BOLETÌN N.002

IMPORTANCIA DE LOS RIESGOS (GESTIÒN, CORRUPCIÒN Y TIC)

GOBERNACIÓN DEL HUILA
Luis Enrique Dussán López
GOBERNADOR

HUILA CRECE

INDERHUILA

RIESGO CORRUPCIÒN

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 N° 167 de 2013).

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.RIESGO CORRUPCIÒN

Los riesgos de corrupción se establecen sobre procesos.

RIESGOS DE CORRUPCIÒN

GESTIÒN RIESGOS DE CORRUPCIÒN

Seguimiento: ***E***l jefe de control interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción, es necesario adelantar seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

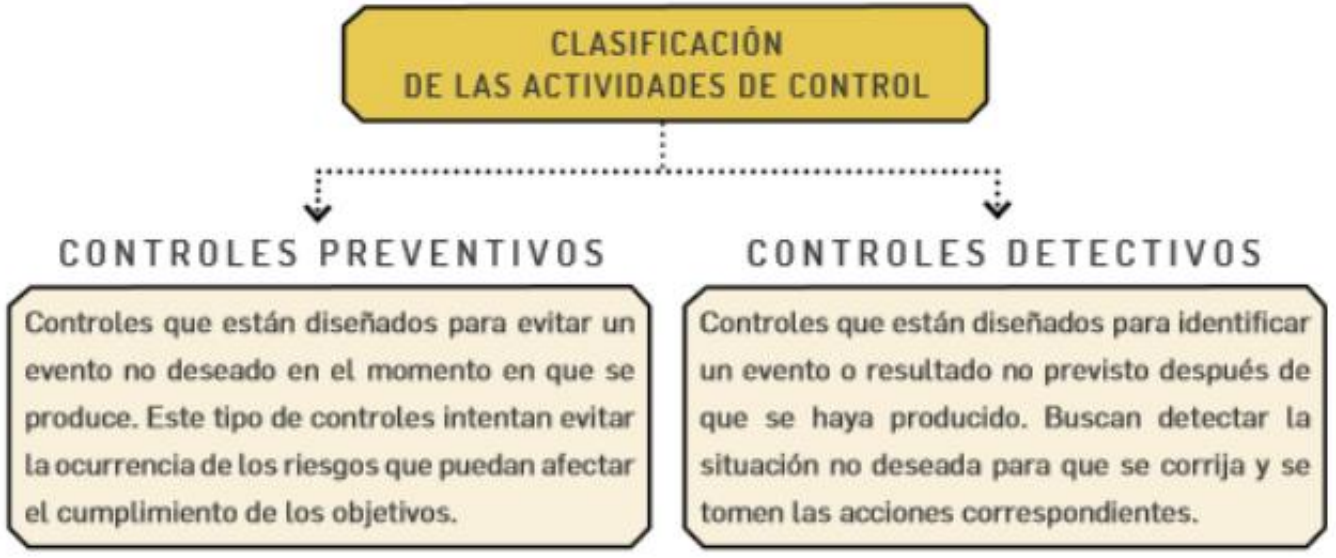
Primer seguimiento:
Corte al 30 de abril. La publicación deberá sustituirse dentro de los diez (10) primeros días del mes de mayo.

Segundo seguimiento:
Core al 31 de agosto. La publicación deberá sustituirse dentro de los diez (10) días del mes de septiembre.

Tercer seguimiento:
Corte 31 de diciembre. La publicación deberá sustituirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la oficina de Control Interno deberá ser publicado en la página web de la entidad o en un lugar fácil acceso para el ciudadano.

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de actividades de control.



(Fuente DAFP)

RIESGO SEGURIDAD DE LA INFORMACIÒN

Se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI) 3 , el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Riesgos que se encuentran

-Pérdida de la confidencialidad
-Pérdida de la integridad
-Pérdida de la disponibilidad

RIESGOS DE SEGURIDAD DE LA INFORMACIÒN

CONTROLES → Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.
Copias de respaldo	Objetivo: proteger la información contra la perdida de datos.
Respaldo de información	Control: se deberían hacer copias de respaldo de la información, del *software* y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.

RIESGOS DE GESTIÒN-POR PROCESO

-Incertidumbre en los objetivos de una organización.
-Todas las actividades de la organización involucran riesgos que se deberían ***GESTIONAR***

***SE GESTIONAN*:**

- Identificación
- Análisis
- Evaluación
- Modificación por medio del tratamiento de riesgos.

IMPORTANTE

Pregúntese si el riesgo de gestión identificado está relacionado directamente con las características del objetivo. Si la respuesta es "no", este puede ser la causa o la consecuencia.

IMPORTANCIA

- Aumenta la probabilidad de alcanzar los objetivos.
- Ser consiente de la necesidad de identificar y tratar todos los riesgos en toda la organización.
- Cumplir con los requisitos legales aplicables .
- Mejora la honestidad y confianza de las partes interesadas .
- Base confiable para la toma de decisiones y planificación.
- Mejorar controles existentes.
- Mejora la prevención de perdidas (minimiza las perdidas).

TIPOS DE RIESGOS

RIESGOS ESTRATÉGICOS

- Forma en la que se administra la empresa
- Se enfoca asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos.

RIESGOS DE IMAGEN

- Percepción y confianza por parte de la ciudadanía hacia la organización.

RIESGOS OPERATIVOS

- Percepción y confianza por parte de la ciudadania hacia la organización.

RIESGOS FINANCIEROS

- Manejo de los recursos de la empresa que incluyen : la ejecución presupuestal, la elaboración de estados financieros

RIESGOS DE CUMPLIMIENTO

- Capacidad de la empresa para cumplir con los requisitos legales, contractuales, de ética.

RIESGOS DE TECNOLOGÍA

- Capacidad tecnológica de la empresa para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión

INDERHUILA

GOBERNACIÓN DEL HUILA
Luis Enrique Dussán López

HUILA CRECE

Tabla 3. Criterios para calificar el impacto – riesgos de gestión

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.