Boletín
Oficina Control Interno
Fomento de la Cultura del Autocontrol y la Transparencia

Gestión de Riesgos y Controles

Líneas de Defensa

Define como la cultura, los procesos y la estructura organizacional debe administrar las OPORTUNIDADES POTENCIALES y los EFECTOS ADVERSOS, a través de un conjunto de acciones y elementos de CONTROL que al interrelacionarse fomenten la eficiencia y conserven la estabilidad institucional

Roles y Responsabilidades

L.E.

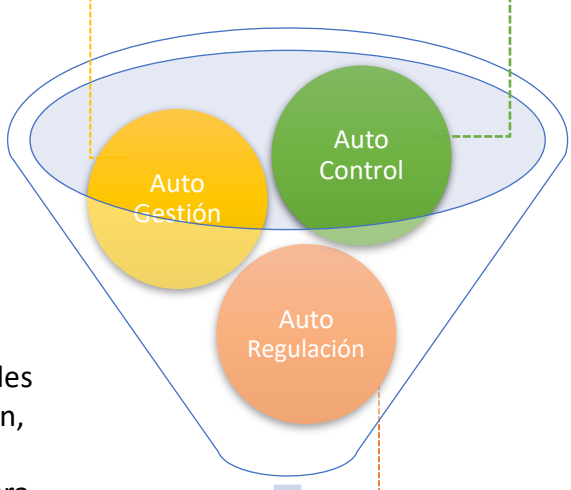
Línea Estratégica

Alta Dirección ⇨ Define la Política de Administración del Riesgo, analiza riesgos críticos y establece lineamientos para su mejora y los responsables del control interno

2ª L.

2ª Línea de Defensa

Oficina Asesora de Planeación ⇨ Como Responsable del Proceso Dirección y Planeación, define la Metodología de Administración del Riesgo, estableciendo roles, responsabilidades y controles para garantizar su aplicación, mejora y mantenimiento. Capacita, acompaña y genera recomendaciones.



Ejercicios de Control

1ª L.

1ª Línea de Defensa

Servidores ⇨ Detecta riesgos y ejecuta controles

⇧

Líder de cada Proceso ⇨ Gestionan los riesgos y hacen seguimiento a la aplicación de controles para garantizar su eficiencia

3ª L.

3ª Línea de Defensa

Oficina de Control Interno y Grupo de Gestión de la Calidad ⇨ Evalúa la gestión del riesgo y la aplicación de controles en las diferentes líneas, a través del ejercicio Auditor. Informa de los resultados para su mejora.

Auditoría Externa

Organismos de Control

AUTOCONTROL
Mejoramiento Personal e Institucional

Boletín
Oficina Control Interno

Fomento de la Cultura
del Autocontrol y la Transparencia

Gestión de Riesgos y Controles

Conceptos Básicos

IDENTIFICACIÓN del Riesgo

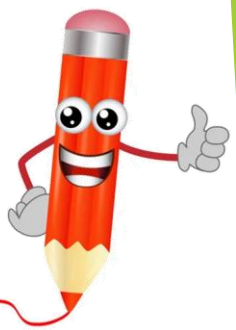
RIESGO: Exposición a una situación donde hay una posibilidad de sufrir un daño

- **DE GESTIÓN** — Posibilidad de ocurrencia de un evento potencial no doloso que pueda entorpecer los objetivos institucionales o del proceso
- **DE SEGURIDAD DE INFORMACIÓN** — Posibilidad de amenaza, vulnerabilidad o perdida de activos de información, software, hardware
- **FISCAL** — Efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial
- **DE CORRUPCIÓN** — Posibilidad de que, por acción u omisión (dolo), se use el poder para desviar la gestión de lo público hacia un beneficio privado

Riesgo = **¿Qué?** Impacto + **¿Cómo?** Causa Inmediata + **¿Por qué?** Causa Raíz → Sub-causa 1, Sub-causa 2

Lo que puede Ocurrir

- Impacto: Consecuencias de la materialización del riesgo
- Causa Inmediata: Circunstancias por las que se presenta el riesgo, pero no es la causa principal
- Causa Raíz: Causa principal o razón por la cual se puede presentar el riesgo



Ten en cuenta

El Riesgo **DE GESTIÓN** se diferencian de el **DE CORRUPCIÓN** porque su Causa NO es con Dolo

El Riesgo **DE SEGURIDAD DE LA INFORMACIÓN** siempre se identifica con pérdida de confidencialidad, integridad o disponibilidad de activos

En el Riesgo **FISCAL** las Causas pueden ser por Eventos Potenciales dolosos o no

No todo Impacto con Efecto Económico son Riesgo **FISCAL**, por ejemplo, los riesgos de daño antijurídico y efectos económicos generados por causas exógenas.

AUTOCONTROL
Mejoramiento Personal e Institucional

Boletín
Oficina Control Interno

Fomento de la Cultura del Autocontrol y la Transparencia

Gestión de Riesgos y Controles

Conceptos Básicos

VALORACIÓN del Riesgo

CONTROL: Medida o acción MANUAL o AUTOMATICA que permite reducir o mitigar el riesgo

- **PREVENTIVO** — Medida proactiva para evitar que los errores ocurran o se produzcan situaciones no deseadas, reduciendo riesgos y fomentando la eficiencia
- **DETECTIVO** — Medida de detección temprana, implementada en el desarrollo de la actividad, para tratar las causas que generan errores o irregularidades
- **CORRECTIVO** — Medida de mitigación del impacto que se implementa al materializarse el riesgo, pero que tiene costos implícitos

Ten en cuenta

Ciclo del Proceso

Entradas	Interrelaciones	Salidas
Recursos	Actividades	Producto/Servicio
PREVENTIVO	**DETECTIVO**	**CORRECTIVO**
Ataca CAUSAS Disminuye PROBABILIDAD	Detecta ERRORES Devuelve a PREVENTIVOS	Ataca CONSECUENCIAS Disminuye IMPACTO

Control = Respon sable + Acción + Comple mento

	Respon sable	Acción	Comple mento
Manual	Cargo del servidor que realiza el control	Verbo que indica el desarrollo/ejecución a realizarse como parte del control o medida	Detalles que permiten identificar el objeto del control o medida y los registros o soportes y a quien se comunica
Automático	Nombre del sistema que ejecuta la medida		

Estructura de CONTROL que aplica para definición en mapas de riesgos y documentos del COGUI+

Gestión de Riesgos y Controles

Conceptos Básicos

VALORACIÓN del Riesgo

NIVEL del Riesgo: Estrategia para obtener la valoración de CAUSAS e IMPACTOS

- **Capacidad** Máximo valor del Riesgo a partir del cual no es posible cumplir los objetivos
- **Tolerancia** Máximo valor admisible del Riesgo
- **APETITO del riesgo** Valor del riesgo que se puede aceptar

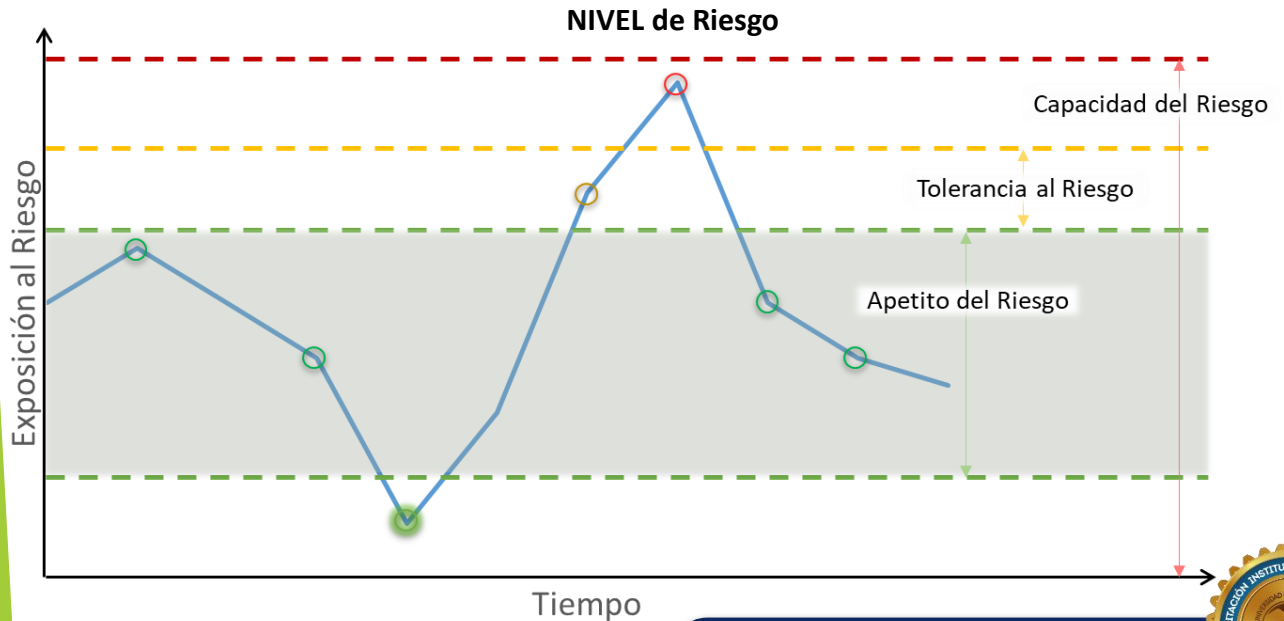
Ten en cuenta

Para determinar el **NIVEL** del riesgo, es necesario contar **INDICADORES CLAVES** del Riesgo

Los **INDICADORES CLAVES** del Riesgo son datos históricos sobre **eventos** relacionados

Los **eventos** relacionados pueden indicar mayor o menor exposición a determinados riesgos

Cada proceso debe definir **indicadores** y sus **métricas**, que registren los datos por periodos de tiempo



AUTOCONTROL
Mejoramiento Personal e Institucional

Boletín
Oficina Control Interno

Fomento de la Cultura
del Autocontrol y la Transparencia

Gestión de Riesgos y Controles

Conceptos Básicos

VALORACIÓN del Riesgo

ESTRATEGÍAS: Inclusión eficaz de la GESTIÓN e implementación de CONTROLES

- Evita la materialización del riesgo
- Permite reducir el impacto
- Proporciona agilidad para aprovechar oportunidades

REDUCIR

Riesgos en ZONA **MODERADA** o **ALTA** se determina si se **MITIGA** o **COMPARTE**

Plan de Acción

MITIGAR

Acciones para disminuir la probabilidad y el impacto de la materialización del riesgo. Pueden ser o no **Controles**

ACEPTAR

Riesgos en ZONA **BAJA** se determina **ASUMIR** los efectos de posible materialización. Riesgo de **Corrupción** NO puede ser aceptado

COMPARTIR

Tercerizar procesos o transferir el riesgo mediante pólizas. Transfiere Impacto Económico, pero no Reputacional. Riesgo de **Corrupción** *comparte* el riesgo, pero *no transfiere* responsabilidad

EVITAR

Riesgos en ZONA **EXTREMA** se determina **NO ASUMIR** o **ELIMINAR** en lo posible la actividad que genera el riesgo

Gestión de Riesgos y Controles

Conceptos Básicos

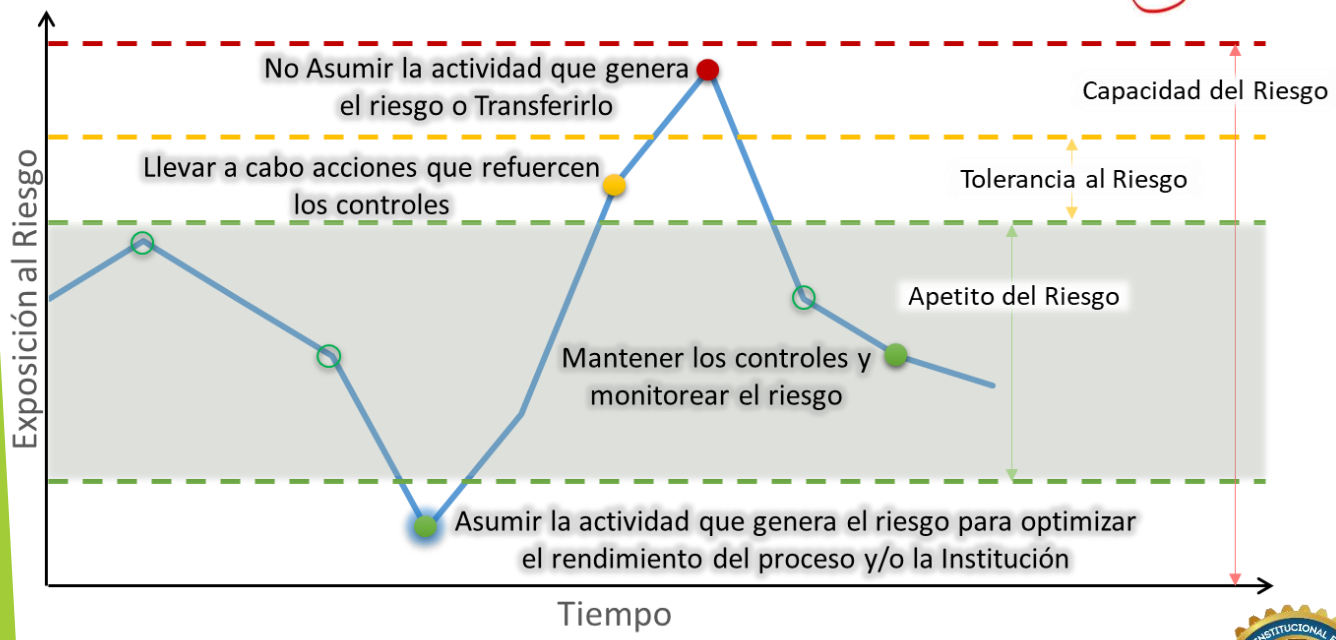
VALORACIÓN del Riesgo

ZONA de Riesgo: Permite determinar Estrategias según el NIVEL del Riesgo

DE GESTIÓN
DE SEGURIDAD DE INFORMACIÓN
FISCAL
DE CORRUPCIÓN

ZONA RIESGO		
EXTREMO	Evitar - Reducir	Eliminar - Evitar - Reducir - Transferir
ALTO	Evitar - Reducir	Eliminar - Evitar - Reducir - Transferir
MODERADO	Reducir	Eliminar - Evitar - Reducir
BAJO	Aceptar - Reducir	Evitar - Reducir

Ten en cuenta



Gestión de Riesgos y Controles

Ejemplos

Ejemplo 1 **DE GESTIÓN**

Proceso: Gestión de Contratación

Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Alcance: Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisiciones) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas

Riesgo = Impacto (¿Qué?) + Causa Inmediata (¿Cómo?) + Causa Raíz (¿Por qué?)

Lo que puede ocurrir

Posibilidad de

- Afectación económica
- Por multa o sanción del ente regulador

Debido a adquisición de bienes y servicios sin el cumplimiento de los requerimientos normativos

Causa Raíz → Sub-causa 1, Sub-causa 2

Control
PREVENTIVO
Ataca causa Raíz, identificando las sub-causas

Control = Respon sable + Acción + Comple mento

PREVENTIVO
Manual

- Evaluadores designados por el Ordenador de Gasto
- Verifica que la documentación suministrada por el proveedor cumpla con los requerimientos establecidos por tipo de contratación
- A través del CO-F33 Listado de documentos contractuales y lo deja registrado en el CO-F06 o CO-F07 Acta de Evaluación de Propuesta. Los resultados los comunica al jurídico de la dependencia Ordenadora

Gestión de Riesgos y Controles

Ejemplos

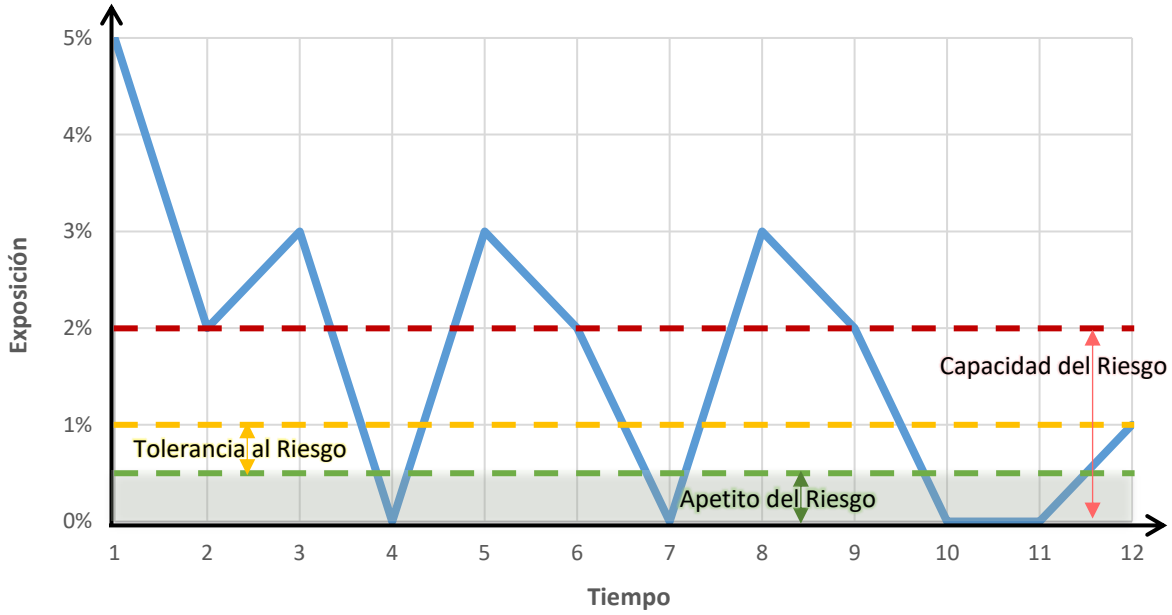
Ejemplo 1 **DE GESTIÓN**

Proceso	Indicador	Métricas
Gestión de Contratación	Bienes y servicios adquiridos sin el cumplimiento de requisitos	**1.** % de bienes-servicios adquiridos en el mes sin el cumplimiento de requisitos. **2.** Valor de bienes-servicios adquiridos en el mes sin cumplimiento de requisitos.

Tiempo: Meses
Exposición: %

Cálculo M1: $\frac{\text{Bienes y Servicios adquiridos en el mes sin el cumplimiento de requisitos}}{\text{Bienes y Servicios adquiridos en el mes}}$

Tiempo	1	2	3	4	5	6	7	8	9	10	11	12
Exposición M1	5%	2%	3%	0%	3%	2%	0%	3%	2%	0%	0%	1%



ANALISIS DE RESULTADOS: Se presenta % de adquisición de bienes-servicios fuera de la capacidad del riesgo, determinándose que las sub-causas, que producen estos resultados: 1. falencias en las *solicitudes de propuestas*, debido a que no se tienen en cuenta los requerimientos establecidos por tipo de contrato (CO-F33). 2. No se está ejecutando correctamente el control establecido.

PLAN DE ACCIÓN: ***Establecer Nuevo Control y Reforzar el Control existente***
Sub-Causa 1: * El jurídico de la dependencia Ordenadora verifica la información registrada por evaluadores, si conforme da visto bueno para firma del ordenador del gasto, en caso contrario devuelve.
* Líder de proceso capacita a personal que solicita propuestas en CO-F33
Sub-Causa 2: Establecer periodos y responsables de seguimiento a la ejecución del control preventivo.

Gestión de Riesgos y Controles

Ejemplos

Ejemplo 2 **DE SEGURIDAD DE INFORMACIÓN**

Proceso: Gestión de Talento Humano

Objetivo: Realizar las actividades necesarias para la vinculación, permanencia y bienestar laboral del personal vinculado a la institución.

Alcance: Inicia con la planificación de la planta de personal, selección, vinculación, administración de salarios y prestaciones, seguridad y salud en el trabajo y termina con la implementación de acciones frente a resultados de evaluación de gestión humana y clima laboral

Riesgo = Impacto (¿Qué?) + Causa Inmediata (¿Cómo?) + Causa Raíz (¿Por qué?)

Causa Raíz → Sub-causa 1, Sub-causa 2

Lo que puede ocurrir

Posibilidad de

- Pérdida de la integridad de información
- Por modificación no autorizada de la base de datos de nomina
- Debido al acceso por personal no autorizado al sistema de gestión de nomina

Control
PREVENTIVO
Ataca causa Raíz, identificando las sub-causas

Control = Responsable + Acción + Complemento

PREVENTIVO
Manual

- El administrador del sistema de gestión
- Identifica, limita y controla la asignación y el uso de los accesos privilegiados según roles definidos por el líder del proceso
- A través del sistema de gestión y deja registro en la base de datos de usuarios. Los resultados los comunica al líder del proceso

Gestión de Riesgos y Controles

Ejemplos

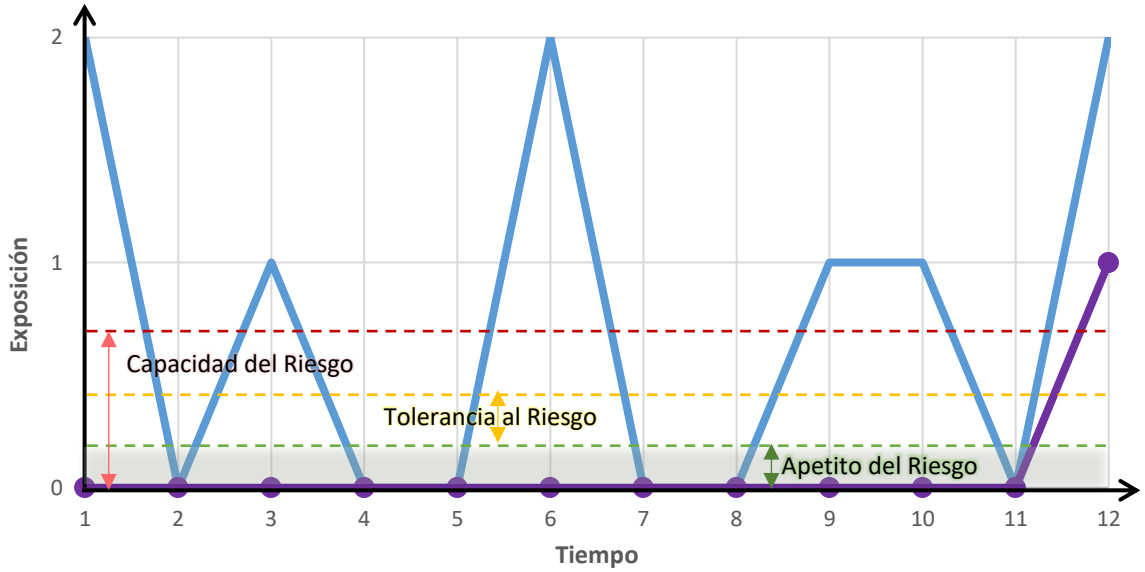
Ejemplo 2 **DE SEGURIDAD DE INFORMACIÓN**

Proceso	Indicador	Métricas
Gestión de Talento Humano	Acceso por personal no autorizado al sistema de gestión de nomina	**1.** Numero de accesos en el mes por personal no autorizado **2.** Número de veces de pérdida de integridad de la información

Tiempo: Meses
Exposición: Número entero

Cálculo M1: Numero de accesos en el mes por personal no autorizado
Cálculo M2: Número de veces de pérdida de integridad de la información

Tiempo	1	2	3	4	5	6	7	8	9	10	11	12
Exposición M1	2	0	1	0	0	2	0	0	1	1	0	2
Exposición M2	0	0	0	0	0	0	0	0	0	0	0	1



ANALISIS DE RESULTADOS: Se observa accesos por personas no autorizadas en la mayoría de los meses, y una pérdida de integridad de información, estando las sub-causas relacionadas con la gestión de accesos: 1. falta de definición de límites de tiempo para los derechos de acceso a usuarios con vinculación a término fijo. 2. no se cancelaron los derechos de acceso a usuarios que se desvincularon o sufrieron la pérdida/robo de credenciales

PLAN DE ACCIÓN: ***Establecer Acciones de Mejora***

Sub-Causa 1: Incluir dentro de la base de datos de usuarios restricciones de tiempo para todos los usuarios, personal con vinculación a término fijo la fecha de terminación del contrato y los de termino indefinido al terminar cada vigencia que se actualice automáticamente una nueva vigencia si no existen novedades

Sub-Causa 2: Informar al administrador del sistema las novedades de desvinculación, perdida/robo de credenciales para la cancelación de derechos.

Gestión de Riesgos y Controles

Ejemplos

Ejemplo 3 **FISCAL**

Proceso: Gestión Administrativa

Objetivo: Administrar y mantener los bienes de la Universidad para lograr la conformidad con los requisitos de los servicios prestados.

Alcance: Inicia con la identificación de necesidades de servicios que garanticen el normal funcionamiento de la institución, incluyendo la administración de los recursos físicos y termina con el suministro y entrega de los bienes y/o servicios requeridos.

Riesgo =

- **¿Qué?** Impacto
- **¿Cómo?** Causa Inmediata
- **¿Por qué?** Causa Raíz
  - Sub-causa 1
  - Sub-causa 2

Lo que puede ocurrir

Posibilidad de

- Efecto dañoso sobre bien(es) público(s)
- Por pérdida, extravío, hurto, robo o declaratoria de bien faltante
- A causa de la omisión en la aplicación de políticas de ingreso, permanencia y salida de bienes

Control
CORRECTIVO
Se prepara para Atacar al materializarse el Riesgo

Control =

- Respon sable: El responsable del Grupo de Compras
- Acción: Verifica la vigencia y actualización de la póliza de acuerdo con los bienes que ingresan
- Comple mento: En caso de presentarse un siniestro informa a la Oficina Jurídica para que adelante las reclamaciones respectivas ante la compañía aseguradora

CORRECTIVO
Manual

Gestión de Riesgos y Controles

Ejemplos

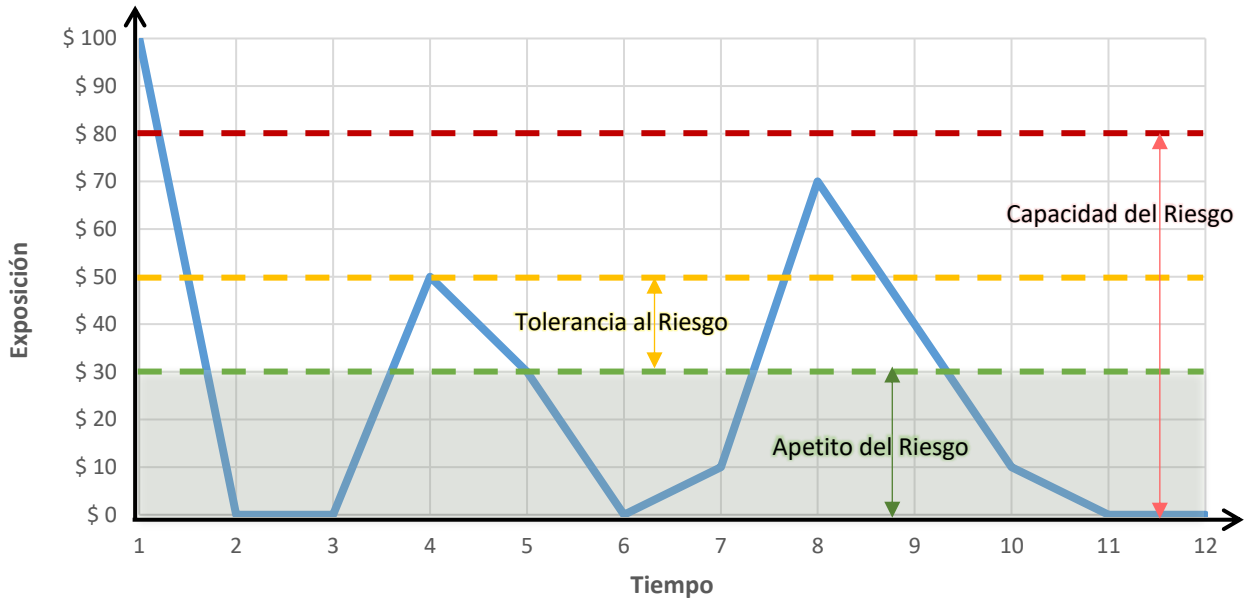
Ejemplo 3 **FISCAL**

Proceso	Indicador	Métricas
Gestión Administrativa	Siniestros por omisión en el ingreso, permanencia y salidas de bienes	1. % de siniestros presentados en el mes 2. Valor en pesos de los bienes siniestrados en el mes

Tiempo: Meses
Exposición: Pesos (Millones)

Cálculo M2: Valor en pesos de los bienes siniestrados en el mes

Tiempo	1	2	3	4	5	6	7	8	9	10	11	12
Exposición M2	$100	$0	$0	$50	$30	$0	$10	$70	$40	$10	$0	$0



ANALISIS DE RESULTADOS: Se presenta valor de bienes siniestrados por fuera de la capacidad del riesgo, determinándose que las sub-causas de la causa raíz, que producen estos resultados: 1. falencias en el registro y control de préstamo y traslado de bienes AD-F26. 2. falencias en la actualización del inventario dado cambios en la custodia y/o ubicación del bien.

PLAN DE ACCIÓN: ***Establecer Acciones de monitoreo y Controles preventivos***
Causa 1: Implementar aplicativo que registre y documente diariamente cada etapa de la administración del bien: entrada, permanencia (entrega, préstamo, traslado, etc.), y salida. Por respectivos usuarios según roles.
Causa2: Establecer para el aplicativo responsable de control y validación de la documentación en cada etapa que permita la actualización y ubicación del inventario

Gestión de Riesgos y Controles

Ejemplos

Ejemplo 4 **DE CORRUPCIÓN**

Proceso: Gestión de Contratación

Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Alcance: inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisiciones) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas

Riesgo = Impacto (**¿Qué?**) + Causa Inmediata (**¿Cómo?**) + Causa Raíz (**¿Por qué?**) → Sub-causa 1, Sub-causa 2

Lo que puede ocurrir

Posibilidad de

- Afectación económica y reputacional
- Por condenas o sanciones de entes de control
- Debido al recibimiento de beneficio privado para la celebración de contratos sin el cumplimiento de requerimientos normativos

Control
PREVENTIVO
Ataca causa Raíz, identificando las sub-causas

Control = Respon sable + Acción + Comple mento

PREVENTIVO
Manual

- Evaluadores designados por el Ordenador de Gasto
- Verifica que la documentación suministrada por el proveedor cumpla con los requerimientos establecidos por tipo de contratación
- A través del CO-F33 Listado de documentos contractuales y lo deja registrado en el CO-F06 o CO-F07 Acta de Evaluación de Propuesta. Los resultados los comunica al jurídico de la dependencia Ordenadora

Gestión de Riesgos y Controles

Ejemplos

Ejemplo 4 **DE CORRUPCIÓN**

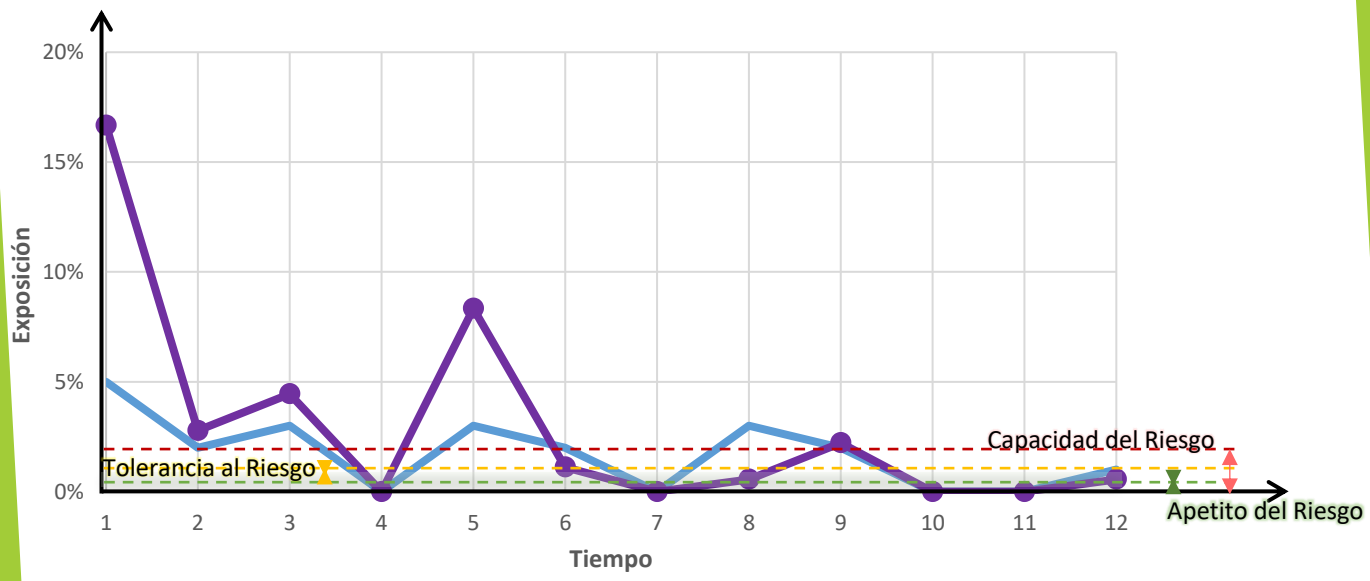
Proceso	Indicador	Métricas
Gestión de Contratación	Contratos celebrados sin el cumplimiento de requisitos	1. % de contratos celebrados en el mes sin el cumplimiento de requisitos. 2. % del valor de contratos celebrados en el mes sin cumplimiento de requisitos.

Tiempo: Meses **Exposición:** %

Cálculo M1: Contratos celebrados en el mes sin el cumplimiento de requisitos / Contratos celebrados en el mes

Cálculo M2: Valor contratos celebrados en el mes sin cumplimiento de requisitos / Valor de contratos celebrados en el mes

Tiempo	1	2	3	4	5	6	7	8	9	10	11	12
Exposición M1	5%	2%	3%	0%	3%	2%	0%	3%	2%	0%	0%	1%
Exposición M2	16,7%	2,8%	4,4%	0,0%	8,3%	1,1%	0,0%	0,6%	2,2%	0,0%	0,0%	0,6%



ANALISIS DE RESULTADOS: Se presenta % de adquisición de bienes-servicios fuera de la capacidad del riesgo, determinándose que las sub-causas, que producen estos resultados: 1. falencias en las *solicitudes de propuestas*, debido a que por acción u omisión no se tienen en cuenta los requerimientos establecidos por tipo de contrato (CO-F33). 2. Por acción u omisión no se está ejecutando correctamente el control establecido.

PLAN DE ACCIÓN: ***Establecer Acciones de Monitoreo y Reforzar el Control Preventivo***

Causa 1: * El jurídico de la dependencia Ordenadora verifica la información registrada por evaluadores, si conforme da visto bueno para firma del ordenador del gasto, en caso contrario devuelve.

* Líder de proceso capacita a personal que solicita propuestas en CO-F33

Causa 2: Establecer periodos y responsables de seguimiento a la ejecución del control preventivo.