Administración del riesgo y Auditoría basada en riesgos

Bello, Julio 13 de 2017

Elaborado por:
Federico Alonso Atehortúa Hurtado, M. Sc.
Especialista en alta gerencia con énfasis en calidad
Coordinador de Formación e Investigación
Gestión y Conocimiento®

Objetivo General

Presentar los fundamentos de la gestión de riesgos y de la metodología de auditoría basada en riesgos.

RIESGO

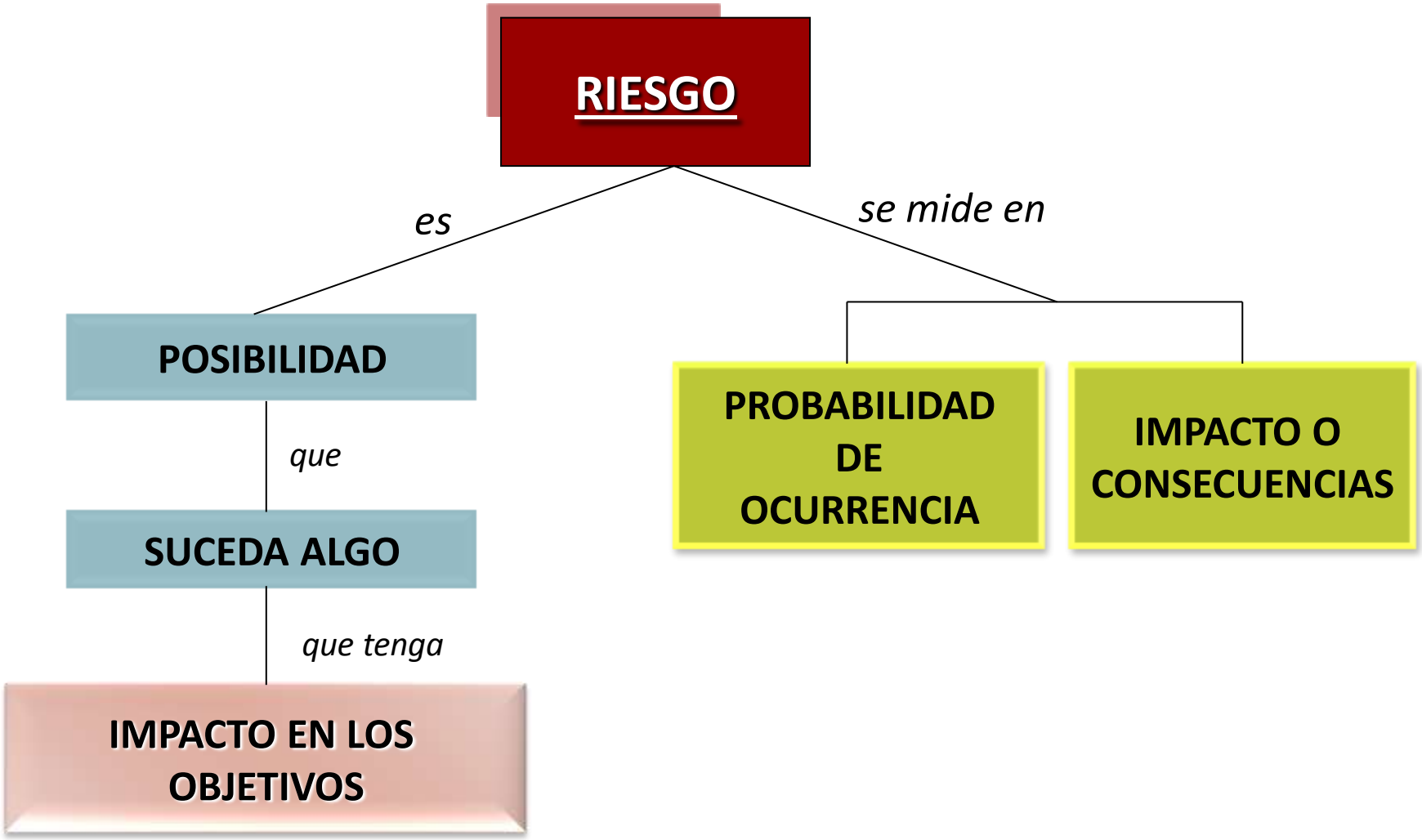
- Efecto de la incertidumbre sobre los objetivos.

(Norma NTC –ISO31000:2011)

Efecto de la incertidumbre.

(NTC-ISO9000:2015 – Numeral 3.7.9)

RIESGO



ACTITUD HACIA EL RIESGO

- "**Actitud hacia el riesgo.** Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del **riesgo**."

(NTC ISO31000:2011)

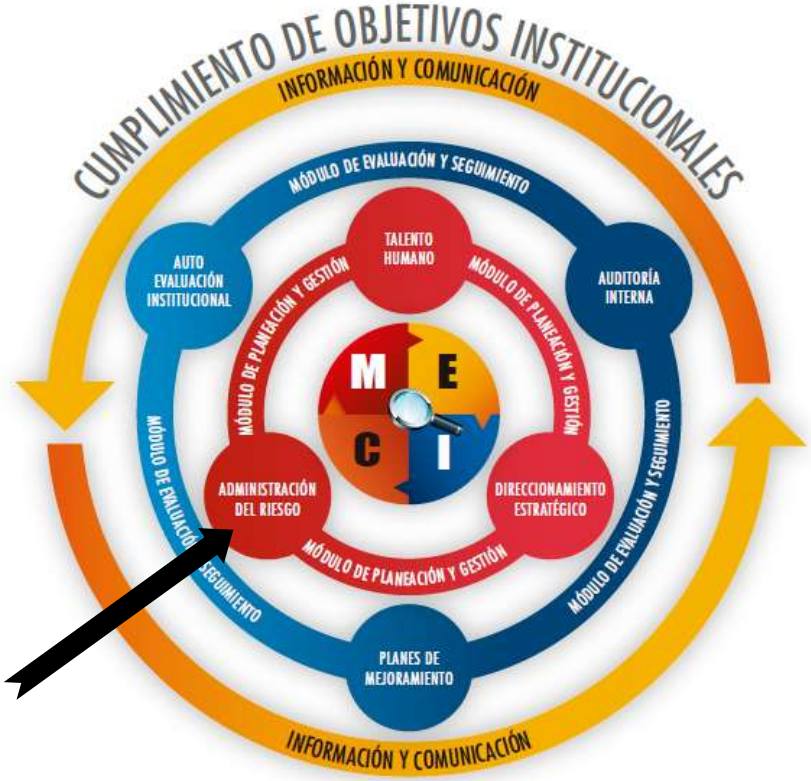
TIPOS DE RIESGOS

TIPOS DE RIESGOS POR ÁREAS DE IMPACTO

- Riesgos estratégicos
- Riesgos de seguridad y salud en el trabajo
- Riesgos operativos
- Riesgos ambientales
- Riesgos de corrupción
- Riesgos financieros
- Riesgos de reputación
- Riesgos de seguridad de la información
- Riesgos de continuidad

Gestión del Riesgo en las entidades públicas en Colombia

MECI 2014



Elaboración: Equipo DAFP

NTCGP 1000:2009

"4.1 g) La entidad debe establecer controles sobre los riesgos identificados y valorados que puedan afectar la satisfacción del cliente y el logro de los objetivos de la entidad."

ISO9001:2015

www.gestionyconocimiento.com

Gestión y Conocimiento Consultoría Organizacional

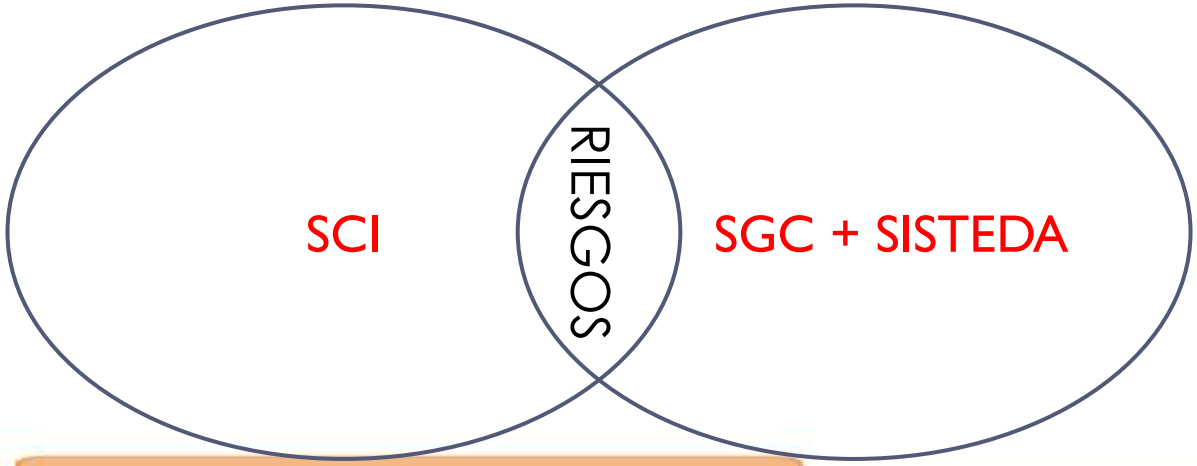
Componentes del Plan Anticorrupción y de Atención al Ciudadano

Fuente: Estrategias para la construcción del plan anticorrupción y de atención al ciudadano. Versión 2. 2015 Página 11

Nuevo Modelo Integrado de Planeación y Gestión MIPYG

"Incorporar la gestión del riesgo como elemento de articulación del sistema resultado de la integración, de los sistemas de gestión de calidad y de desarrollo administrativo, con el sistema de control interno.".

Fuente: DAFP. Modelo Integrado de Planeación y Gestión Versión 2 Documento Conceptual y Orientaciones Generales



Nuevo Modelo Integrado de Planeación y Gestión MIPYG

"el modelo de la Tres Líneas de Defensa específicamente en la primera línea (nivel estratégico y operacional) y la segunda línea (la administración de riesgos y funciones de cumplimiento)".

Fuente: DAFP. Modelo Integrado de Planeación y Gestión Versión 2 Documento Conceptual y Orientaciones Generales

METODOLOGÍA DE GESTIÓN DEL RIESGO

GESTIÓN DEL RIESGO

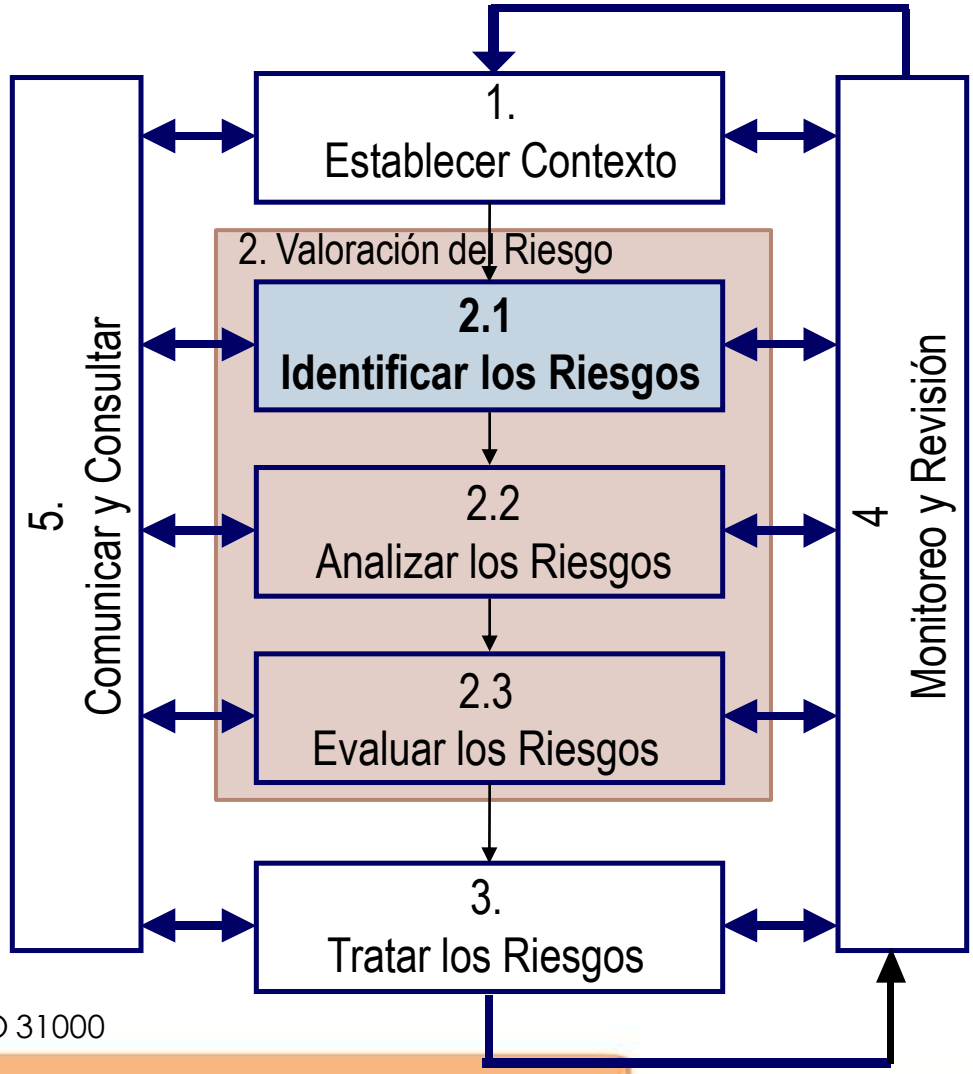
Un proceso para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto al alcance de los objetivos de la organización.

(MECI1000:2014)

ELEMENTOS CLAVES DE LA GESTIÓN DEL RIESGO

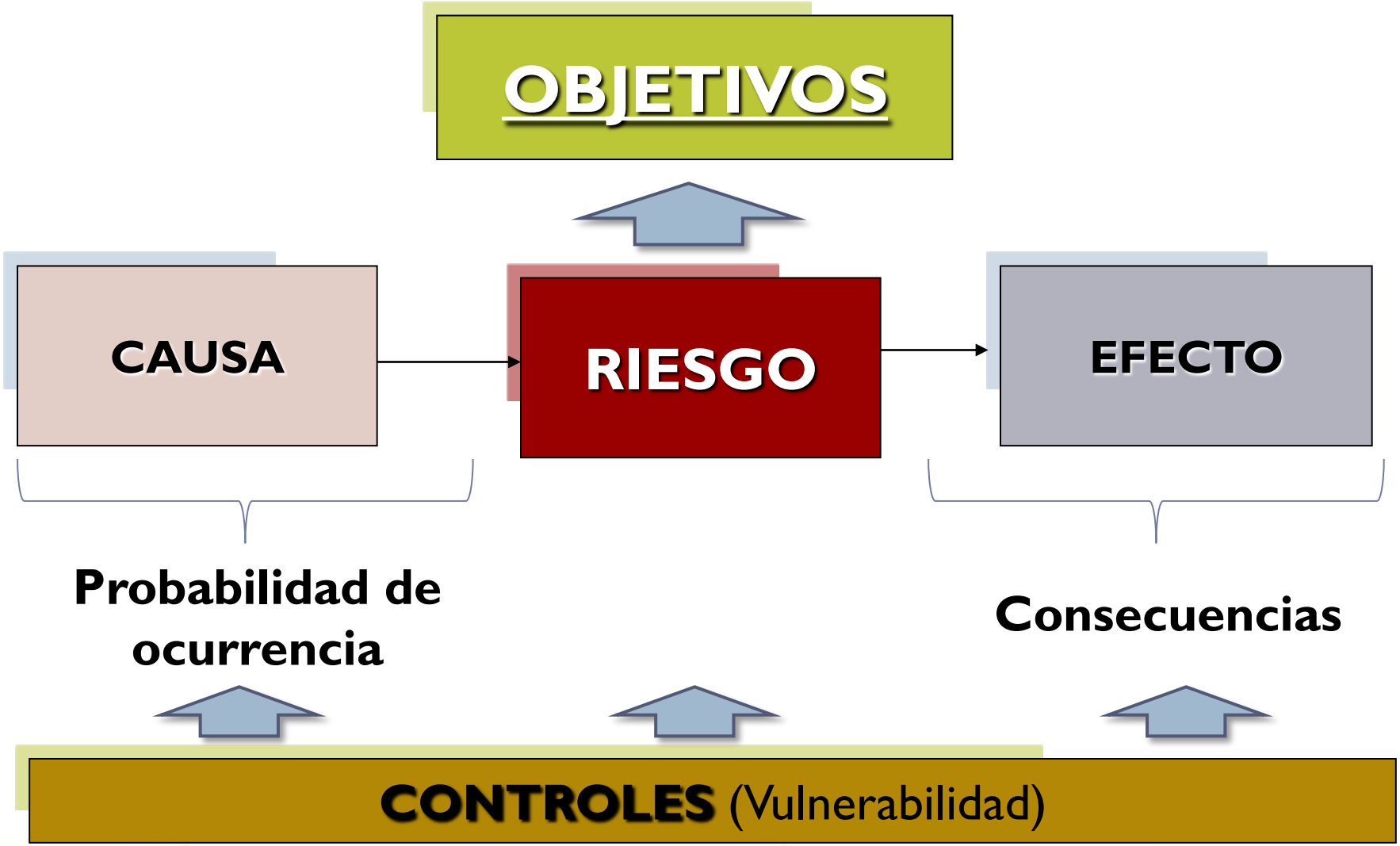
1. Cubrir los riesgos de manera integral
2. Focalizarse en los riesgos relevantes
3. Sirve para validar los controles
4. Se deben fundamentar en una política
5. Requieren seguimiento y revisión periódica
7. Responsabilidades y autoridades definidas
8. Gestionar a nivel de procesos
9. Objeto de auditoría

Metodología de Gestión del Riesgo



NTC-ISO 31000

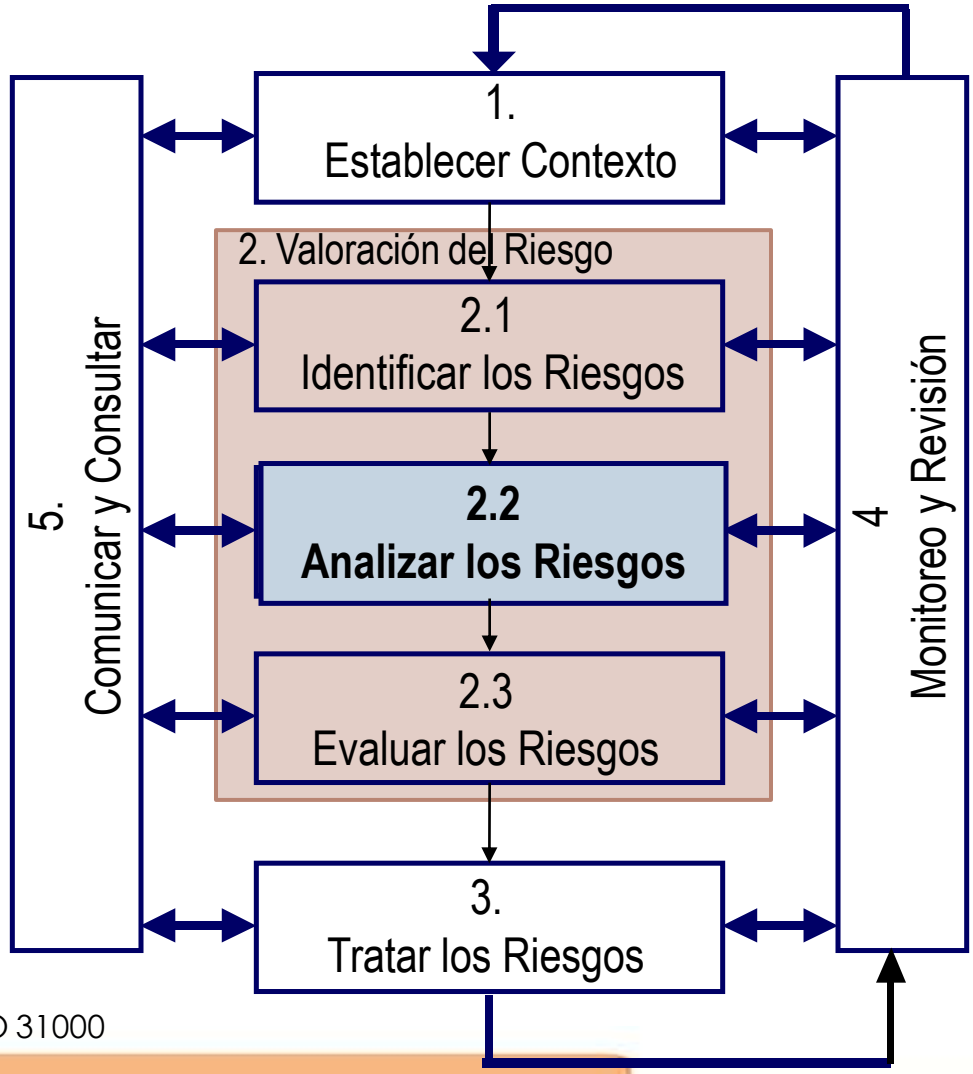
IDENTIFICACIÓN DEL RIESGO



EJEMPLO DE IDENTIFICACIÓN DEL RIESGO

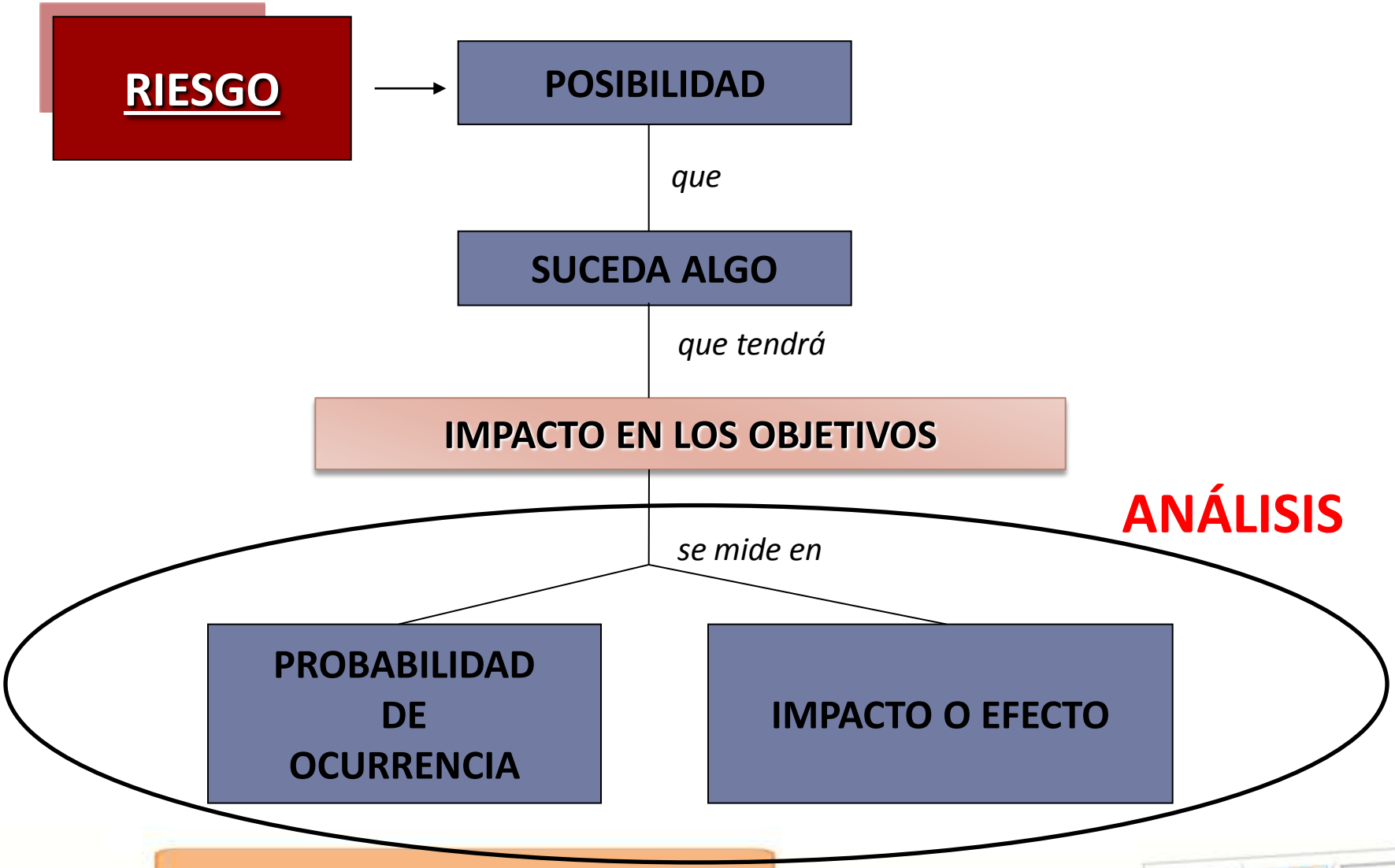
PROCESO	RIESGO	CAUSAS	CONSECUENCIAS
Gestión del talento humano	Selección de personal que no cumple las competencias necesarias para los procesos.	• Competencias de los cargos obsoletas o no definidas. • Insuficiente evaluación del personal que se contrata. • Adulteración o falsificación de documentos por parte de los candidatos a un empleo.	• Sanciones administrativas • Deterioro de la imagen pública de la entidad • Retrasos en la prestación de los servicios. • Facilitación de la comisión de actos de corrupción.

Metodología de Gestión del Riesgo

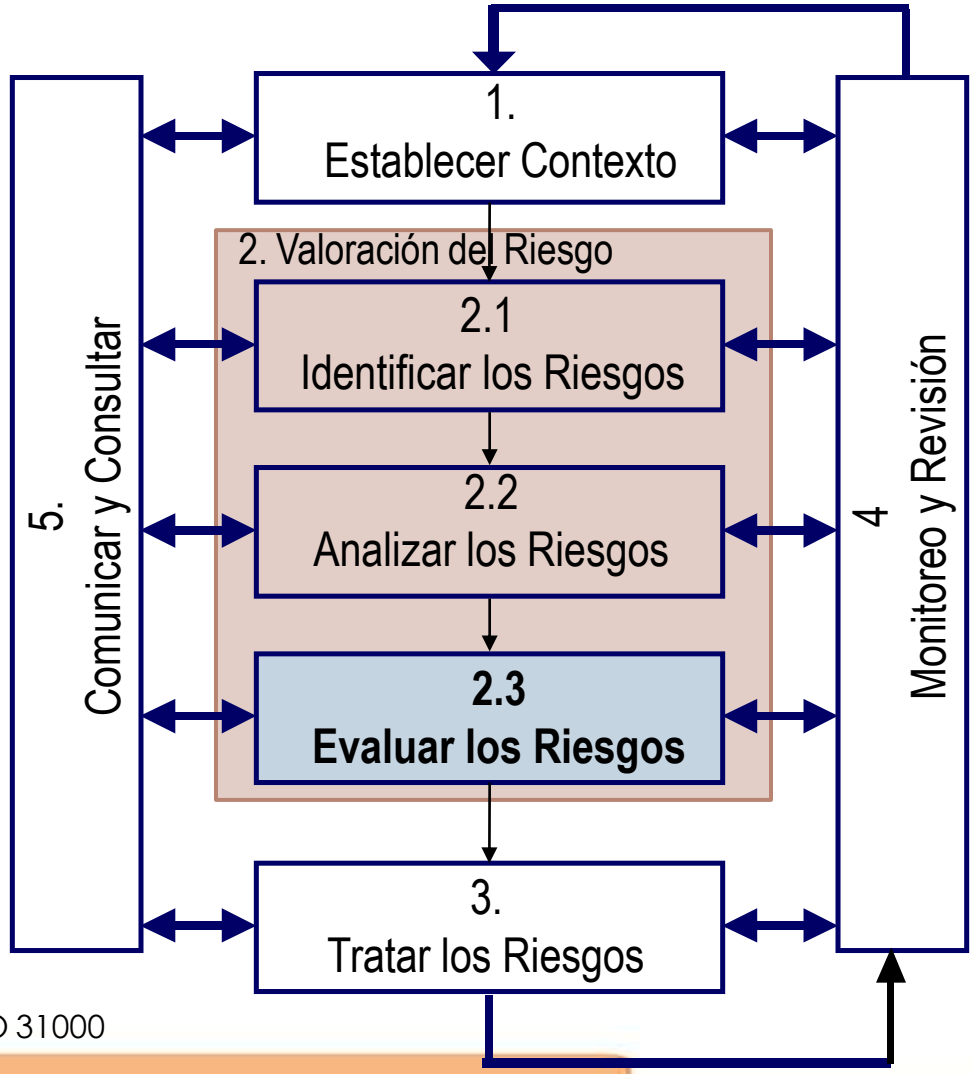


NTC-ISO 31000

ANÁLISIS DEL RIESGO

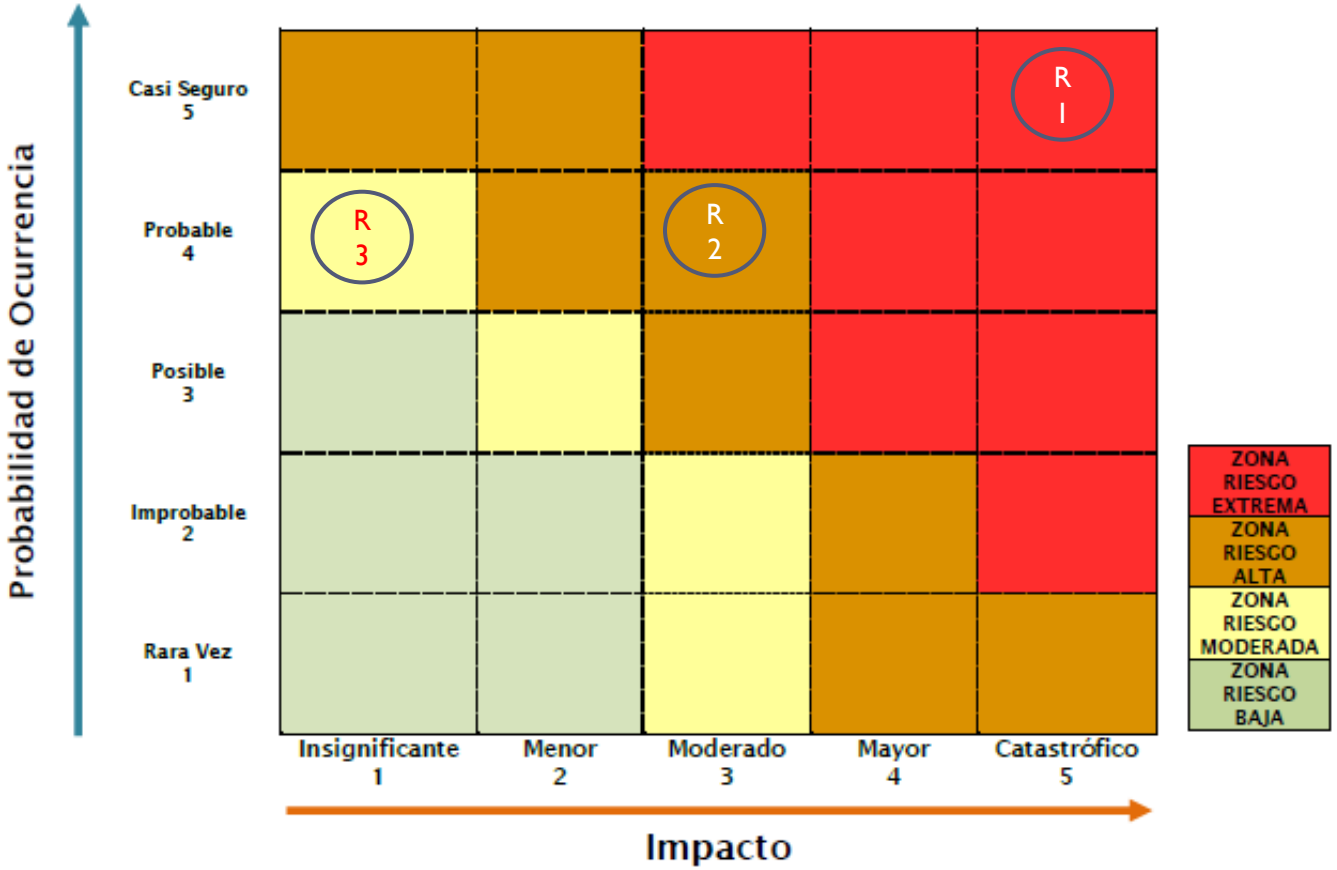


Metodología de Gestión del Riesgo



NTC-ISO 31000

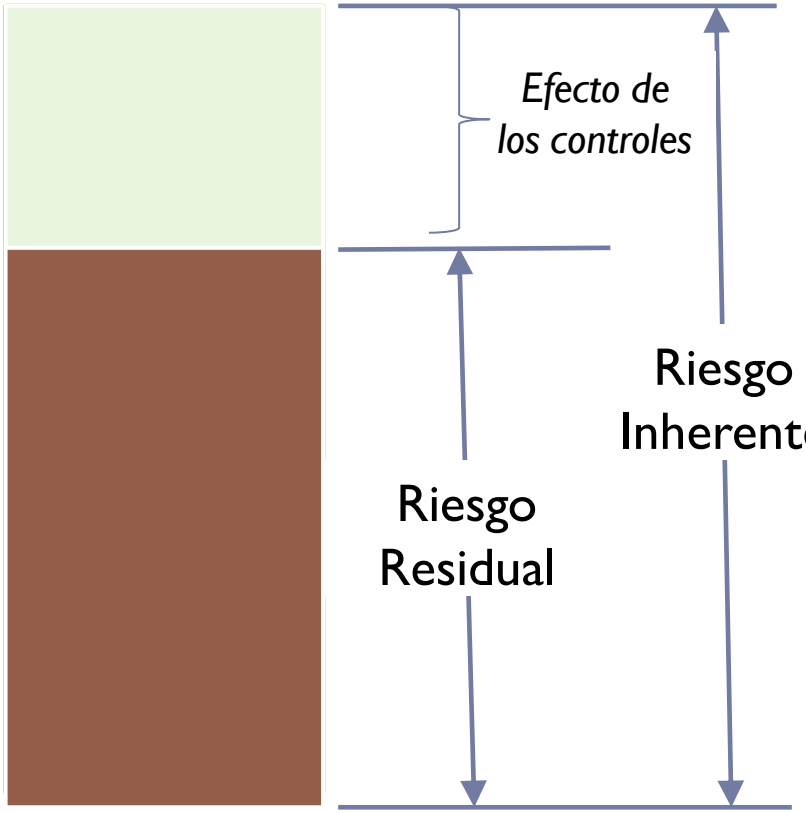
EVALUACIÓN DEL RIESGO

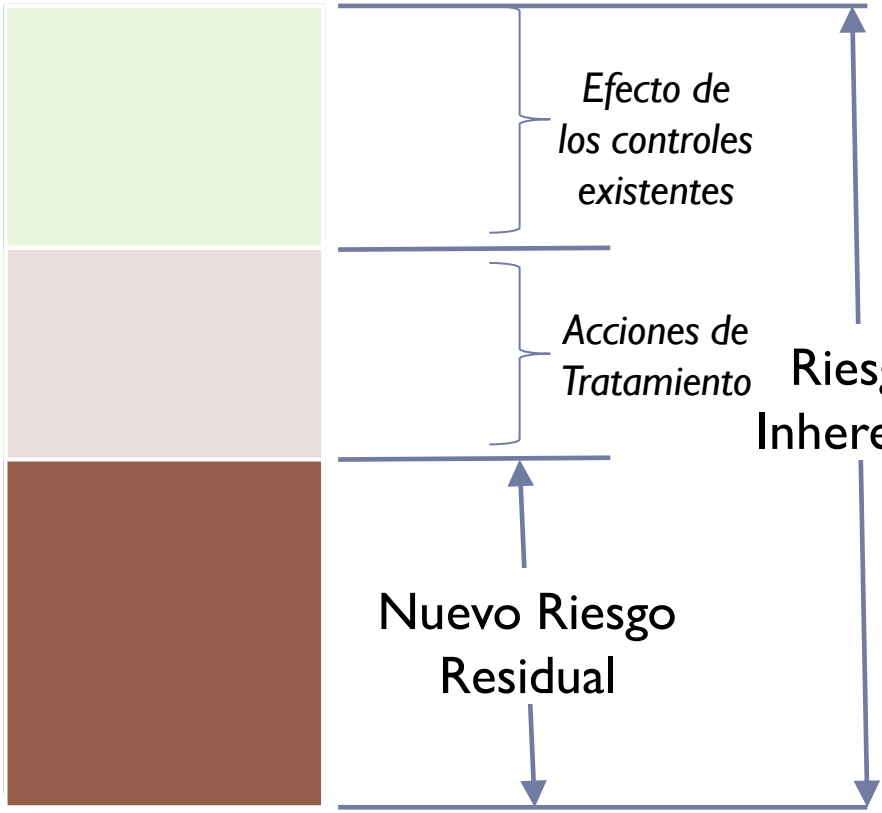


(DAFP. Guía de administración del riesgo. Versión 3. Octubre 2014)

21

RIESGOS VS CONTROLES





Riesgo **Inherente**: Riesgo **sin** Control
Riesgo **Residual**: Riesgo **con** Control

EVALUACIÓN DEL RIESGO

Riesgo Inherente

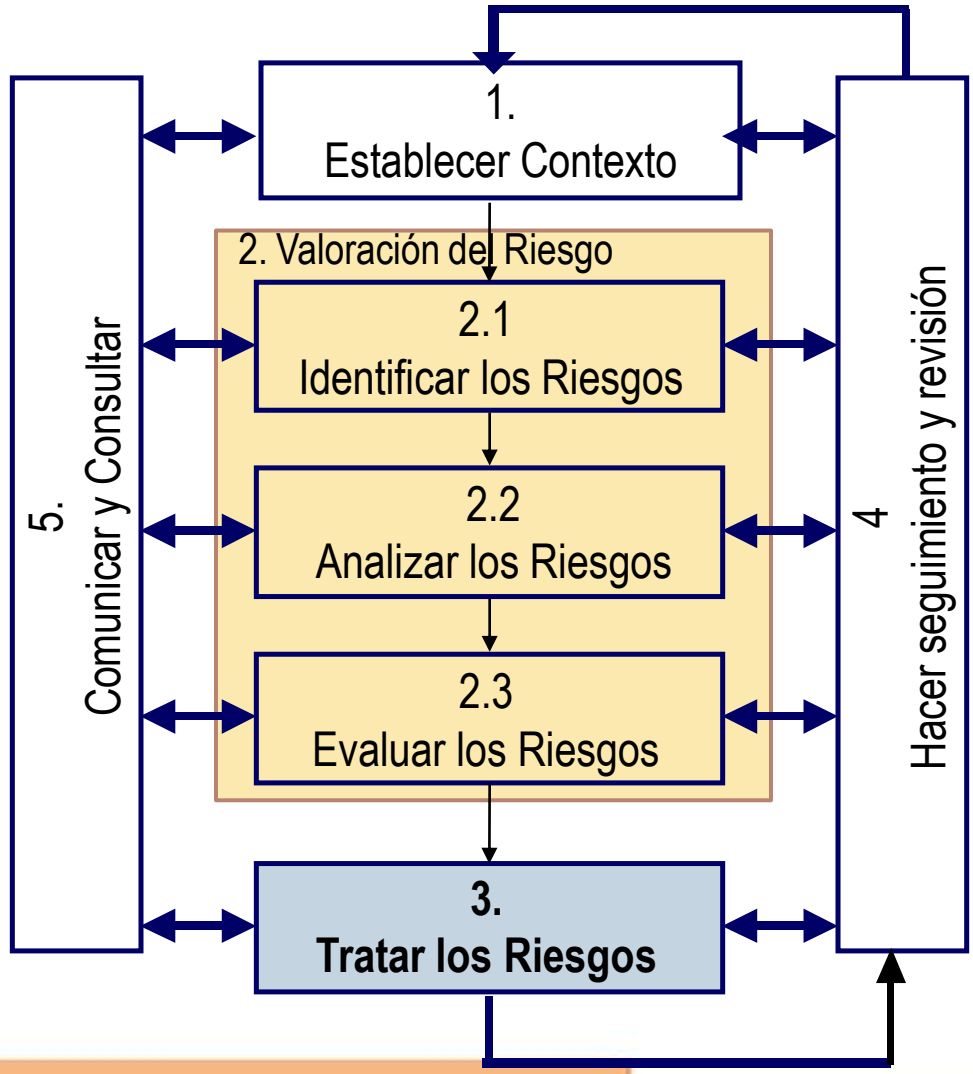
Riesgo Residual

CALIFICACIÓN Y EVALUACIÓN DE RIESGOS

PI-PR-02-FR-01

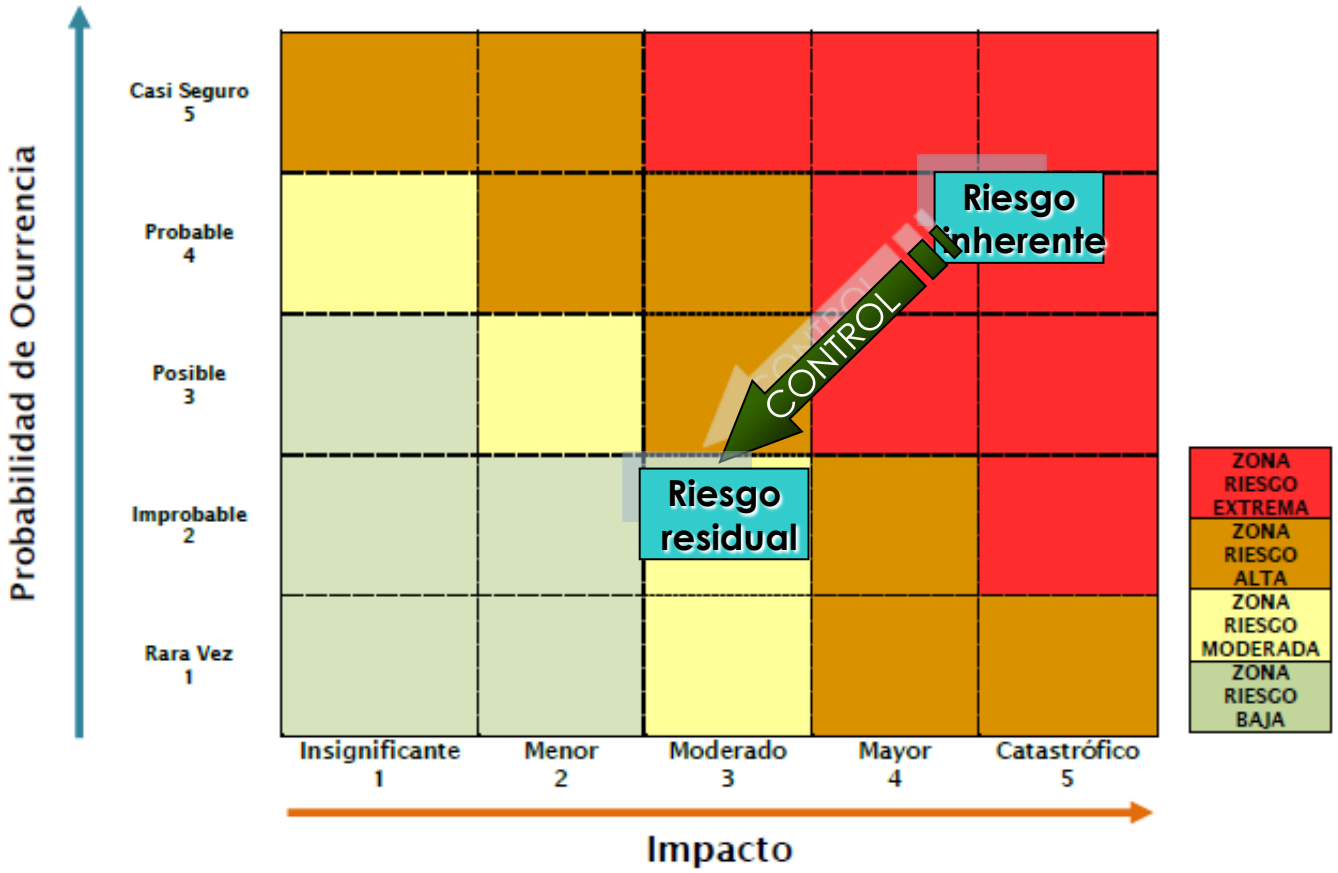
No.	RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO								NIVEL DEL RIESGO	NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO								NIVEL DEL RIESGO
			P	B	F	Im	A	If	C	L			P	B	F	Im	A	If	C	L	
		SIN CONTROL										CON CONTROL									
00	#¡REF!										0										0
00	#¡REF!										0										0
00	#¡REF!										0										0
00	#¡REF!										0										0
00	#¡REF!										0										0
00	#¡REF!										0										0

Metodología de Gestión del Riesgo



TRATAR EL RIESGO

Efecto deseable de los tratamientos



TRATAMIENTO DEL RIESGO

(GTC ISO9002:2017)

Las opciones para tratar los riesgos son:

- Evitar el riesgo
- Eliminar la fuente del riesgo
- Reducir el riesgo.
- Compartir o Transferir el riesgo.
- Asumir un riesgo.
- Tomar el riesgo para aprovechar una oportunidad.

EVITAR EL RIESGO (GTC ISO9002:2017)

"Dejar de desempeñar el proceso en el que puede encontrarse el riesgo."

EVITAR EL RIESGO (NTC ISO31000: 2011)

"decidiendo no iniciar o continuar la actividad que lo originó."

ELIMINAR LA FUENTE DEL RIESGO

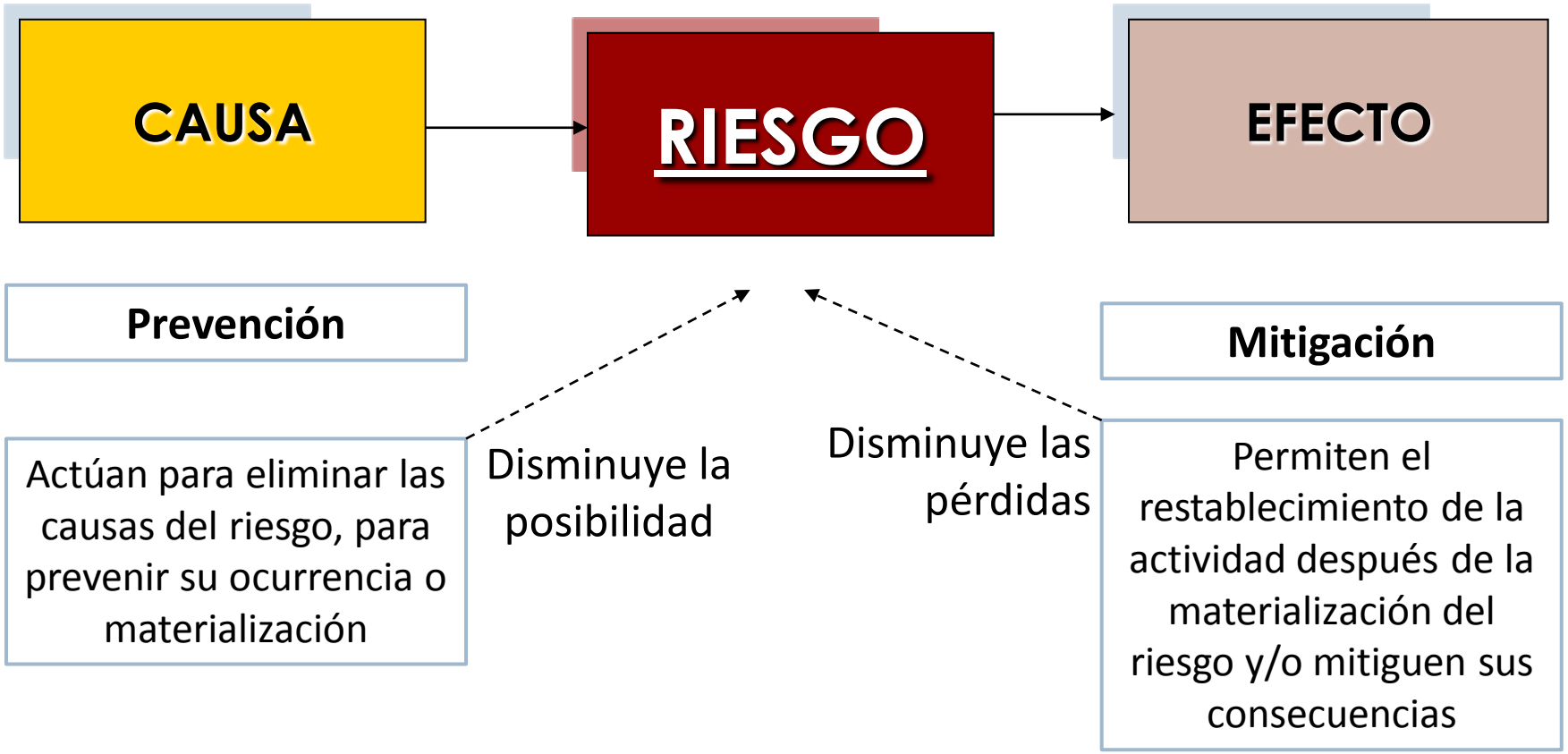
"**Fuente de riesgo.** Elemento que solo o en combinación tiene el potencial intrínseco de originar un **riesgo .**" **(NTC ISO 31000:2011)**

REDUCIR EL RIESGO (NTC ISO31000: 2011)

Cambiar la **probabilidad**

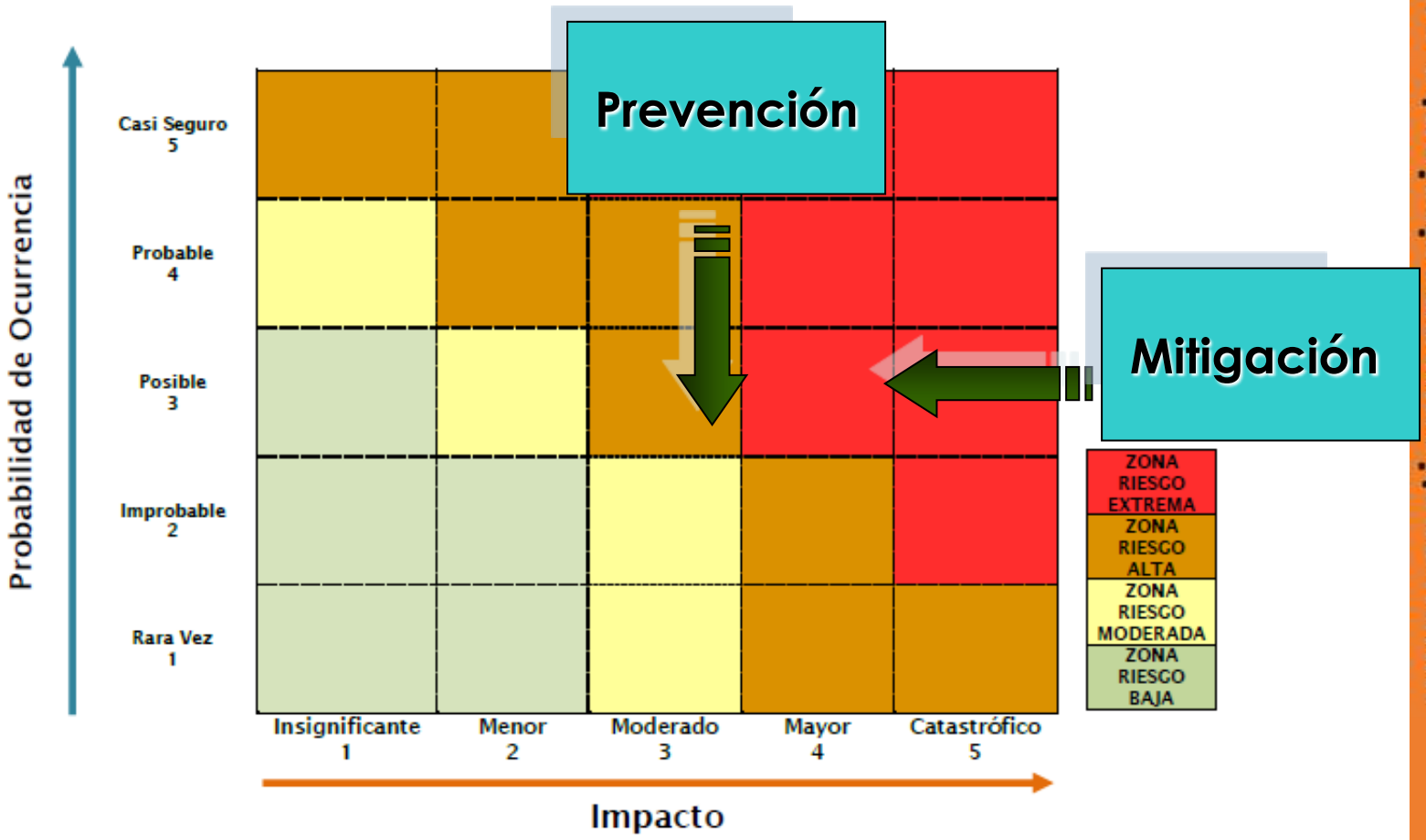
Cambiar las **consecuencias**

REDUCIR EL RIESGO



TRATAMIENTO DEL RIESGO

Reducción del Riesgo



REDUCIR EL RIESGO (NTC ISO31000: 2011)

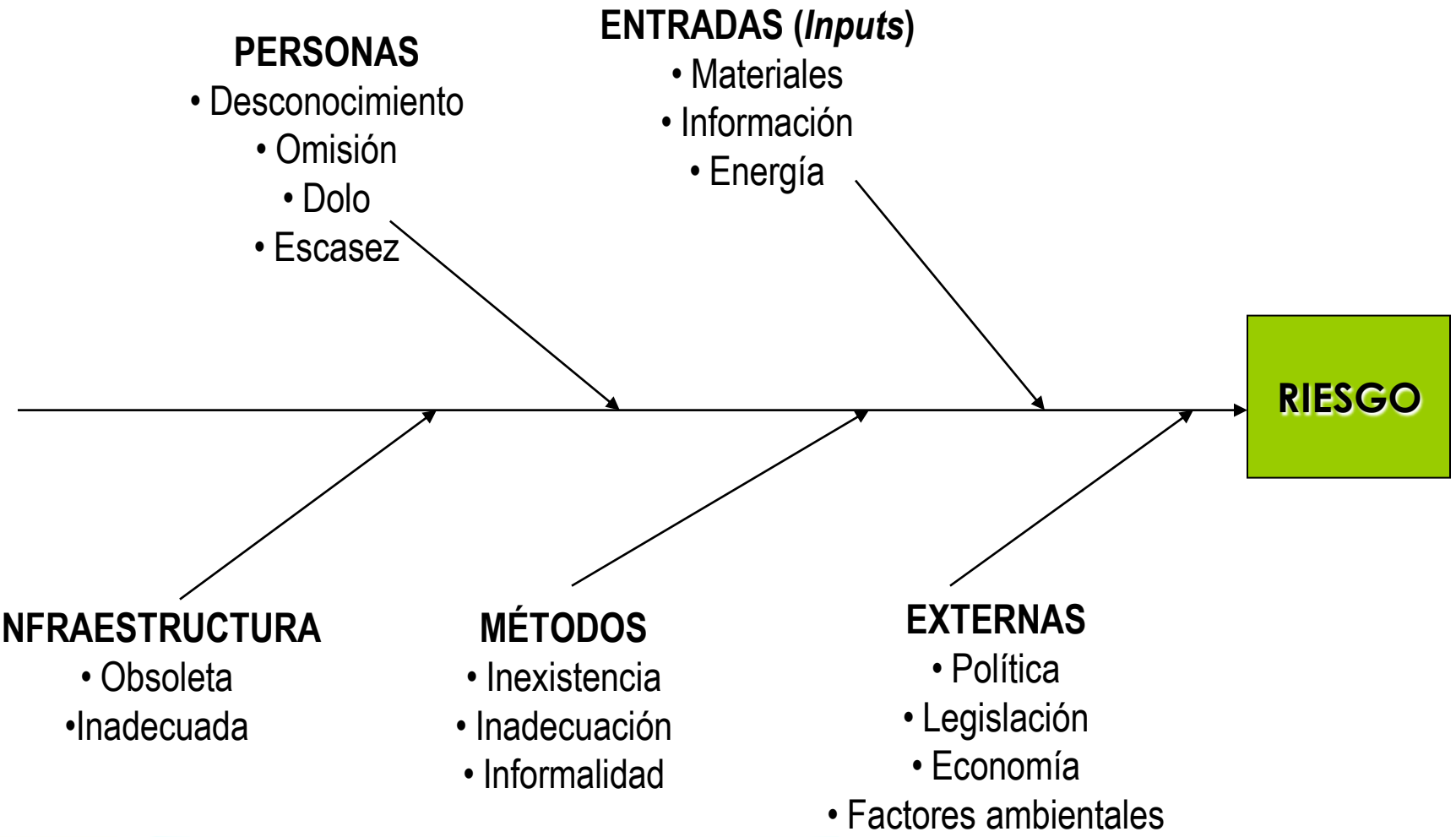
Cambiar la **probabilidad:**

"Probabilidad (*Likelihood*).
Oportunidad de que algo suceda."

REDUCIR EL RIESGO (NTC ISO31000: 2011)

Cambiar la **probabilidad:**
Prevenir la ocurrencia de las causas del riesgo.

CAUSAS DEL RIESGO



REDUCIR EL RIESGO (NTC ISO31000: 2011)

Cambiar las **consecuencias: Consecuencia.** Resultado de un **evento** que afecta a los objetivos.

REDUCIR EL RIESGO

Cambiar las **consecuencias:**

ÁREA DE IMPACTO DE LA CONSECUENCIA	ACCIÓN PARA MITIGAR LA CONSECUENCIA
Imagen o reputación	Plan de manejo de crisis
Continuidad de la prestación del servicio	Plan de continuidad del negocio
Calidad de la prestación del servicio	Sistema de peticiones, quejas, reclamos y sugerencias
Legal (sanciones)	Soporte jurídico para atención de litigios Procesos disciplinarios internos
Ambiental, seguridad de la información, seguridad y salud en el trabajo	Plan de preparación y respuesta ante emergencias
Financiero	Pólizas de seguros

COMPARTIR O TRANSFERIR EL RIESGO

1. Financiación del riesgo
2. Alianzas o convenios
3. Pólizas de seguros
4. *Outsourcing*

ASUMIR EL RIESGO

"No tomar ninguna acción cuando la organización acepta el propio riesgo, basándose en su efecto potencial o en el costo de las acciones necesarias." (GTC ISO9002:2017)

TOMAR EL RIESGO PARA APROVECHAR UNA OPORTUNIDAD

1. Implementar los planes, programas y proyectos del plan de desarrollo.
2. Adoptar una nueva tecnología.

Auditoría a la gestión de riesgos versus Auditoría basada en riesgos

IMPORTANCIA DE LA GESTIÓN DE RIESGOS PARA LA AUDITORÍA

"La gestión de riesgos es una preocupación primordial para los comités de auditoría. Más del 40% de los miembros de los comités de auditoría creen que sus programas y procesos de gestión de riesgos necesitan "mucho trabajo" aún, y un porcentaje similar, que cada vez es más difícil vigilar estos grandes riesgos."

(KPMG International. ¿Está todo bajo control?. Revista Gestión & Desarrollo Económico y Financiero. Junio 2017)

Marco de referencia para la gestión del riesgo

Auditoría a la gestión de riesgos

Proceso para la gestión del riesgo

Marco de referencia para la gestión del riesgo

BASES

La política
Los objetivos
El comando
El compromiso

DISPOSICIONES

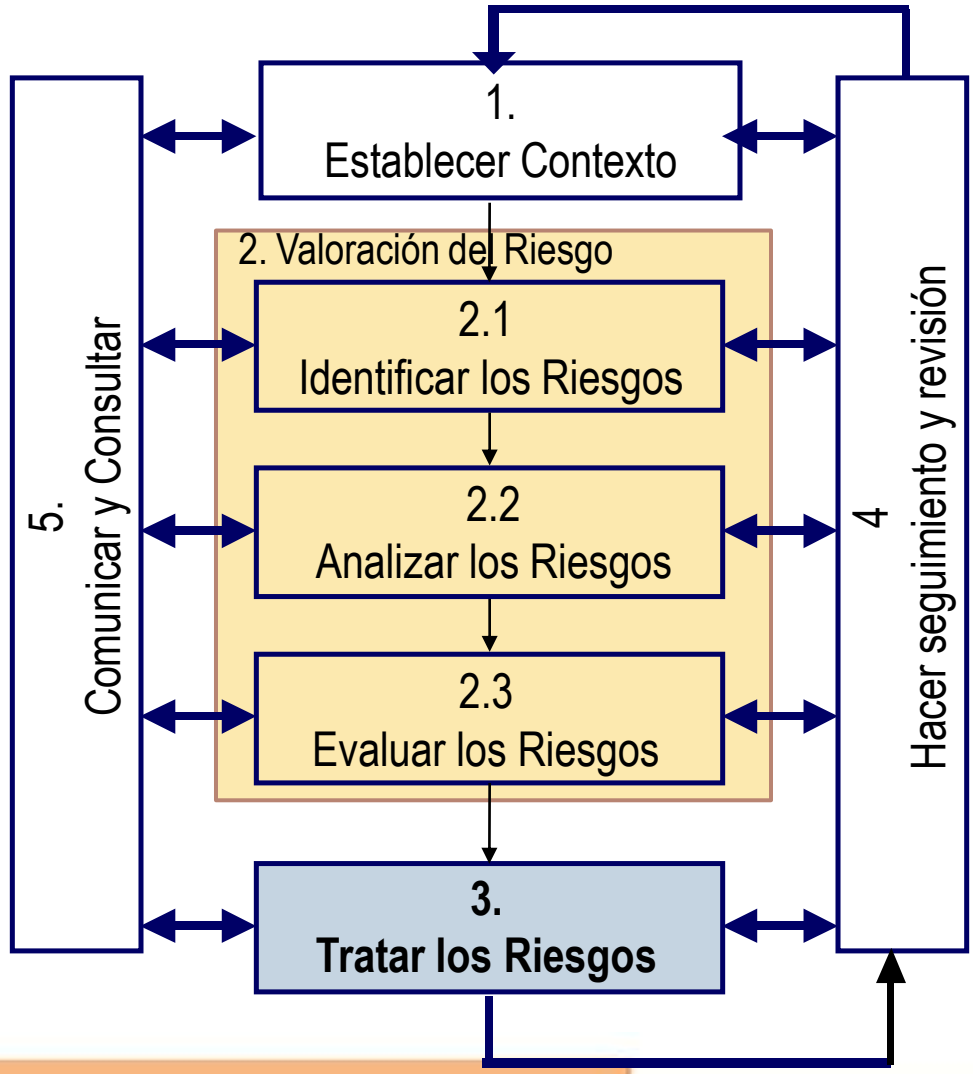
Planes, relaciones, rendición de cuentas (*Accountability*), recursos, procesos y actividades

Marco de referencia para la gestión del riesgo

Auditoría a la gestión de riesgos

¿Está definida y divulgada la política y los objetivos institucionales de gestión de riesgos?
¿Hay una estructura de responsabilidades, autoridades y rendición de cuentas para la gestión del riesgo?
¿Están definidos los mecanismos de comunicación interna y externa para la gestión del riesgo?

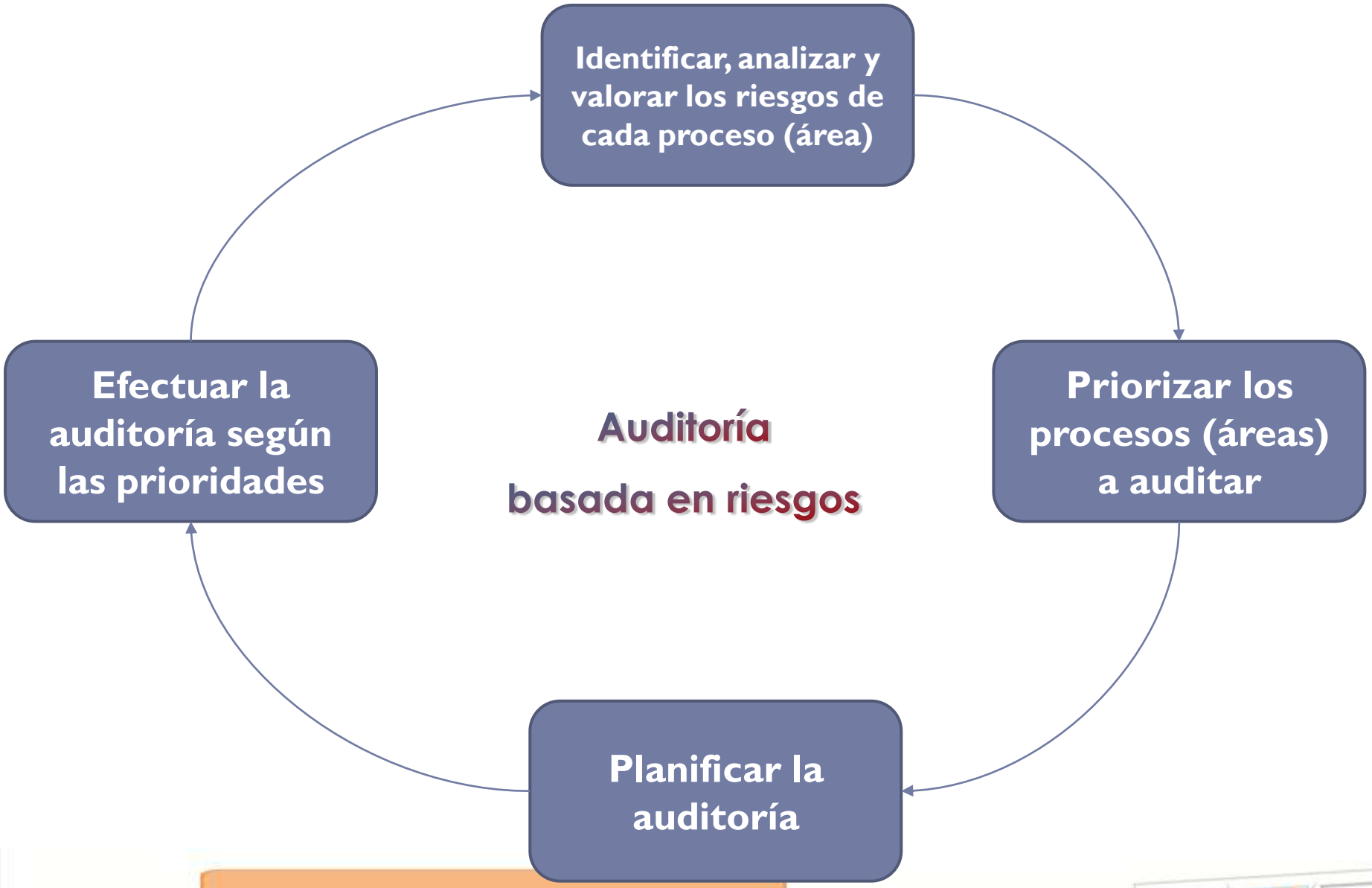
Proceso para la gestión del riesgo



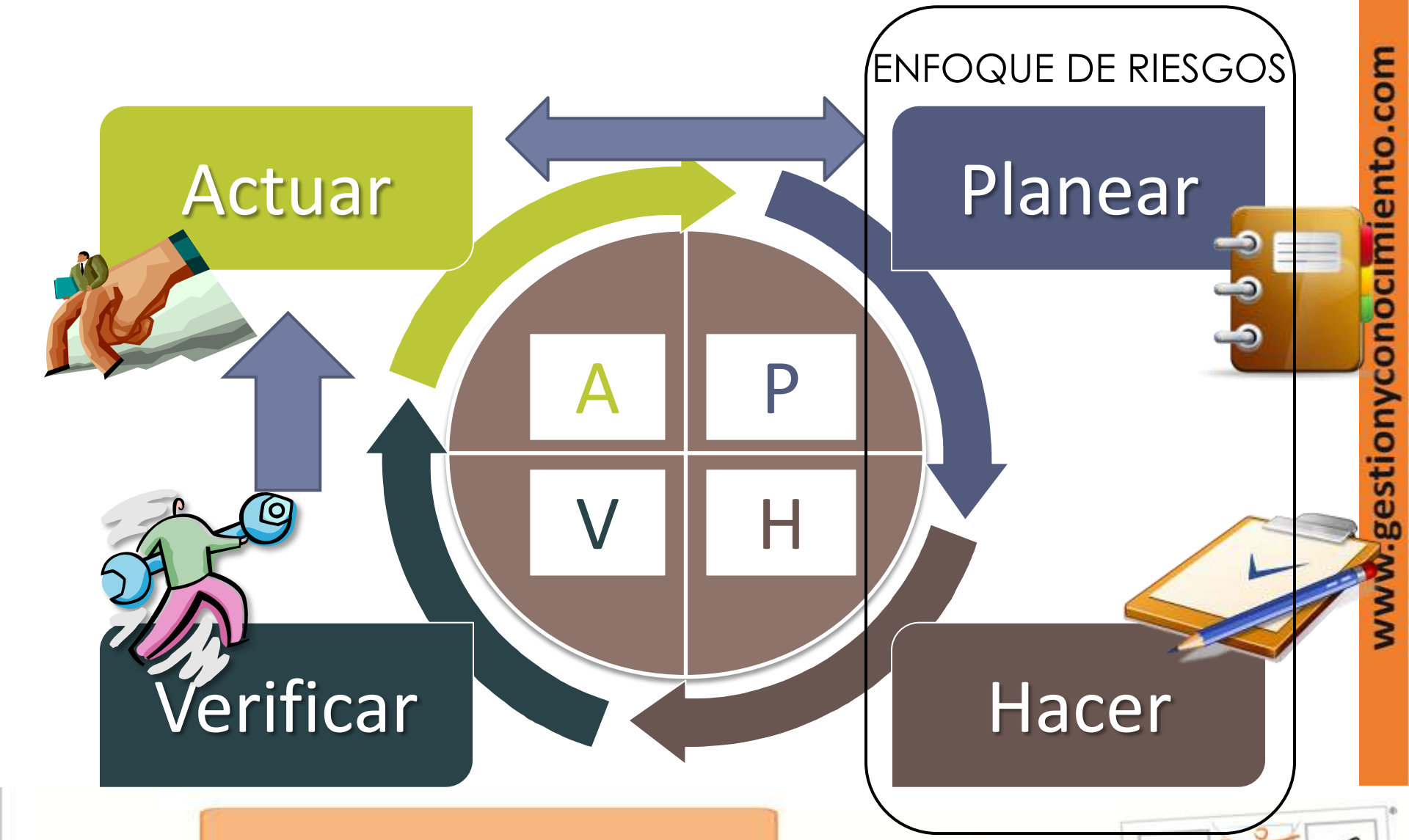
Auditoría a la gestión de riesgos

Proceso de gestión de riesgos

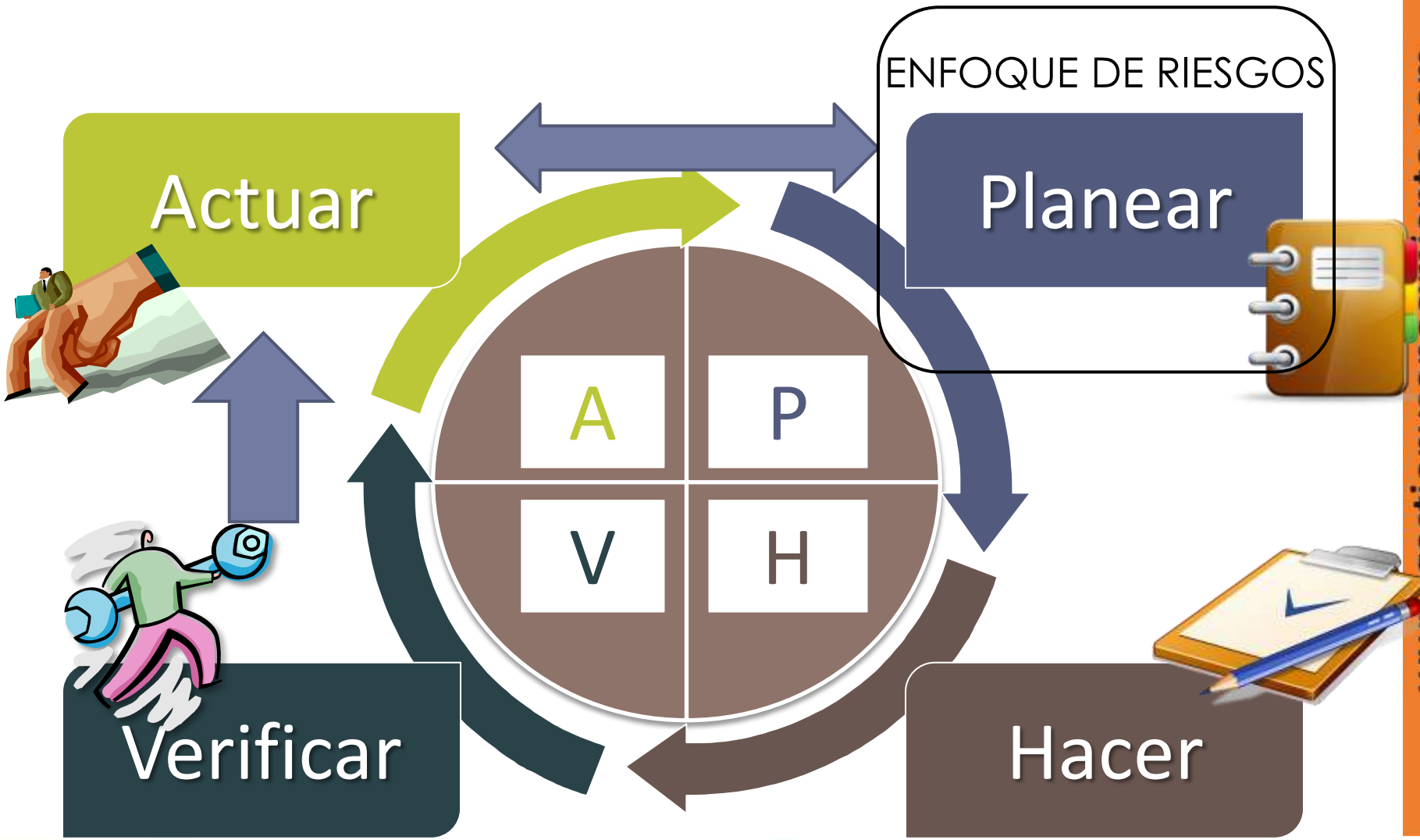
1. Identificación: ¿Hay riesgos que faltan por identificar? ¿Hay riesgos que ya no deben estar identificados? ¿Están adecuadamente determinadas las causas y las consecuencias?
2. Análisis y evaluación: ¿Ha cambiado la evaluación del riesgo?
3. ¿Se han implementado eficazmente acciones de tratamiento de los riesgos?



Ciclo de auditoría



Ciclo de auditoría



Priorización de las Auditorías

"Al abordar el proceso de planificación de auditoría, las unidades de auditoría interna se enfrentan a un problema económico, ya que generalmente **el Universo de Auditoría ofrece posibilidades casi ilimitadas para auditar**."

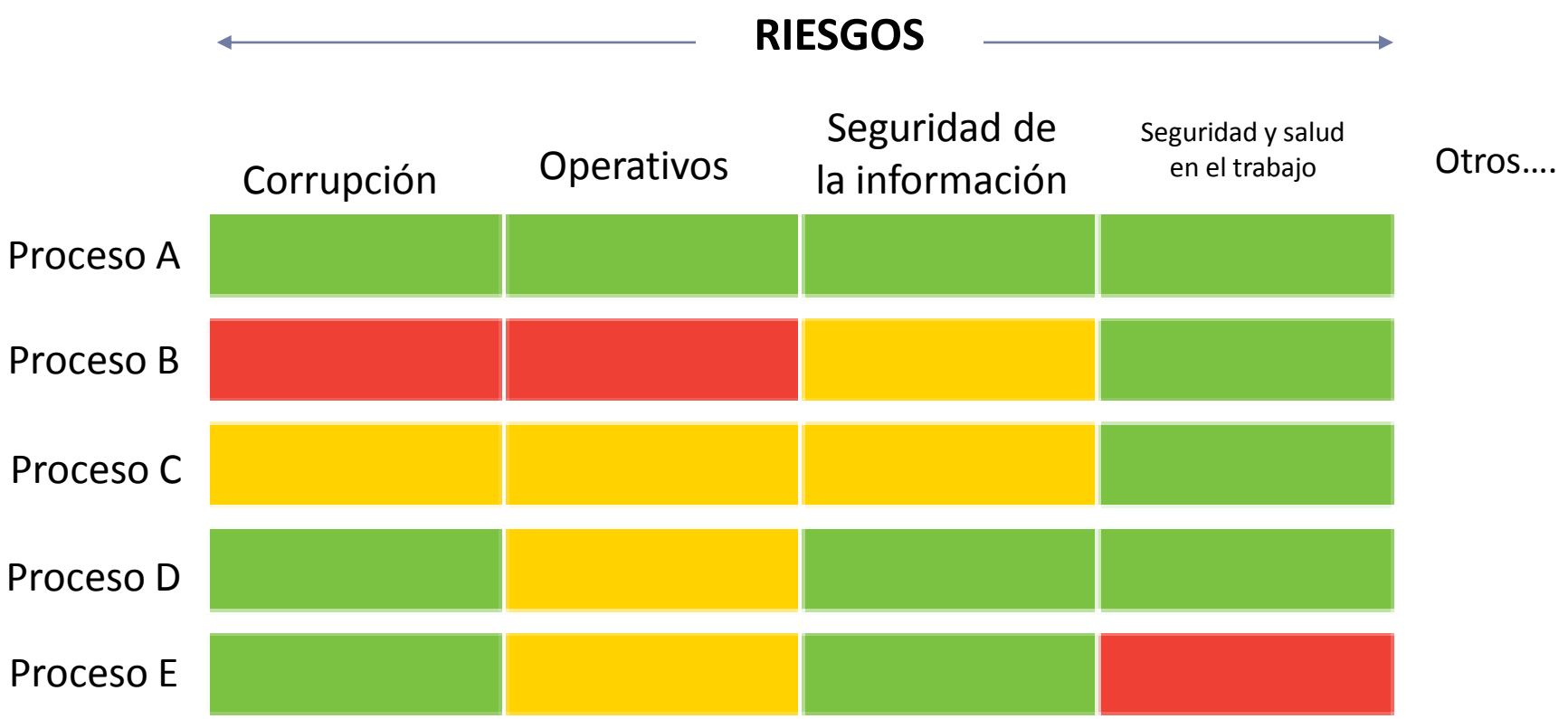
http://www.funcionpublica.gov.co/documents/418537/506911/Gu%C3%ADaAuditoriaEntidadesPublicas+V2Octubre2015/fcf84a18-5c74-480a-83c4-2a25ec49bea1

Priorización de las Auditorías

"Para tener como resultado una planificación adecuada, el auditor interno debe obtener información de todos los elementos relevantes para la organización, **incluyendo los riesgos**, factores internos y externos que podrían afectar el normal desarrollo de la misma."

http://www.funcionpublica.gov.co/documents/418537/506911/Gu%C3%ADaAuditoriaEntidadesPublicas+V2Octubre2015/fcf84a18-5c74-480a-83c4-2a25ec49bea1

Auditoría basada en riesgos



Fuente: Elaboración propia

Ciclo de auditoría

Actuar

Planear

A P V H

Verificar

ENFOQUE DE RIESGOS

Hacer

www.gestionyconocimiento.com

Gestión y Conocimiento
Consultoría Organizacional

Zafra Gutiérrez, Jaime Alejandro. Universidad Nacional de Colombia, 2010

Auditoría basada en riesgos

Gestión de los controles

1. ¿Documentado?
2. ¿Con responsable asignado?
3. ¿Con frecuencia definida?
4. ¿Manual o automático?
5. ¿Implementado?
6. ¿Efectivo?

GRACIAS

Federico Alonso Atehortúa Hurtado
Coordinador de Formación e investigación
Gestión y Conocimiento S.A.S.
Telefax: (4) 3524848
e-mail: federalo@gestionyconocimiento.com

www.gestionyconocimiento.com

Gestión y Conocimiento
Consultoría Organizacional