

# *Introducción a la* **Gestión Pública**

---

## **Gestión en el Estado**



# **INTRODUCCIÓN A LA GESTIÓN PÚBLICA**

## **GESTIÓN EN EL ESTADO**

*Un Estado al servicio de la ciudadanía*

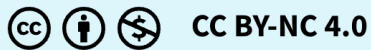
**Mario Weissbluth – Editor General**

**Ximena Pizarro y Analía Medrano – Editoras**

**Centro de Sistemas Públicos**


**Universidad de Chile**


**2019**



## **Creative Commons Attribution-NonCommercial 4.0 International**

This license requires that reusers give credit to the creator. It allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, for noncommercial purposes only.

 **BY:** Credit must be given to you, the creator.

 **NC:**  
Only noncommercial use of your work is permitted. *Noncommercial means not primarily intended for or directed towards commercial advantage or monetary compensation.*

Este libro se distribuye bajo la licencia

### **Creative Commons Atribución–NoComercial 4.0 Internacional (CC BY-NC 4.0).**

Usted es libre de compartir (copiar y redistribuir) y adaptar (remezclar, transformar y construir a partir del material), siempre que otorgue el crédito correspondiente a los autores y no utilice el material con fines comerciales.

Para más información sobre los términos de esta licencia:

<https://creativecommons.org/licenses/by-nc/4.0/>

# SECCIÓN III: HERRAMIENTAS DE GESTIÓN

## 12. LA VITAL GESTIÓN INTEGRAL DEL RIESGO

*Mario Weissbluth con la colaboración de Rafael del Campo y José Inostroza*

### **Gestión integral de riesgos**

No es exagerado decir que un buen gerente público, para tener éxito, debe dedicar un porcentaje significativo de su tiempo, junto con su equipo, a “olfatear” la existencia de riesgos, evaluarlos y prevenirlos, con una visión e incluso una intuición sobre la complejidad de los sistemas. Si tuviéramos que escoger una función estratégica de las múltiples mencionadas en este texto, la gestión de riesgos es una de las prioritarias, que además, consume comparativamente muy poco tiempo y esfuerzo en desarrollarla.

Diariamente sabemos del fracaso de emprendimientos: entre el 80% y el 90% de los negocios de menor tamaño fracasan en los primeros 3 años; escuchamos a menudo de sobrecostos, irregularidades y corrupción en grandes proyectos de infraestructura y/o tecnología en América latina; así como de gobiernos con mayoría parlamentaria que no son capaces de estructurar mecanismos de acuerdos/gobernanza orientados al éxito en sus políticas públicas

Las famosas “Leyes de Murphy” dicen: a) todo lo que puede fallar...falla, b) cuando las cosas fallan, fallan de la peor manera posible. Esto puede ocurrir en:

- Un proyecto en particular
- Una cartera de proyectos
- Conflictos de intereses
- Un cambio institucional significativo (cambio en el modelo de atención, cambio tecnológico, transformación digital, entre otros)
- Falta de aseguramiento de la continuidad operacional y la mejora continua de procesos
- Gestión institucional que no toma en cuenta directrices para minimizar riesgos de fraudes, acciones del crimen organizado, deterioro del contexto económico, entre otros.
- Falta de prevención de los efectos de desastres naturales de alto impacto.  
¿Cuántas muertes hemos leído en la prensa por derrumbe de represas?

La gestión integral de riesgos es una función de humildad, inteligencia, sagacidad, conversaciones significativas con los actores e intereses relevantes, acceso a información clave y de disciplina metodológica, para analizar riesgos y anticiparnos a sus probables consecuencias. Decimos “humildad” pues psicológicamente la primera barrera a superar es nuestra humana tendencia a no querer ver fallas, a “barreras bajo la alfombra”, porque duele confrontar la realidad, hasta que esta explota mucho peor que cuando el riesgo se estaba gestando. Los riesgos más importantes tienen una gran capacidad de camuflarse...no andan por ahí con un cartel anunciando su existencia; así que no es trivial identificarlos de lejos; muchas veces son propiedades emergentes (como los temas políticos complejos)

**El RIESGO tiene que GESTIONARSE, de una MANERA PROACTIVA, no reactiva**

Gestionar riesgos en el sector público requiere de competencias técnicas y relacionales. Una de las mayores amenazas en las instituciones públicas proviene de ignorar o minimizar los síntomas detectables en stakeholders, actores externos e internos (personas o instituciones) que están o puedan estar involucradas o influidas o que tengan influencias respecto a nuestro quehacer. Algunos directivos públicos caen tarde en la cuenta de la razón por la que sus proyectos no fueron exitosos: haber identificado mal a TODOS los stakeholders, lo que imposibilitó el mantenerlos informados, motivados, o a lo menos neutralizados.

Es responsabilidad de los directivos la definición de la estrategia institucional y la identificación de eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro de un rango aceptable criticidad y proporcionar una seguridad razonable sobre el logro de los objetivos institucionales.

### **Metodología de gestión de riesgos**

La gestión de riesgos es una combinación inteligente entre componentes relacionales o sutiles y gestión estructurada.

### **Mapeo de actores e intereses relevantes**

Los componentes relacionales o sutiles dicen relación con la lectura de los intereses en juego, vía conversaciones con los actores relevantes y análisis de escenarios. El mapeo de actores busca identificar a los actores concernidos con un determinado problema o desafío, distinguiendo aquellos que más pueden contribuir al objetivo buscado, así como quienes más pueden obstaculizarlo, dependiendo de los intereses propios de cada quien (“grupos de interés”), las orientaciones más o menos favorables al proceso según dichos intereses (actuales, de corto plazo; y posibles futuros de mediano o largo plazo), los niveles de poder e influencia que tienen o pueden ejercer respecto del proceso según sus intereses u orientaciones, y las relaciones de cooperación o conflicto entre los diferentes actores concernidos. El diálogo multi-actor facilita la construcción de lazos de asociación para el establecimiento de metas en común, nutriendo con ello a los actores en la toma de decisiones.

**Muchas veces los directivos públicos pecamos de excesos tecnocráticos y perdemos sensibilidad política para ver a los tiburones debajo del agua.**

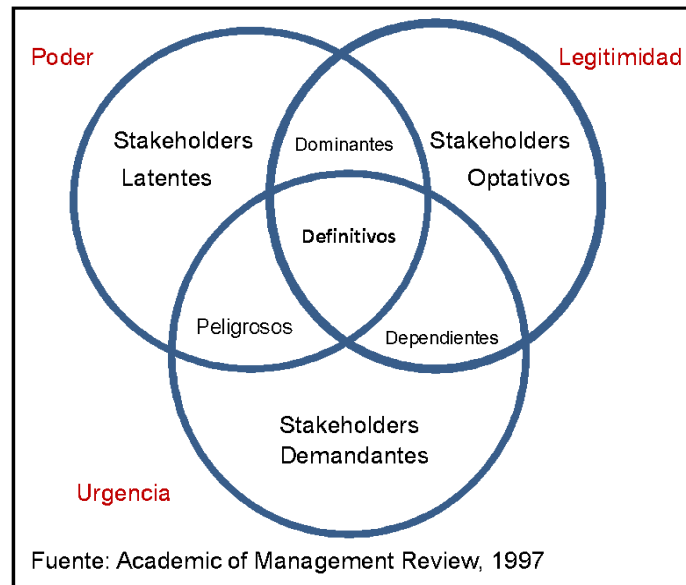
Para identificar el tipo de actores, proponemos usar una “**tipología de stakeholders**” (Mitchell, 1997), que permite identificar sus posiciones de poder y legitimidad, y cómo a partir de ello, pueden relacionarse respecto de una determinada iniciativa, oportunidad o propósito. Dicha tipología considera la combinatoria de 3 tipos de atributos o características de los grupos de interés: legitimidad, urgencia y poder. Según la presencia o ausencia de dichas características, se distinguen 7 tipos de actores, a saber:

- Latentes: tienen poder, pero carecen de legitimidad, y no poseen reclamaciones.
- Discretos: tienen legitimidad.
- Demandantes: tienen reclamos, pero no poder y legitimidad.
- Dominantes: tienen poder y legitimidad, pero no urgencia.
- Dependientes: tienen urgencia y legitimidad, pero no poder.
- Peligrosos: tienen poder y urgencia, pero no legitimidad.

- Definitivos: poseen los tres atributos (legitimidad, urgencia y poder).

Su distribución, puede graficarse como sigue:

*Ilustración 1: tipología de stakeholders*

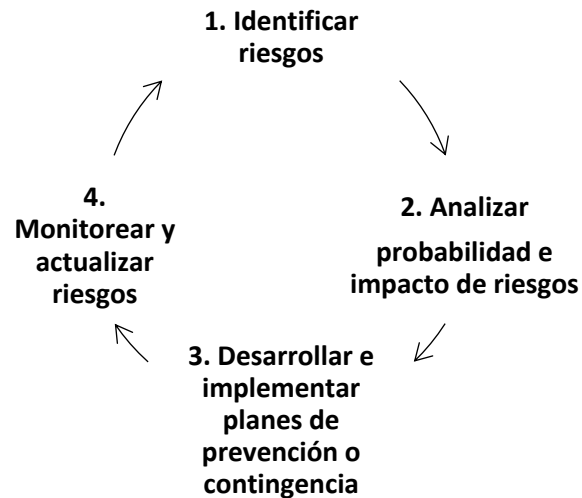


Una vez que determinamos los actores que resulten de mayor interés para efectos del diagnóstico, en consideración a sus posibilidades de incidencia en el proceso a impulsar, se procede al “mapeo” de orientaciones según sean sus intereses respecto del proceso de cambio, así como de los niveles de poder e influencia respecto de ello, y de las relaciones posibles de gestionar en función del desarrollo de alianzas o coalición en función de dicho proceso.

### **Matriz de riesgos**

La gestión formal de riesgos es una práctica analítica, preventiva, anticipatoria de las emergencias y flexible ante escenarios cambiantes, como producto de hechos emergentes, de las decisiones de terceros o de nuestra propia organización, que se puede organizar en cuatro pasos.

Ilustración 2: Pasos de la gestión de riesgos



1.- Identificar riesgos: reconocerlos y describirlos.

2.- Analizar/evaluar el impacto de los riesgos: Determinar su posibilidad de ocurrencia, aunque sea aproximadamente. Determinar la magnitud de los daños en caso de que se verificara, aunque sea aproximadamente. **Nunca encontrará un algoritmo que le permita calcular matemáticamente las probabilidades e impactos.** El único que sirve es el “estómago” colectivo del equipo que está elaborando el análisis.

3.- Tratar los riesgos: Desarrollar planes de mitigación de riesgos (para evitar que ocurran) y de contingencia (para tener un “plan B” en caso de que ocurran para mitigar los impactos residuales).

4.- Monitorear y actualizar riesgos: Vigilar su evolución, sus potenciales alteraciones o agravaciones, así como la aparición de nuevos riesgos.

Un sistema corporativo ayuda a identificar los diferentes procesos de la organización que suponen un riesgo para la consecución de los objetivos institucionales. A nivel internacional existe la Norma de Gestión de Riesgos ISO 31000<sup>1</sup>, que establece los principios, el marco y proceso para la gestión de cualquier tipo de riesgo de forma transparente, sistemática y fiable en cualquier ámbito o contexto.

En dicho marco, las entidades deben contar con una Política de Riesgos, con definición de roles y estructuras. Deben realizar un levantamiento sistemático y/o revisión de los procesos de la institución, identificando, analizando y valorizando los riesgos críticos y sus controles mitigantes y en especial, la formulación de medidas de tratamiento de dichos riesgos, expresada en una Matriz de Riesgos Estratégicos, identificando claramente a los responsables de la identificar y mitigar los riesgos. **Si existen riesgos muy probables y de grave impacto, debe aparecer en el escritorio de los directivos máximos de manera inmediata.** Muchas veces hay verdaderas catástrofes institucionales cuyos riesgos ya se conocían, pero no por parte de los directivos... nada se hizo.

<sup>1</sup> <https://www.iso.org/iso-31000-risk-management.html>

Dicha matriz es una herramienta de gestión del equipo directivo institucional, que le sirve para sistematizar el análisis de los procesos, sus riesgos, la severidad de los mismos, los controles asociados, la exposición al riesgo que presenta cada uno y las estrategias y acciones para riesgos en niveles de exposición no aceptables, mediante Planes de Tratamiento.

Suena tedioso, ¿verdad? Sí, pero... Hágalo.

Requiere una alta capacidad de intuición y recuerde que varios ven y evalúan riesgos mejor que una sola persona. Trábjelo en equipos.

El objetivo de esta herramienta principal es visualizar con facilidad los riesgos. No exageramos al decir que el gerente de un cierto ámbito, organización o proyecto debiera tener esta matriz en su escritorio o como un cuadro en la pared.

Como ejemplo, a continuación veremos la forma de aplicar una matriz de riesgos a un proyecto específico de adquisición e implementación de una plataforma de gestión documental, para digitalizar los procesos institucionales. El objetivo del proyecto es lograr menores tiempos en procesos, contar con documentos digitales a disposición de todos los involucrados, menores costos de recepción y proceso de documentos, entre otros.

#### EJEMPLO FICTICIO DE MATRIZ DE RIESGO DE UN PROYECTO

Categoría del riesgo	Descripción de los eventos riesgosos	Probabilidad de ocurrencia (0 a 100)	Impacto 1:Mínimo 5: Catastrófico	Riesgo P*I	Acciones preventivas o de contingencia
Político o conflictos intra o extra Proyecto	No contar con el apoyo del Ministro para el Proyecto	20	5	100	Presentaciones previas al gabinete de asesores del Ministro, destacando los resultados de corto plazo
Administrativos, contractuales o presupuestarios	No aprobación de la inversión por la Oficina de Presupuesto	50	5	250	Revisión previa y mejora del proyecto en conjunto con los profesionales de Gobierno Digital
Descoordinación y desinformación	Falta de acuerdo entre las áreas, respecto a la velocidad del cambio.	80	3	240	Constituir equipo de integración de procesos multi áreas. Realizar laboratorios de pruebas por proceso
Defectos técnicos	Lentitud de la plataforma ante múltiples requerimientos	70	5	350	Pagos al proveedor basados en niveles de servicio (SLA) Múltiples casos de uso en plataforma de prueba
Falta de claridad en alcances, plazos y costos	Necesidad de efectuar cambios en otros procesos, para integrarlos a la plataforma de gestión documental	60	4	240	Levantar mapa completo de procesos, indicando el impacto de la gestión documental en ellos. Dimensionar y presupuestar cambios requeridos, asociados a los ahorros potenciales

Insatisfacción o cambio de foco del cliente	Resistencia de los usuarios del Servicio a reemplazar documentos físicos por digitales, en sus trámites	40	2	80	Destacar las ventajas de tiempo de proceso de los trámites digitales. Digitalizar los documentos físicos recibidos, para iniciar procesos sólo por vía digital. Trabas progresivas a la recepción de documentos físicos
Deficiente integración de terceros	Exigencia de los usuarios de realizar trámites en papel	60	2	120	Detectar "normas con exigencia de papel" y solicitar cambios legales. Suscribir convenios con otras entidades que faciliten la integración de procesos digitales

Vea usted que, en este caso ficticio, los defectos técnicos son los que presentan los mayores riesgos en cuanto a su probabilidad de ocurrencia e impacto. Hay que aplicarse a ellos a la brevedad. Y de ahí seguir hacia abajo de acuerdo a su valor de P\*I.

Las acciones preventivas son actividades "rentables" para reducir, contener y/o controlar los riesgos del proyecto. Esto quiere decir que el costo de la prevención debe ser menor que el costo financiero o político de la materialización del riesgo. Las acciones de contingencia, en cambio, generan un colchón para eventos inesperados. Un plan formal de contingencia se debe desarrollar cuando las acciones preventivas no son viables o son muy costosas.

### Una anécdota ilustrativa

Una consultoría a un importante ministerio chileno, contemplaba realizar un diagnóstico institucional y una propuesta de mejoras de gestión. Como parte estándar de la metodología de trabajo, solicitamos todos los informes pertinentes: consultorías previas, informes anuales, etc. En ese país hay una norma de gobierno, consistente en mantener anualmente actualizada una matriz de riesgo de los procesos institucionales. De hecho, hay un departamento de auditoría interna que tiene ésta como parte de sus obligaciones.

Al revisar la matriz, quedamos verdaderamente impactados. Había no menos de 20 riesgos caracterizados como de nivel máximo, y la mayoría de ellos podía, en caso de materializarse, generar una crisis institucional, con repercusiones en la prensa, etc. Estaba elaborada hacía 4 meses.

Al preguntarle a los auditores si habían entregado esta matriz a las autoridades (Ministra y Subsecretario), nos indicaron que sí, que les habían enviado un memorándum con la matriz, pero que no habían recibido ninguna respuesta.

Decidimos que no tenía mucho sentido hacer esta consultoría antes de ayudar a mitigar todos estos riesgos. Por tanto, solicitamos entrevista con el subsecretario, un personaje que conocíamos de antes, y como de costumbre, muy político y muy amable. Por cierto, en Chile los Subsecretarios son los responsables de la gestión de los ministerios. Cuando le mostramos la matriz y le pedimos su opinión, su respuesta fue... "ahhh, siiii, recuerdo

haberla visto hace algún tiempo pero en realidad me aburrí revisándola y no le di mayor importancia"... y en toda su actitud se notaba que ni siquiera entendía el concepto.

Pedimos entonces hablar con la Ministra (de un partido político diferente al del subsecretario) y tuvimos el buen cuidado, antes de mostrársela, de explicarle en detalle en qué consistía esta matriz, cómo se elaboraba, y cuáles eran sus implicaciones. Luego, le mostramos los riesgos, y ahí sí que ella palideció, se preocupó, y formó un equipo para enfrentar estas verdaderas amenazas.

Las moralejas: a) esta institución elaboraba esta matriz como una obligación burocrática impuesta por el gobierno central; b) los auditores, si bien hacían correctamente la matriz, no tenían ninguna capacidad ni interés por "venderle el concepto" a las autoridades superiores, y c) el Subsecretario no tenía ninguna capacidad ni interés por gestionar los riesgos. Nuestro mayor valor agregado a esta institución fue, en realidad... hacerles notar lo que ellos sabían.

### **Errores que deben evitarse al realizar la evaluación de riesgos**

**No generar un ambiente de confianza** para que todos puedan aportar respecto a identificar los riesgos que visualizan.

**Poner el foco en riesgos puntuales vigentes** y no tener un enfoque sistemático para identificar todos los riesgos.

**Concentrarse en riesgos individuales**, sin tener en cuenta el panorama general. La "lista de prioridades" debe partir desde los riesgos mayores hacia los menores y cómo actuar en relación con ellos.

**Evaluaciones disociadas de los procesos.** Es necesario conocer muy bien los procesos y solo así podrá identificar todos los riesgos potenciales y planificar las medidas para gestionarlos.

**Realizar la evaluación como una tarea obligada y burocrática**, sin conciencia real de su necesidad y aporte de valor. Una evaluación bien hecha y las medidas que se tomen en base a eso ciertamente evitarán muchas consecuencias no deseadas a las personas y a la institución.

**No identificar factores desencadenantes de cada riesgo.** Los desencadenantes son indicadores de que el riesgo se ha desarrollado u ocurrirá pronto. Para identificar estos indicadores, debe hablar con las personas que saben en detalle cómo y qué podría suceder en su lugar de trabajo. Los indicadores son la base del posterior sistema de monitoreo de riesgos.

**Evaluaciones desactualizadas.** A medida que se introducen nuevos equipos, nuevos procesos, nuevos empleados, se necesita complementar, modificar y ajustar la evaluación de riesgos.

**Evaluaciones excesivamente complicadas.** Determine en forma simple los riesgos y sus consecuencias, con las personas que tienen experiencia en el área, para descubrir factores que no son obvios a primera vista, y concéntrese en los riesgos principales.

**No tomar en cuenta las características de las personas relacionadas con un trabajo en particular.** No es lo mismo si tiene un empleado con experiencia o un principiante, una persona con discapacidades o una mujer embarazada a punto de salir con licencia, al evaluar los riesgos de una actividad. No olvide a las personas que no son sus empleados, pero que son importantes para cada actividad, como visitantes, usuarios, y proveedores.

## Riesgos críticos

La consultora británica AON [1] elaboró un ranking de riesgos críticos a nivel global, a partir del análisis de grandes entidades privadas. El cuadro siguiente muestra para 2017, los 28 principales riesgos, cuáles de ellos no tenían cobertura en seguros (destacados en gris oscuro), cuáles tenían una cobertura parcial o mínima (en blanco) y cuáles sí tenían cobertura en seguros (gris claro). Por cierto, lo relevante de este cuadro no es la cobertura de seguros propia del sector privado, sino sus componentes intrínsecos.

*Ilustración 3: Principales riesgos para el sector privado*

1. Daño a la reputación o marca	2. Desaceleración económica	3. Incremento de la competencia	4. Cambios regulatorios
5. Cibercrimen y hackeos	6. Incapacidad de innovar o responder a la demanda de clientes	7. Incapacidad de atraer o retener talentos	8. Disrupción de los negocios, cambio en su base de rentabilidad
9. Incertidumbres políticas	10. Responsabilidad de terceros	11. Precios de materias primas	12. Ilquidez
13. Daño a la propiedad	14. Responsabilidad de directivos y ejecutivos	15. Falla mayor de proyectos	16. Fluctuaciones de tipo de cambio
17. Responsabilidad social corporativa y sostenibilidad	18. Falla tecnológica y de sistemas	19. Falla o disrupción de cadena de suministros	20. Innovación o tecnologías disruptivas
21. No disponibilidad de Capital o Crédito	22. Crédito de contraparte (Garantías)	23. Crecientes costos y consecuencias de Compliance	24. Desastres naturales y meteorológicos
25. Incapacidad de implementar o comunicar la estrategia	26. Restructuraciones, fusiones y adquisiciones	27. Accidentes laborales y daño a los trabajadores	28. Fallas en planes de recuperación de desastres o continuidad de servicios

Fuente: AON

De los anteriores, si centramos la mirada sólo en entidades públicas, los motivos críticos más frecuentes son: 1. Daño a la Reputación institucional, que pueden producirse por ejemplo, al dejar de entregar un servicio crítico a la ciudadanía, 4. Cambios regulatorios, 5. Cibercrimen y hackeos, 6. Incapacidad de innovar o responder a la demanda de clientes, 7. incapacidad de atraer o retener talentos, 9. Incertidumbres políticas, 15. Falla mayor en proyectos y 18. Falla tecnológica y de sistemas.

De acuerdo al análisis anterior, el riesgo reputacional es el de mayor incidencia. En un reciente ensayo, “La organización amenazada” [2], su autor propone que para que una

organización subsista y prospere necesita relacionarse adecuadamente con su entorno de stakeholders, lo que incluye a todos los que se ven afectados por la existencia y las iniciativas de una entidad: usuarios, proveedores, competidores, complementadores, reguladores, políticos, ambientalistas, entre otros.

Las relaciones pasan a ser más importantes que los activos o los productos/servicios de las organizaciones y sus estrategias de servicios y comunicacionales deben converger estratégicamente y adecuarse permanentemente. La gestión de relaciones ha pasado a ser una de las habilidades clave del liderazgo y explica la ventaja de la mayoría de las entidades más valoradas y admiradas, tanto en el sector privado como público.

### **Preguntas para reflexionar**

1. Si Ud. ha trabajado (o conocido de cerca) una institución pública: ¿ha observado que la práctica de elaboración de matrices de riesgo se efectúe, ya sea a nivel institucional o de proyectos específicos?
2. Si se han elaborado matrices de riesgo ¿se les ha dado seguimiento para realizar acciones preventivas o paliativas, o se hacen para cumplir un simple requisito burocrático?
3. La elaboración de matrices de riesgo ¿se ha hecho como un auténtico trabajo en equipo en que se han discutido constructivamente la existencia de los riesgos, sus probabilidades de ocurrencia y sus impactos? O la inversa, han sido elaboradas “a puertas cerradas” para cumplir con esa obligación.
4. Si Ud. ha participado u observado una verdadera “catástrofe institucional” o de un proyecto: ¿se podría haber evitado si se hubiera anticipado adecuadamente al desarrollar un análisis de riesgos?