Concejo de Bogotá

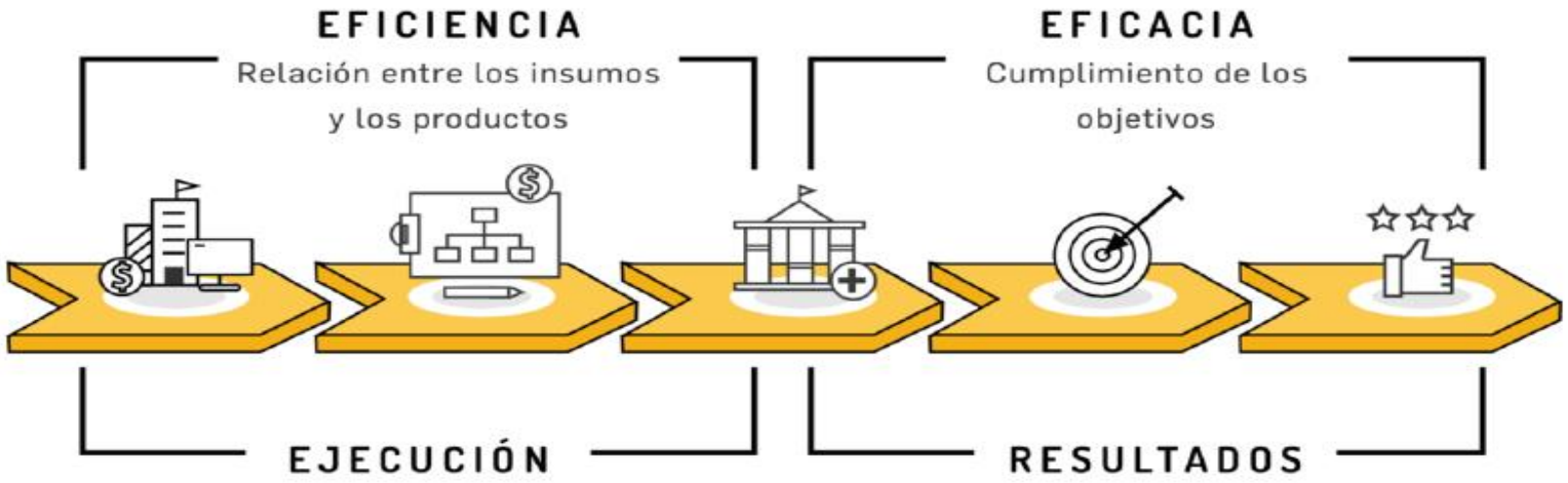
ADMINISTRACIÓN DEL RIESGO

OBJETIVOS SESIÓN

Compartir conceptos y metodologías disponibles para la implementación del Componente Evaluación del Riesgo de la Dimensión de Control Interno del MIPG.

Generar en los auditores de la Oficina de Control Interno la disposición de algunos elementos importantes a tener en cuenta en las diferentes auditorias programas para ejecutar en el tema de riesgos.

CADENA DE VALOR



Insumos	Procesos	Productos	Resultados o efectos	Impactos
Recursos financieros, humanos y materiales empleados para generar los productos.	Actividades realizadas para transformar los insumos en productos.	Bienes y servicios elaborados que requiere la población para satisfacer una demanda o dar respuesta a las causas concretas de un problema.	Cambios en el comportamiento o en el estado de los beneficiarios como consecuencia de recibir los productos (bienes o servicios).	Cambios en las condiciones de vida en la población objetivo. Mayor valor público en términos de bienestar, prosperidad general y calidad de vida de la población.

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2017.

OBJETIVO GENERAL

Facilitar el cumplimiento de la visión, misión y objetivos institucionales de una entidad, a través de la prevención y administración de los riesgos.

OBJETIVOS ESPECIFICOS

- Apoyar la toma de decisiones.
- Involucrar y comprometer a todos los servidores, en la búsqueda de acciones encaminadas a prevenir y administrar el riesgo.
- Introducir la A.R. dentro de los procesos y procedimientos.
- Proteger los recursos del Estado.
- Generar una visión sistémica acerca de la administración y la evaluación de riesgos.
- Asegurar el cumplimiento de las normas, leyes y regulaciones.
- Propender porque cada entidad interactúe con otras para fortalecer su desarrolle.

ROL DE LA OFICINA DE CONTROL INTERNO

Rol Directo:
Asesorar el proceso de administración de los riesgos institucionales.
Realizar recomendaciones preventivas y/o correctivas.
Hacer seguimiento a la evaluación de los riesgos.

Rol Indirecto:
Velar por la implementación de la política de administración del riesgo.

La OCI en su función asesora y evaluadora debe acompañar y comprometer a la alta dirección y funcionarios en general, en el ejercicio y cumplimiento de las acciones programadas para la administración del riesgo.

DEFINICIÓN DE RIESGOS

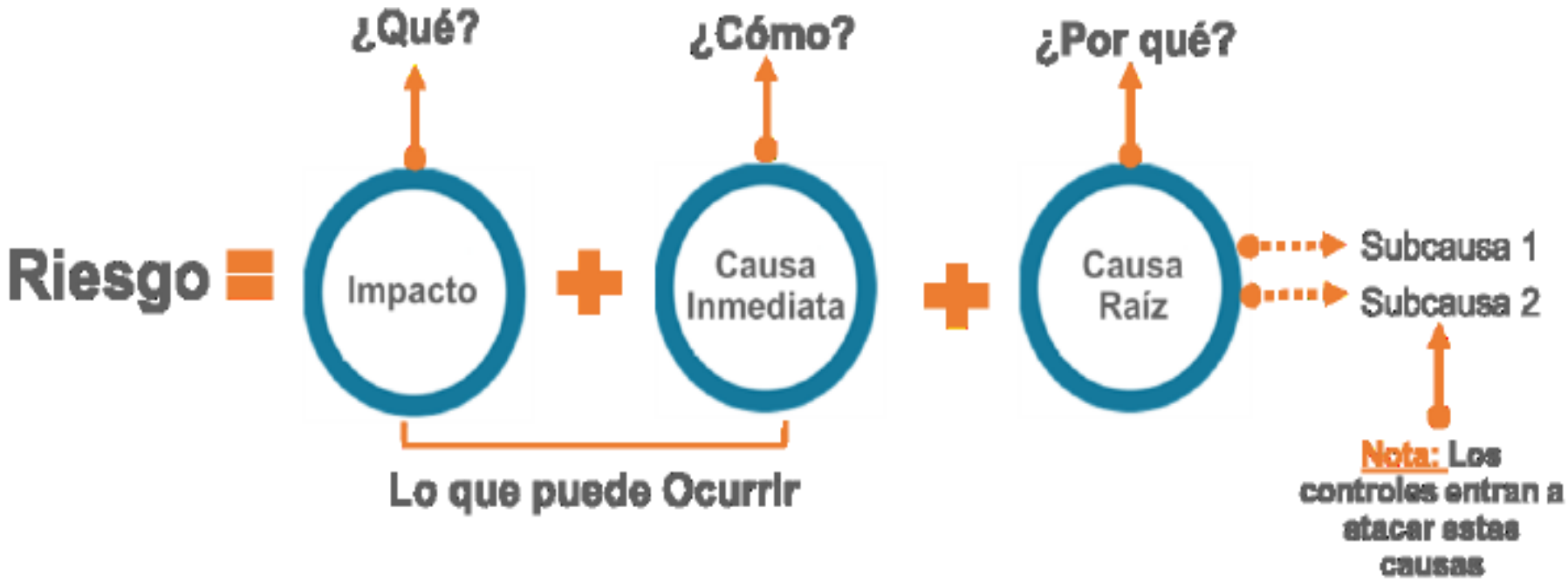
EL RIESGO

Evento indeseable con potencial daño.

Efecto de la incertidumbre sobre los objetivos. (3,1 de la ISO 31000 de 2018).

Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

ESTRUCTURA REDACCION 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.

AUDITORÍA

La auditoría se constituye en “una actividad independiente y objetiva de aseguramiento y consultoría, concebida para agregar valor y mejorar las operaciones de la entidad. Ayuda a las organizaciones a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno. (IIA GLOBAL. Marco internacional para la practica profesional de auditoría interna, 2017, p 17).

AUDITORÍA

Entre los factores que el auditor interno debe incluir en el Plan de Auditoría, están:

- Riesgos inherentes.
- Riesgos residuales.
- Controles de mitigación.
- Planes de tratamiento.
- Registros de riesgos: Sistemáticos, completos y precisos.
- Documentación.

EL RETOS DE LA DIRECCIÓN Y LA ADMINISTRACIÓN DEL RIESGO

HERRAMIENTAS DE ADMINISTRACIÓN DEL RIESGO

ESTANDARES DE ADMINISTRACIÓN DE RIESGOS

La Administración del Riesgo (AS/NZ 4360) ®

El modelo integral de Control Interno basado en el modelo *COSO ®*

La Auto Evaluación (CRSA)

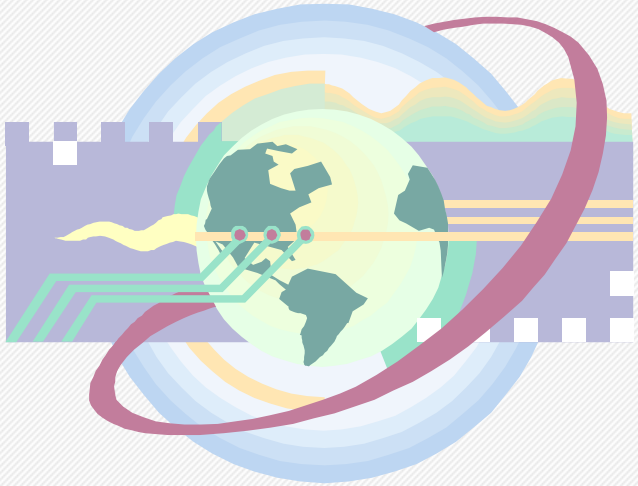
La Gestión, Control y Auditoría de la Tecnología de Información, con base en el modelo *CobIT ®*

El proceso de Auditoría Paso a Paso o basado en la Administración del Riesgo, (*Estándares del IIA ®*)

Estandar de Administración del Riesgo
(Risk Management Standard)

- Proyectos e Inversiones.
- Programas de prevención de fraudes.
- Cambios Organizacionales y Tecnológicos.
- Aspectos ambientales.
- Planeamiento de contingencias y desastres de TI.
- Salud y Seguridad Ocupacional.
- Operaciones en moneda extranjera.
- Sistemas de información y redes.
- Administración de Activos.

ESTANDAR COSO



- **Modelo Internacional de Control Integral, diseñado para apoyar a la Dirección en un mejor control de su organización.**
- **Provee un estándar, para la evaluación del control interno e identificar las "mejores prácticas" aplicables.**

ESTANDAR COSO

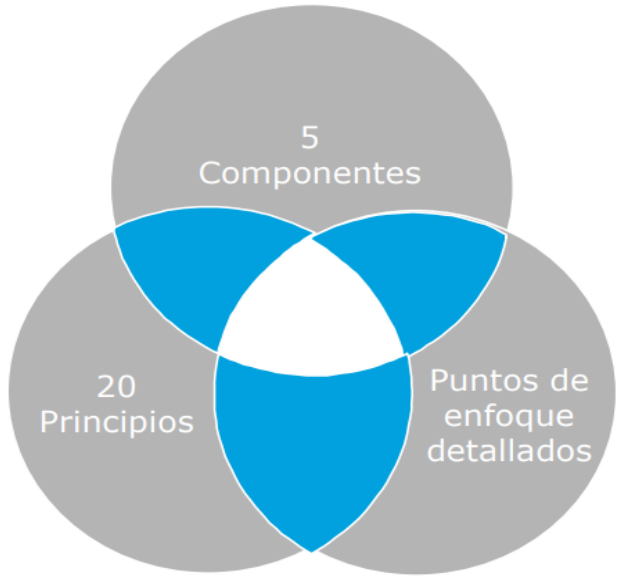
COSO 2017: GESTIÓN DE RIESGOS EMPRESARIALES – INTEGRADO CON ESTRATEGIA Y DESEMPEÑO

El marco actual vigente para el control interno de los riesgos es el llamado COSO ERM 2017, también conocido como COSO - Gestión de riesgos empresariales: integración con estrategia y rendimiento.

Esta actualización mantiene el enfoque financiero de sus predecesores, pero no obstante, su flexibilidad y estructura permite que sea utilizado indistintamente por cualquier tipo de actividad.

ESTANDAR COSO

COSO 2017: GESTIÓN DE RIESGOS EMPRESARIALES – INTEGRADO CON ESTRATEGIA Y DESEMPEÑO



- Mayor comprensión del valor de la gestión de riesgo para definir y ejecutar la estrategia.
- Alineación entre desempeño y gestión de riesgos.
- Acondiciona de mejor manera las expectativas de gobierno y supervisión.
- Reconoce la globalización de los mercados y las operaciones, así como el incremento de la volatilidad, complejidad y ambigüedad de los negocios.
- Presenta nuevos caminos para ver el riesgo, para alcanzar los objetivos en un contexto de negocios de alta complejidad.
- Mayor transparencia hacia los Stakeholders (Partes interesadas).
- Interpreta la evolución de la tecnología y la proliferación del análisis de datos que soporta la toma de decisiones.
- Establece definiciones claves, componentes y principios para todos los niveles de la gestión de riesgos.

COSO ERM 2017

ENTENDIMIENTO DE LA ESTRUCTURA DEL NUEVO COSO ERM 2017

GESTIÓN DE RIESGO EMPRESARIAL

Fuente: COSO - Enterprise Risk Management - Integrating with Strategy and Performance.

COMPONENTES COSO ERM 2017

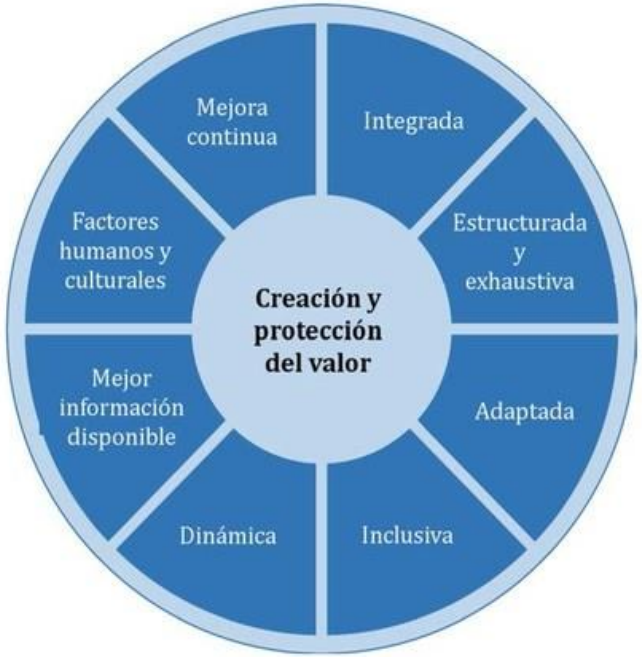
Gobierno y Cultura	El gobierno establece el tono de la organización, reforzando la importancia de, y estableciendo responsabilidades de supervisión, para la gestión de riesgos empresariales. La cultura se refiere a valores éticos, comportamientos deseados y comprensión del riesgo en la entidad.
Estrategia y objetivos	Gestión de riesgos empresariales, estrategia y objetivos trabajan juntos en el proceso de planeación estratégica. El apetito al riesgo es definido y alineado con la estrategia; los objetivos de negocio ponen la estrategia en practica mientras sirve para identificar, evaluar y responder a los riesgos.
Desempeño	Riesgos que pueden afectar el logro de la estrategia y los objetivos de negocio pueden ser identificados y evaluados. Riesgos son priorizados por severidad y en el contexto del apetito al riesgo. La organización selecciona las respuestas al riesgo y toma el riesgo que ha asumido.
Revisión	Para revisar el desempeño de la entidad, una organización puede considerar qué tan bien funcionan los componentes de gestión de riesgos empresariales a lo largo del tiempo a la luz de cambios sustanciales y qué revisiones se necesitan.
Información, comunicación y reporte	La gestión de riesgos empresariales requiere un proceso continuo para obtener y compartir información necesaria, de fuentes internas y externas, que fluya en todas las direcciones y a través de toda la organización.

PRINCIPIOS COSO ERM 2017

Gobierno y Cultura	Estrategia y objetivos	Desempeño	Revisión	Información, comunicación y reporte
1. La Junta Directiva ejerce supervisión sobre los riesgos 2. Establece estructuras operativas 3. Define la cultura deseada 4. Demuestra compromiso con los valores éticos 5. Atrae, desarrolla y retiene individuos competentes.	6. Analiza el contexto empresarial 7. Define el apetito al riesgo 8. Evalúa estrategias alternativas 9. Formula los objetivos empresariales	10. Identifica riesgos 11. Evalúa la severidad de los riesgos 12. Prioriza los riesgos 13. Implementas las respuestas al riesgo 14. Desarrollar un portafolio de riesgos	15. Evalúa los cambios sustanciales 16. Revisa los riesgos y el desempeño 17. Propone mejoras en la gestión de riesgos empresariales	18. Aprovecha la información y la tecnología 19. Comunica los riesgos de información 20. Informes sobre riesgos, cultura y desempeño

ISO 31000:2018

PRINCIPIOS



La gestión del riesgo es:

- Iterativa y asiste a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas.
- Parte de la gobernanza y el liderazgo y es fundamental en la manera en que se gestiona la organización en todos sus niveles. Esto contribuye a la mejora de los sistemas de gestión.
- Parte de todas las actividades asociadas con la organización e incluye la interacción con las partes interesadas.
- Considera los contextos externo e interno de la organización, incluido el comportamiento humano y los factores culturales.
- Está basada en los principios, el marco de referencia y el proceso descritos, conforme se ilustra en la Figura.

Estos componentes podrían existir previamente en toda o parte de la organización, sin embargo, podría ser necesario adaptarlos o mejorarlos

ISO 31000:2018

MARCO DE REFERENCIA

Liderazgo y compromiso

La alta dirección y los órganos de supervisión, cuando sea aplicable, deberían asegurar que la gestión del riesgo esté integrada en todas las actividades de la organización.

Integración

La integración de la gestión del riesgo depende de la comprensión de las estructuras y el contexto de la organización. El riesgo se gestiona en cada parte de la estructura de la entidad. Todos los miembros de una organización tienen la responsabilidad de gestionar el riesgo.

Diseño

Comprensión de la organización y de su contexto. Articulación del compromiso con la gestión del riesgo. Asignación de roles, autoridades, responsabilidades y obligación de rendir cuentas en la entidad. Asignación de recursos y Establecimiento de la comunicación y la consulta

Implementación

Valoración

Mejora

Adaptación y Mejora Continua.

ANÁLISIS DEL CONTEXTO

Definición de los parámetros internos y externos que se han de tomar en consideración para la administración de riesgo NTC ISO 31000, Numeral 2,9).

Se debe establecer el contexto tanto interno como externo de la entidad, además del contexto del proceso y sus activos de seguridad.

LÍNEA ESTRATÉGICA

Alta dirección y Comité Institucional de Coordinación de Control Interno, a quienes corresponde:

- Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la entidad.
- Establecer la Política de Administración del Riesgo.
- Asumir la responsabilidad primaria del SCI y de la identificación y evaluación de los cambios que podrían tener un impacto significativo en el mismo.
- Específicamente el Comité Institucional de Coordinación de Control Interno, evaluar y dar línea sobre la administración de los riesgos en la entidad.
- Realimentar a la alta dirección sobre el monitoreo y efectividad de la gestión del riesgo y de los controles. Así mismo, hacer seguimiento a su gestión, gestionar los riesgos y aplicar los controles.

1ª. LÍNEA DE DEFENSA

- Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales.
- A partir de la política de administración del riesgo, establecer sistemas de gestión de riesgos y las responsabilidades para controlar riesgos específicos bajo la supervisión de la alta dirección. Con base en esto, establecen los mapas de riesgos.
- Identificar y controlar los riesgos relacionados con posibles actos de corrupción en el ejercicio de sus funciones y el cumplimiento de sus objetivos, así como en la prestación del servicio y/o relacionados con el logro de los objetivos.
- Implementan procesos para identificar, disuadir y detectar fraudes; y revisan la exposición de la entidad al fraude con el auditor interno de la entidad.

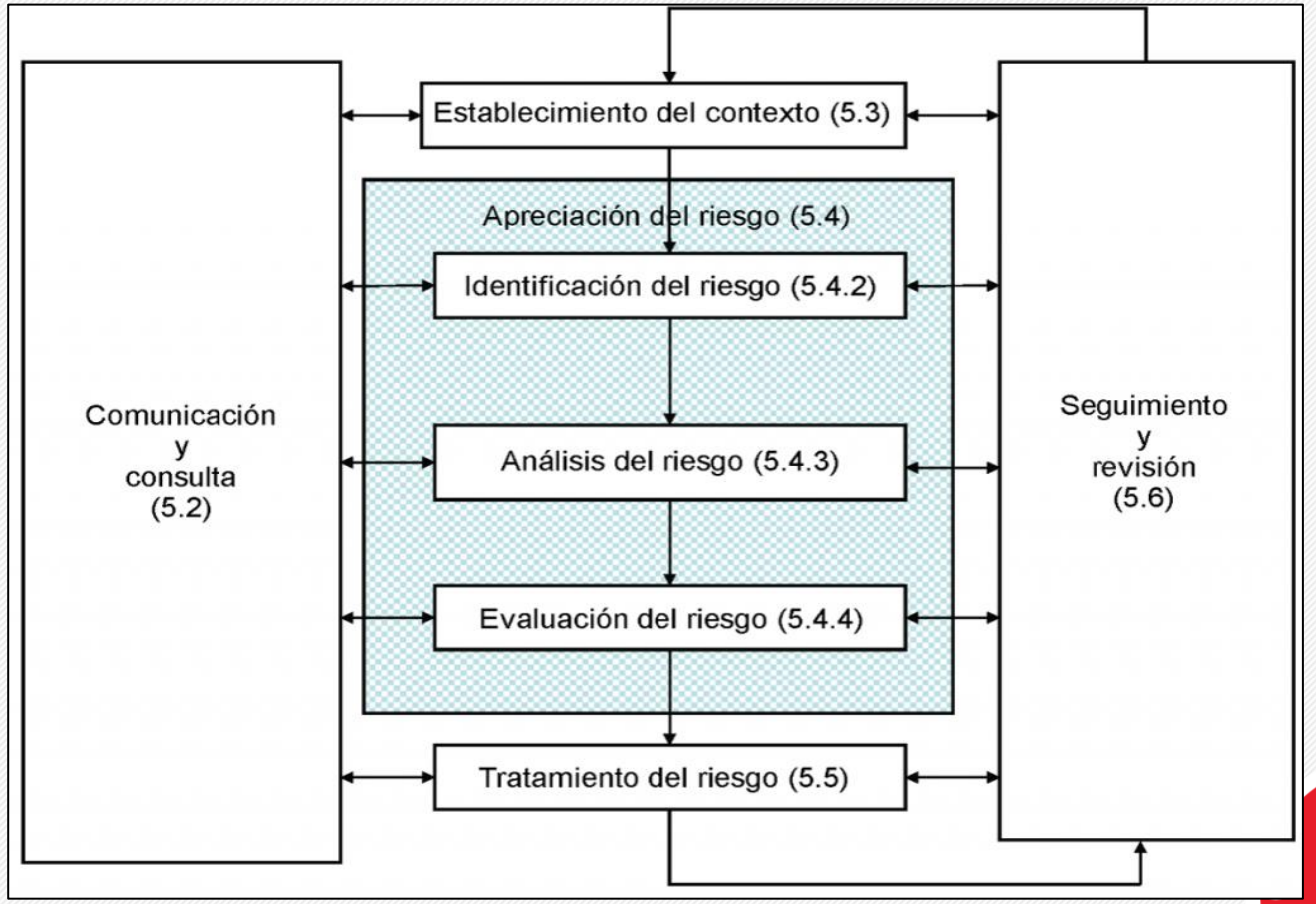
2ª. LÍNEA DE DEFENSA

- Definir un área o líder de la gestión de riesgos para coordinar las actividades en esta materia.
- Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada.
- Asegurar que las evaluaciones de riesgo y control incluyan riesgos de fraude.
- Monitorear cambios en el riesgo legal, regulatorio y de cumplimiento.
- Consolidar los seguimientos a los mapas de riesgo.
- Seguir los resultados de las acciones emprendidas para mitigar los riesgos, cuando haya lugar.
- Los supervisores e interventores de contratos deben realizar seguimiento a los riesgos de estos e informar las alertas respectivas.
- Elaborar informes consolidados para las diversas partes interesadas.

3ª. LÍNEA DE DEFENSA

- Identificar y evaluar cambios que podrían tener un impacto significativo en el SCI, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna.
- Comunicar al Comité Institucional de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías.
- Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad.
- Establecer el plan anual de auditoría basado en riesgos, priorizando aquellos procesos de mayor exposición.
- Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.

PROCESO – ISO 31000



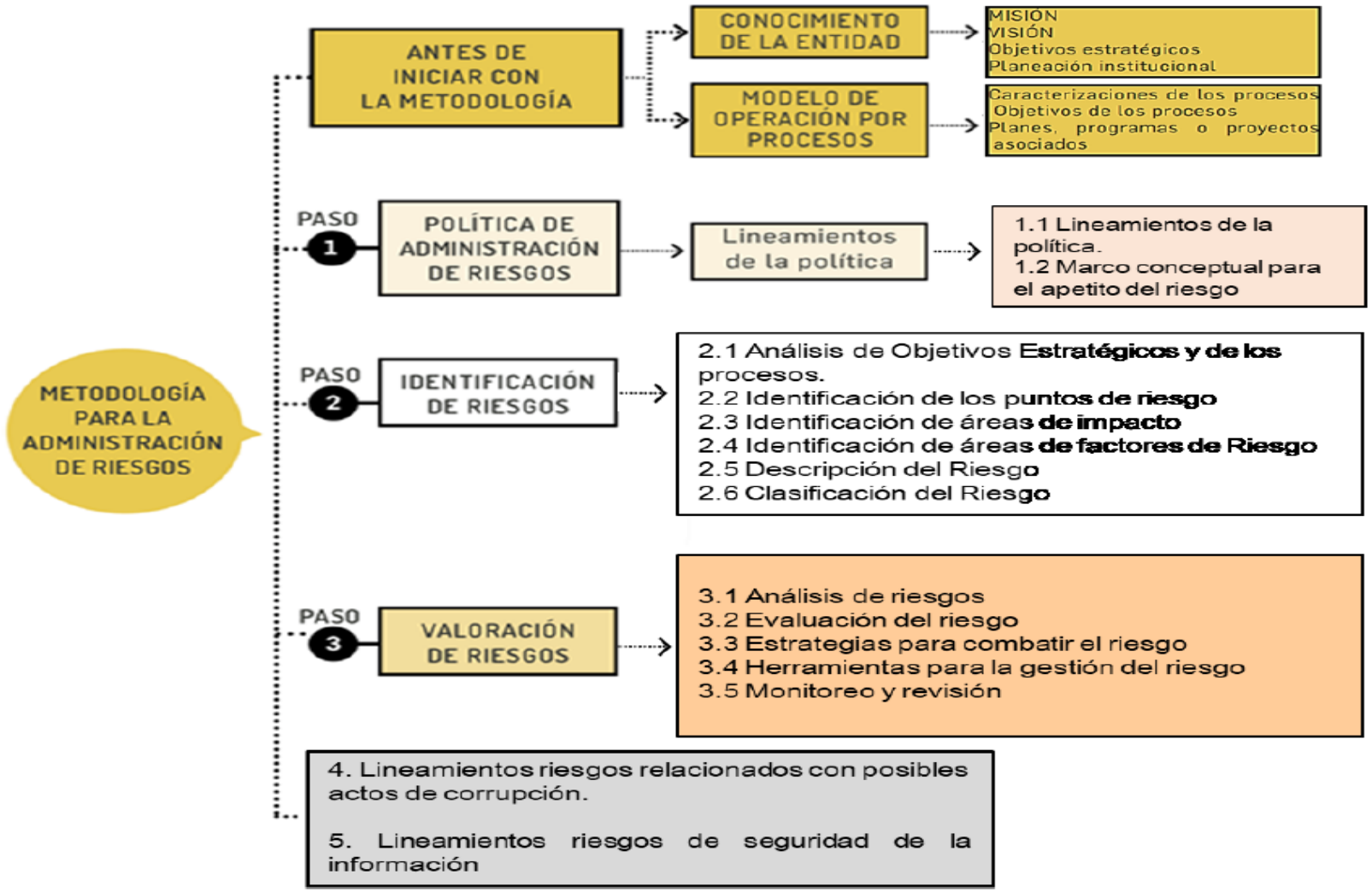
ANALISIS DEL CONTEXTO

CONTEXTO EXTERNO	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).
CONTEXTO INTERNO	FINANCIEROS: presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	PERSONAL: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	PROCESOS: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
	TECNOLOGÍA: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
	ESTRATÉGICOS: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

ANALISIS DEL CONTEXTO

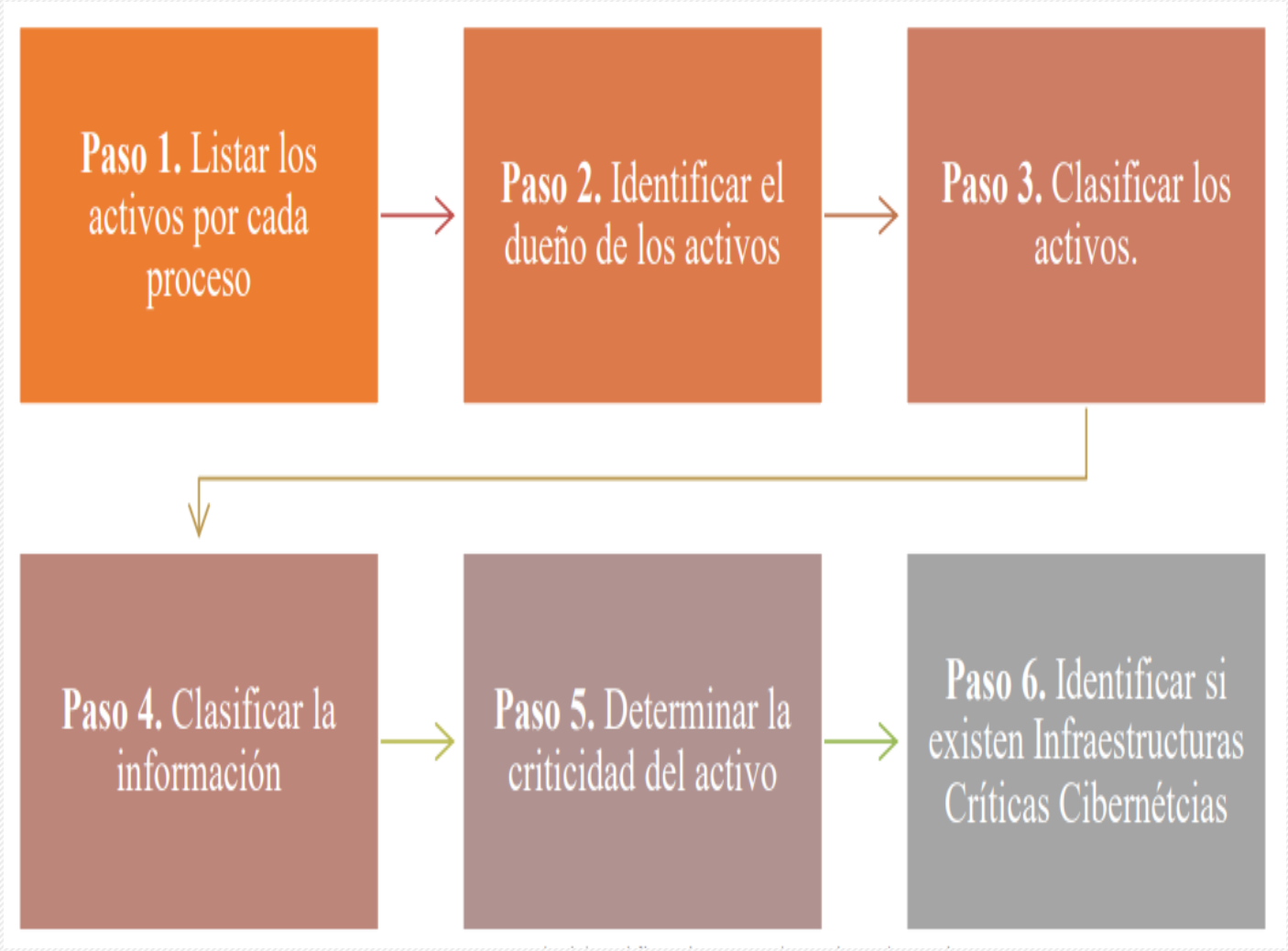
CONTEXTO DEL PROCESO	DISEÑO DEL PROCESO: claridad en la descripción del alcance y objetivo del proceso.
	INTERACCIONES CON OTROS PROCESOS: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	TRANSVERSALIDAD: procesos que determinan lineamientos necesarios 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. Ver conceptos básicos relacionados con el riesgo

METODOLOGÍA PARA ADMINISTRACIÓN DE RIESGOS



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

IDENTIFICACIÓN ACTIVOS DE INFORMACIÓN



IDENTIFICACIÓN ACTIVOS DE INFORMACIÓN

En el modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- 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.

CLASIFICACIÓN DE RIESGOS

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.

ANÁLISIS RIESGOS - PROBABILIDAD

FRECUENCIA ACTIVIDADES DE GESTÓN

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería ***Nota:** En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

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

ANÁLISIS RIESGOS - PROBABILIDAD

FRECUENCIA ACTIVIDADES DE GESTÓN

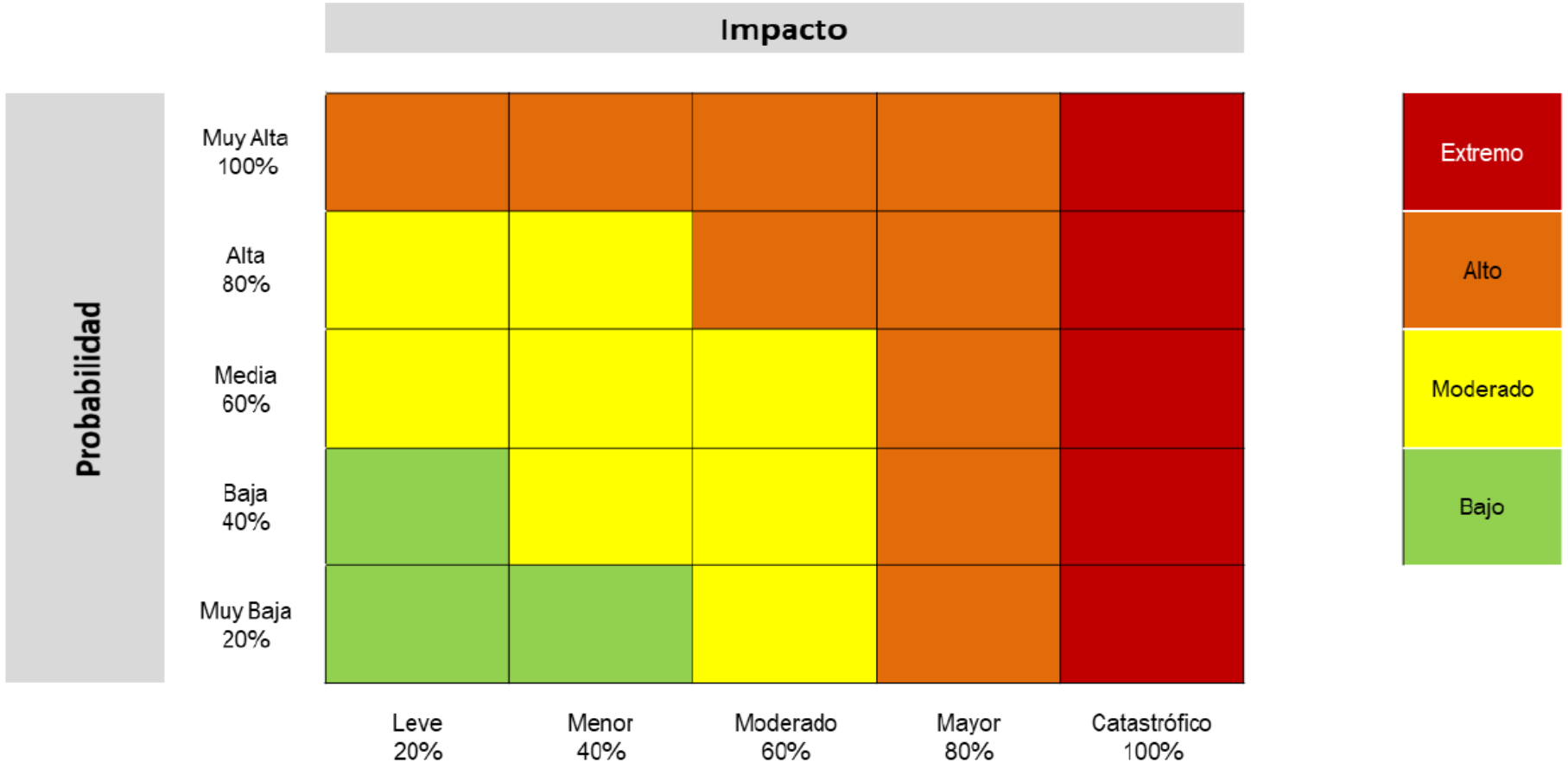
	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad 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%

ANÁLISIS RIESGOS - IMPACTO

FRECUENCIA ACTIVIDADES DE GESTIÓN

	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

MAPA DE CALOR



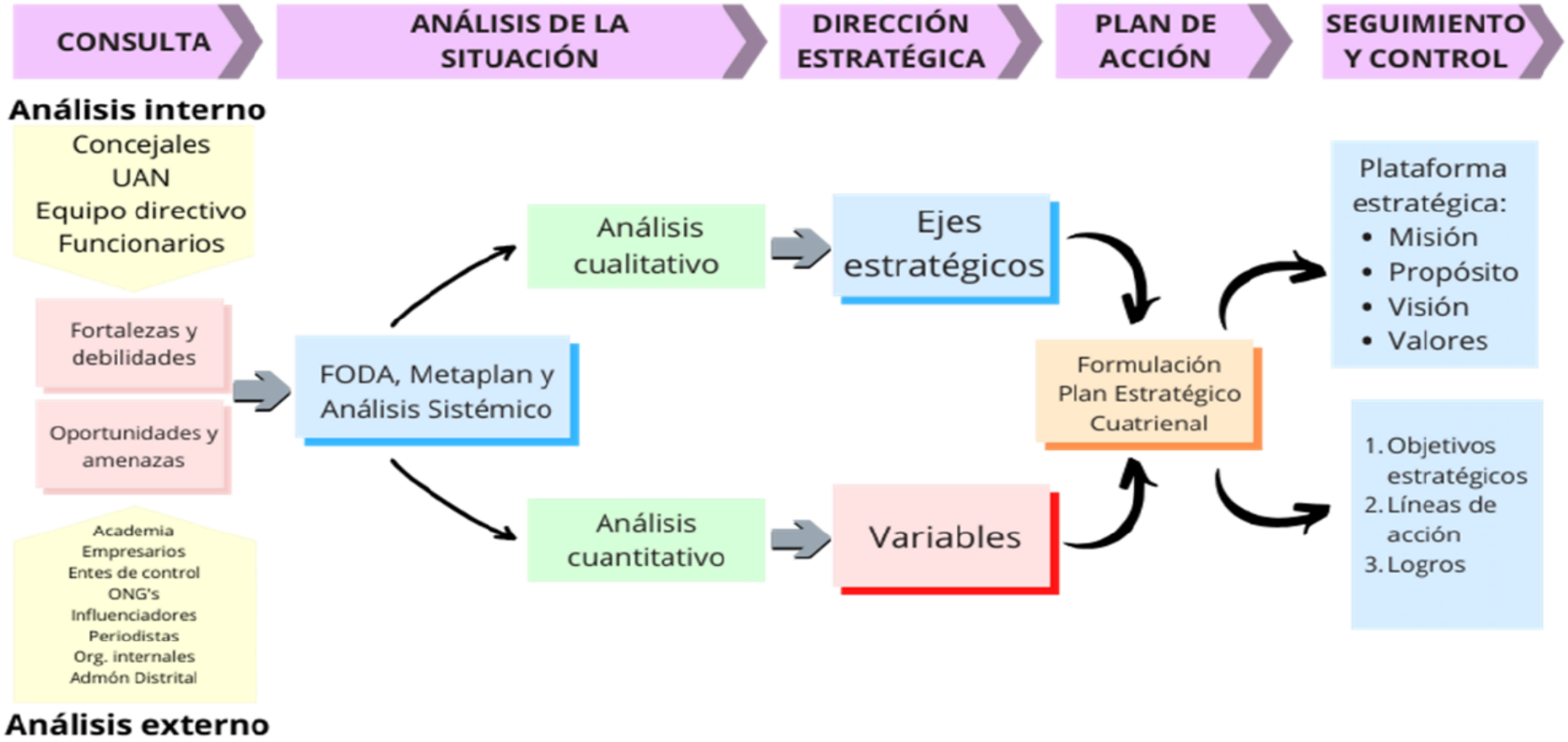
Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

ANÁLISIS CONTEXTO - FODA

	Oportunidades	Amenazas
Fortalezas	Retos ofensivos (FO)	Retos reactivos (FA)
Debilidades	Retos adaptativos (DO)	Retos defensivos (DA)

Fuente: OAP

CONSTRUCCIÓN PLAN ESTRATÉGICO 2020-2023



Fuente: OAP

ESQUEMA PLAN ESTRATÉGICO 2020-2023

Fuente: OAP

PLATAFORMA ESTRATÉGICA

Propósito fundamental	Concejo generador de valor público, transformador de realidades y vidas
Misión	Como máxima autoridad del Distrito Capital, somos el vocero de los intereses plurales de la ciudadanía, y en su nombre realizamos gestión normativa y ejercemos el control político sobre las autoridades distritales, mediante el debate de los asuntos de interés general para promover el desarrollo integral y armónico del territorio y de sus habitantes.
Visión	En el 2023 seremos reconocidos como una corporación plural, incluyente, participativa, innovadora, proba y transparente, generadora de valor público en su ejercicio de control político y gestión normativa, para la transformación de realidades de la ciudad en armonía con la región, y la mejora de la calidad de vida de la gente.
Valores estratégicos	Correspondientes a los valores establecidos en el Código de integridad del Servicio Público para el Concejo de Bogotá, D.C.

APUESTAS ESTRATÉGICAS

1. Concejo **confiable y con credibilidad**, que genere valor público y transforme realidades

2. Concejo **visible, transparente**, abierto, cercano y sintonizado con la ciudadanía

3. Concejo **moderno y eficaz**, con capacidades de gestión fortalecidas y generadora de resultados

OBJETIVOS ESTRATÉGICOS

ATRIBUTOS PARA DISEÑO DEL CONTROL

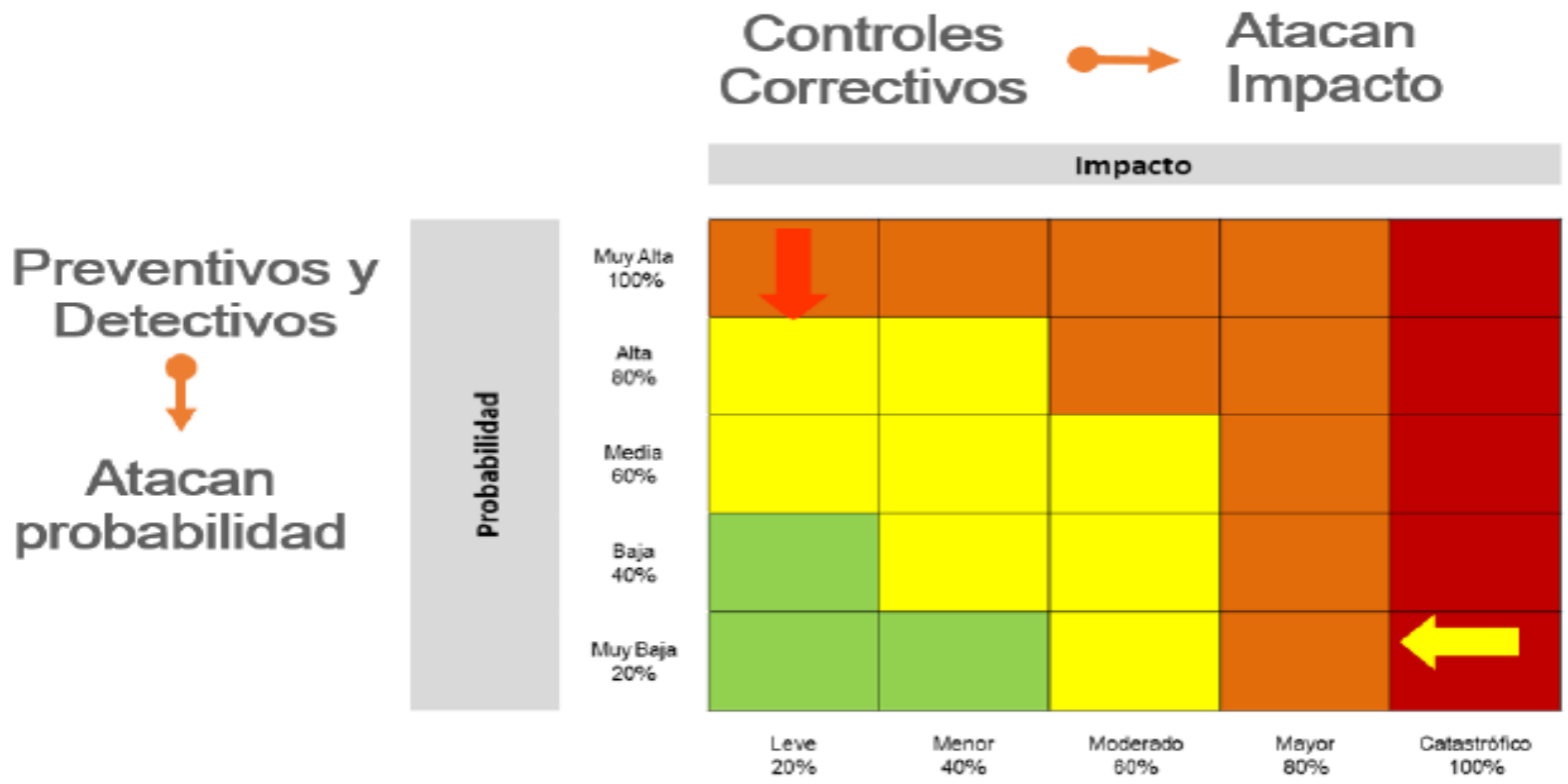
Caracteristicas			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten 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 PARA DISEÑO DEL CONTROL

Características			Descripción	Peso
*Atributos informativos	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	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

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

MOVIMIENTO DEL RIESGO POR CONTROLES



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

VALORACIÓN RIESGO RESIDUAL

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	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

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

ADMINISTRACIÓN DEL RIESGO

Concejo de Bogotá

Gracias