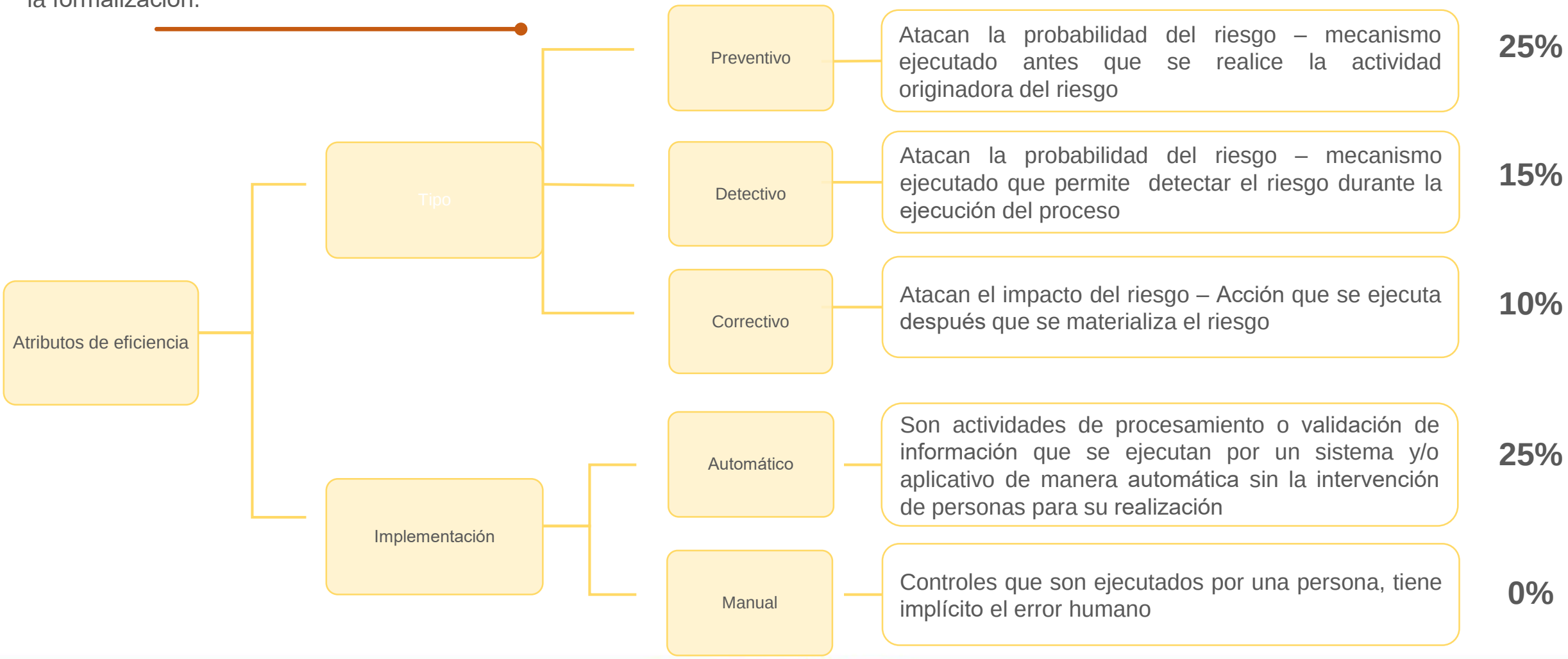
El Jefe de contratación

Verifica en el sistema de información de contratación la información registrada por el profesional asignado y aprueba el proceso para firma del ordenador del gasto

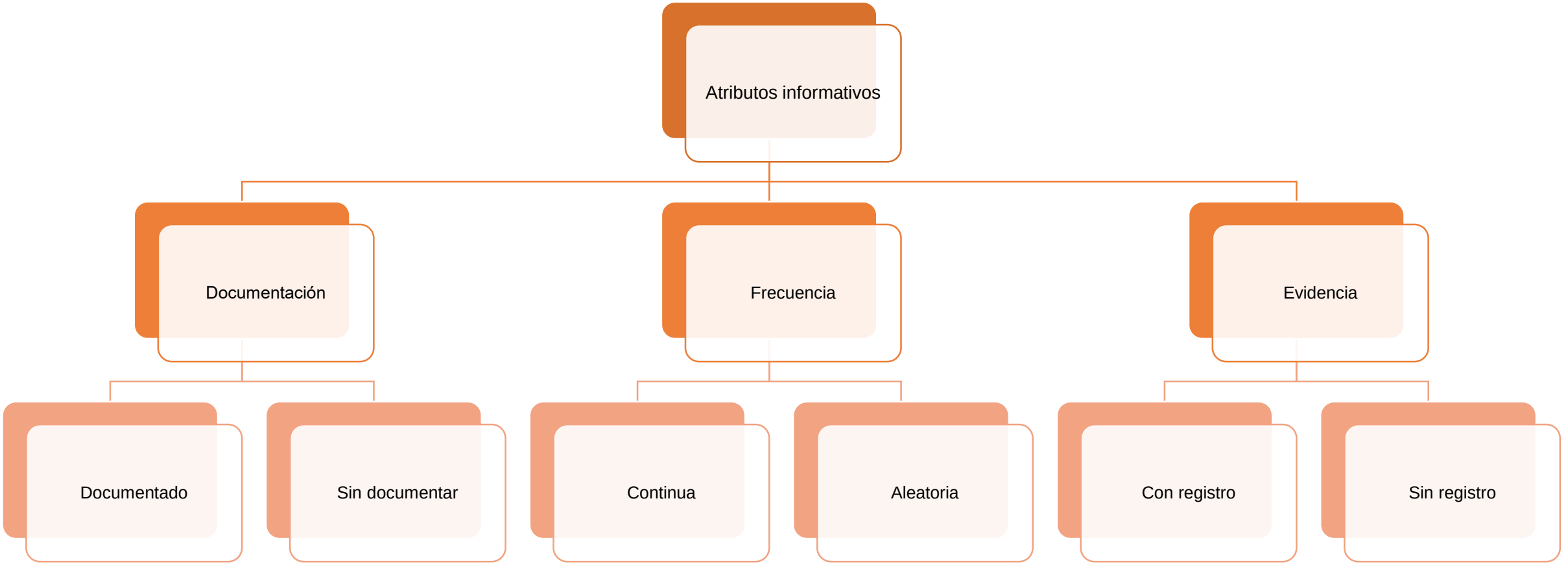
En el aplicativo contable queda el registro correspondiente, en caso de encontrar inconsistencias devuelve el proceso al profesional de contratos asignado

Atributos para el diseño del control

A continuación se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.



Atributos para el diseño del control



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; éstos no tienen una incidencia directa en su efectividad.

Nivel de riesgo residual

Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que éstos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Función Pública tiene como política una reducción del control máximo del 50%, con el fin de evitar que un solo control genere movimientos exagerados dentro de la matriz.

Nivel de riesgo residual

Se da continuación un ejemplo, donde se observan los cálculos requeridos para la aplicación de los controles, teniendo en cuenta las tablas del numeral 4.2.3

Riesgo Residual = R. Inherente – (R. Inherente * Control)

Controles y sus características				Peso	Política de reducción 50%
Control 1 El profesional del área de contratos, verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	Tipo	Preventivo	X	49%	
		Detectivo			
		Correctivo			
	Implementación	Automático			
		Manual	X	25%	
	Documentación	Documentado	X	-	-
		Sin Documentar		-	-
	Frecuencia	Continua	X	-	-
		Aleatoria		-	-
	Evidencia	Registro Sustancial		-	-
		Registro Material	X	-	-
		Sin registro		-	-
Total valoración control 1				**74%**	**37%**
Control 2 El jefe de Contratos, verifica en el sistema de información de contratación la información registrada por el profesional asignado, y aprueba el proceso para firma del ordenador del gasto, en el sistema de información queda el registro correspondiente, en caso de encontrar inconsistencias devuelve el proceso al profesional de contratos asignado.	Tipo	Preventivo			
		Detectivo	X	33%	
		Correctivo			
	Implementación	Automático			
		Manual	X	25%	
	Documentación	Documentado	X	-	-
		Sin Documentar		-	-
	Frecuencia	Continua	X	-	-
		Aleatoria		-	-
	Evidencia	Registro Sustancial	X	-	-
		Registro Material		-	-
		Sin registro		-	-
Total valoración control 2				**58%**	**29%**

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad Inherente	60%	Valoración control 1 preventivo	37%	60%* 37% = 22.2 60% - 22,2% = 37,8%
	Valor probabilidad para aplicar 2o control	37,8%	Valoración control 2 detectivo	29%	37,8%* 29% = 10,96 37,8% - 10,96% = 26,8%
	Probabilidad Residual	**26,8%**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

Evaluación del riesgo residual

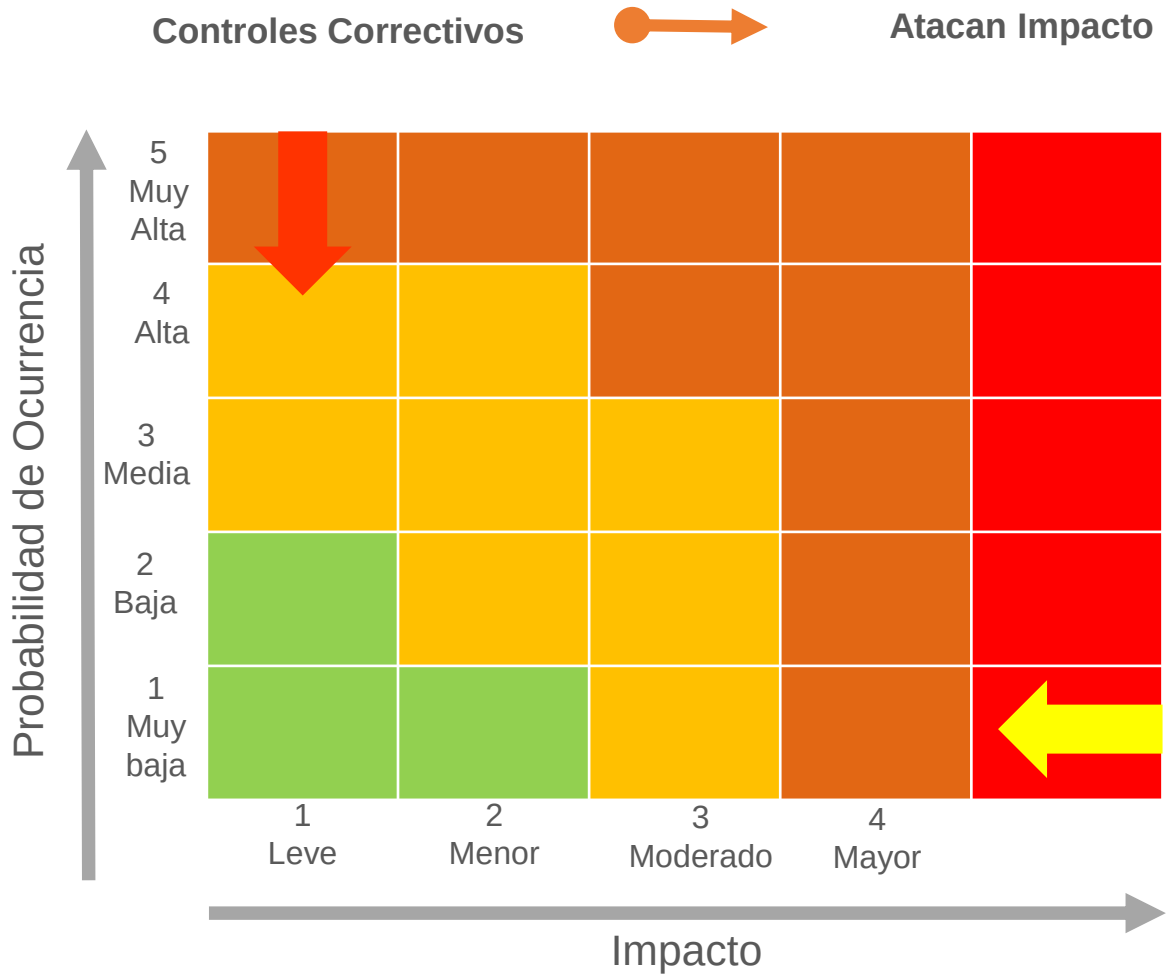
Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, y considerando si lo controles ayudan o no a la disminución de impacto o la probabilidad, procedemos a la elaboración del Mapa de Riesgo Residual (después de los controles)

Con la calificación obtenida se realiza un desplazamiento en la matriz así:

- Si el control afecta la **probabilidad** se desplaza hacia **abajo**
- Si afecta el **impacto** se desplaza a la **izquierda**

Preventivos y Detectivos

Atacan probabilidad



Estrategia para combatir el riesgo

Reducir

Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.

Transferir

Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas.
La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.

Mitigar

Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional

Aceptar

Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

Evitar

Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

Estrategia para combatir el riesgo

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

Al plan de acción referido para la opción de reducir requerirá:

- Responsable
- Fecha de implementación
- Fecha de seguimiento.

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de tratamiento
Riesgos de Gestión, y Seguridad digital	Baja	Se realiza seguimiento **SEMESTRAL** y se registran sus avances en el módulo de riesgos-SGI.
	Moderada	Se realiza seguimiento **TRIMESTRAL** y se registran sus avances en el módulo de riesgos-SGI
	Alta	Se realiza seguimiento **BIMESTRAL** y se registran sus avances en el módulo de riesgos-SGI
	Extrema	Se realiza seguimiento **MENSUAL** y se registra en el módulo de riesgos – SGI.
Riesgos de Corrupción	Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento **MENSUAL** y se registra en el módulo de riesgos – SGI.	

06

Monitoreo y revisión

Estructura mapa de riesgos

Como producto de la aplicación de la metodología se contará con el mapa de riesgo, que cuenta con la siguiente estructura:

Función Pública

Mapa de Riesgos Institucional 20XX
Versión XX - Enero del 20XX

Función Pública

Mapa de Riesgos Institucional 20XX
Versión XX - Enero del 20XX

Ítem	Materializado	Proceso	Dependencia	Estado	Código	Riesgo	Clasificación	Activos	Zona Inherente	Zona Residual	Tratamiento	Periodicidad	No. Controles	Controles
1	NO	Gestión del Talento Humano	Grupo de Gestión Humana	APROBADO	002	Posibilidad de pérdida económica por multa o sanciones del ente regulador Unidad de Gestión Pensional y Parafiscales (UGPP) debido a la omisión en la liquidación y pago de la seguridad social y aportes a parafiscales.	Ejecución y administración de procesos	No Aplica	Riesgo Moderado	Riesgo Moderado	REDUCIR - MITIGAR	TRIMESTRAL	1	El profesional encargado de nómina, mensualmente valida que el cálculo de la seguridad social del sistema de información sea el mismo que el cálculo manual con base a una muestra aleatoria del 10% de los servidores.

La Oficina Asesora de Planeación consolida la Matriz de riesgos Institucional con los riesgos en nivel Alto, Extremo y de Corrupción, debe publicarse antes del 31 de enero de cada vigencia en el Portal web, previa consulta ante los grupos de valor.

Monitoreo, revisión y reporte

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

Ver política de administración de riesgos – Responsabilidades de las líneas de defensa

Función Pública

Carrera 6 No. 12 - 62
Bogotá D.C. Colombia
Teléfono: **601 7395656**
Fax: **601 7395657**
Código Posta: 1117111
Página web: **www.funcionpublica.gov.co**
Email: **eva@funcionpublica.gov.co**