ANEXO N°1 METODOLOGÍA ESTABLECIDA PARA LA VALORACIÓN DE RIESGOS Y CONTROLES

UNIVERSIDAD DE LOS ANDES

1.1. Metodología establecida para la valoración de riesgos y controles

La Universidad establece y determina los elementos centrales necesarios, para que el Sistema de Gestión de Riesgos se desarrolle de la manera esperada, cumpliendo con la normatividad en conjunto con la aplicación de mejores prácticas en gestión de riesgos, como se muestra a continuación.

1.1.1. Definición del riesgo

Evento que afecta el cumplimiento de los objetivos Institucionales.

1.1.1.1. Naturaleza del riesgo

Siguiendo lo establecido en el Marco COSO los riesgos pueden clasificarse en estratégicos, operacionales, reporte y cumplimiento, estas categorías permiten cubrir las actividades y objetivos principales del proceso, asegurando que todos los riesgos significativos son identificados.

Gráfica 1. Naturaleza del riesgo.

1.1.2. Análisis y evaluación del riesgo

La Matriz de evaluación de riesgos es una herramienta para la valoración cualitativa y cuantitativa de los riesgos frente a los impactos o amenazas a personas, reputación, legales, financieros y de procesos de la Universidad y la frecuencia con que estos riesgos pudiesen materializarse.

Evaluación de impacto

La Institución determino las siguientes categorías de impactos potenciales "Reputacional (R), Contingencia Legal (CL), Afectación Financiera (AF), Procesos Operativos (PO) Seguridad en las personas (SP)". Para determinar el nivel de impacto se utiliza una escala de "1" a "5", siendo 5 la calificación de mayor impacto.

Los incidentes pueden tener consecuencias en las cinco categorías de impacto, por lo tanto, para una evaluación o clasificación, deben examinarse todas las categorías y relacionar a la que mayor impacto genere.

Ejemplo: para un caso en el que se encuentre que el riesgo aplica a diferentes categorías de impacto, como:

- Reputacional nivel 5 – Muy alto
- Contingencia legal 2 – Bajo
- Afectación financiera 3 – Medio
- Procesos operativos 1 – Insignificante

El riesgo de este incidente será Reputacional 5 – Muy alto.

Evaluación de la probabilidad

Para evaluar la probabilidad se estableció una escala remota, poco probable, posible, probable o con certeza, basándose en la experiencia o evidencia histórica en que las consecuencias identificadas se han materializado dentro de la Institución; representa la probabilidad de que se desencadenen los impactos potenciales, reales o estimados, según el caso.

La estimación de la probabilidad se basa en información potencial o expectativas a futuro que se tengan del riesgo, información histórica o información expresada en términos porcentuales respecto de casos ocurridos anteriormente en similares condiciones, sabiendo que las circunstancias nunca son exactamente las mismas. El cruce de las dos escalas determina la evaluación y clasificación del riesgo inherente.

Aplicación de la matriz de evaluación de riesgos

Los procesos que realiza la Universidad requieren de una evaluación y clasificación ágil de los riesgos, para ello, se ha adoptado un mecanismo sencillo y fácil de usar, lo cual permite a los dueños de los procesos evaluar sus riesgos con base en la probabilidad e impacto, así:

- Impacto: Se refiere a los efectos sobre la Universidad; lo que podría perder, salir mal o lo que podría estar dejando de ganar.

IMPACTO					
Seguridad en las personas	**Afectación de procesos**	**Afectación financiera**	**Contingencias legales**	**Reputacional**	
Muerte, por accidente o enfermedades profesionales	Fallas operativas, que generan Interrupción de 1 o mas procesos mayor a 5 días.	Afectaciones financieras mayores a $ 9.465.000.000	Intervención por parte de un ente regulador o de control, que conlleve al cierre temporal o definitivo de la operación de la Universidad.	• Presión negativa en medios de comunicación, no controlada y por largo periodo de tiempo. • Destrucción del buen nombre de la Institución.	Muy alta (5)
• Incapacidad permanente que afecta el desempeño laboral por largo tiempo, generando ausencia prolongada en el trabajo. • Daños irreversibles en la salud con inhabilitación seria, sin pérdida de	Fallas operativas, generando interrupción de 1 o mas procesos entre 3 y 5 días	Afectaciones financieras entre $ 6.058.001.000 y $ 9.465.000.000	Sanciones fiscales o penales a la Institución, por parte de un ente regulador o de control.	• El buen nombre de la Institución está comprometido. • Hechos o situaciones adversos significativos en medios influyentes por varios días.	Alta (4)
• Accidente mayor sin incapacidad permanente, afecta el desempeño laboral por largo tiempo, generando ausencia prolongada en el trabajo. • No limita su capacidad para reincorporarse a sus labores diarias dentro de la institución luego de su	Fallas operativas, generando interrupción de 1 o mas procesos entre 1 y 2 días	Afectaciones financieras entre $1.136.001.000 y $ 6.058.000.000.	Demandas a la Institución por agentes externos o internos	• El buen nombre de la Institución podría verse afectado. • Hechos o situaciones adversos puntuales en medios masivos.	Media (3)
• Lesión leve o accidente menor, que requiere atención médica. • Genera una posible incapacidad no mayor a 5 día • No afecta el rendimiento laboral.	Fallas operativas, generando interrupción de 2 o mas procesos menor a 1 día	Afectaciones financieras entre $ 252.001.000 y $1.136.000.000.	Quejas o reclamos que puedan derivar en multas o sanciones por un ente regulador o de control.	• La percepción de los grupos de interés, probablemente no tendrá un efecto duradero. • No hay visibilidad en medios.	Baja (2)
• Incidente o suceso que no produce lesiones personales, por lo cual no requiere atención médica. • Requiere medidas de prevención para que no ocurra un accidente por las mismas causas.	Fallas operativas, generando interrupción de 1 proceso menor a 1 día	Afectaciones financieras menores a $252 millones	No se generan investigaciones ni sanciones.	No hay visibilidad en medios.	Insignificante (1)

Gráfica 3. Escala de Impacto.

- Probabilidad: Frecuencia con la que se podría materializar un riesgo latente o potencial en un periodo determinado.

	PROBABILIDAD				
Potencial	Casi imposible que ocurra el próximo año	Poco probable que ocurra el próximo año	Es posible que ocurra el próximo año	Bastante probable que ocurra el próximo año	Ocurrirá, con alto nivel de certeza, el próximo año
Histórico	Ha ocurrido en el sector educativo (no en la Institución)	Ha ocurrido en los últimos 8 años en la Institución	Ha ocurrido en los últimos 4 años en la Institución	Ha ocurrido en el ultimo año en la Institución	Ha ocurrido mas de una vez en el ultimo año
Numérico	< 1%	1% - 25%	25% - 50%	50% - 75%	> 75%
	Remota (1)	**Poco probable (2)**	**Posible (3)**	**Probable (4)**	**Con Certeza (5)**

$$\text{Probabilidad} = \frac{Numero\ de\ casos\ curridos\ (materializados)}{Numero\ de\ casos\ posibles\ (total\ población)}$$

Gráfica 2. Escala de probabilidad.

Riesgo inherente. Es el riesgo que se presenta tal y como se encuentra la operación. El riesgo inherente es propio del trabajo o proceso, que no puede ser eliminado del sistema; es decir, en todo trabajo o proceso se encontrarán riesgos para las personas o para la ejecución de la actividad en sí misma.
Una vez evaluado el riesgo inherente, se debe evaluar la solidez de los controles que se identificaron para la mitigación del riesgo, de esta forma podemos determinar el riesgo residual.

Riesgo residual. Es aquel riesgo que subsiste, después de haber implementado y probado los controles. Es importante advertir que el nivel de riesgo al que está expuesta la Universidad, nunca puede erradicarse totalmente. Por ello, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar estos riesgos a un cierto nivel de confianza que se puede considerar suficiente (nivel de

riesgo aceptable). El riesgo residual puede verse como aquello que separa a la Institución de la seguridad absoluta

Gráfica 4. Relación riesgo inherente y riesgo residual.

Mapa de calor

Es una herramienta que identifica las actividades o procesos sujetos a riesgo, cuantificando la probabilidad de que los eventos sucedan y mide el daño potencial en caso de que dicho riesgo se pueda materializar. Ayuda a tener un mayor conocimiento del entorno de trabajo, las líneas de actuación e incrementa la seguridad, mejorando la eficiencia, eficacia y efectividad de los procesos

IMPACTO					PROBABILIDAD				
					Casi imposible que ocurra el próximo año	Poco probable que ocurra el próximo año	Es posible que ocurra el próximo año	Bastante probable que ocurra el próximo año	Ocurrirá, con alto nivel de certeza, el próximo año
					Ha ocurrido en el sector educativo (no en la Institución)	Ha ocurrido en los últimos 8 años en la Institución	Ha ocurrido en los últimos 4 años en la Institución	Ha ocurrido en el ultimo año en la Institución	Ha ocurrido mas de una vez en el ultimo año
					< 1%	1% - 25%	25% - 50%	50% - 75%	> 75%
Seguridad en las personas	Afectación de procesos	Afectación financiera	Contingencias legales	Reputacional		Remota (1)	Poco probable (2)	Posible (3)	Probable (4)	Con Certeza (5)
Muerte, por accidente o enfermedades profesionales	Fallas operativas, que generan Interrupción de 1 o mas procesos mayor a 5 días.	Afectaciones financieras mayores a $ 9.465.000.000	Intervención por parte de un ente regulador o de control, que conlleve al cierre temporal o definitivo de la operación de la Universidad.	• Presión negativa en medios de comunicación, no controlada y por largo periodo de tiempo. • Destrucción del buen nombre de la Institución.	Muy alta (5)	Moderado (5)	Alto (10)	Alto (15)	Extremo (20)	Extremo (25)
• Incapacidad permanente que afecta el desempeño laboral por largo tiempo, generando ausencia prolongada en el trabajo. • Daños irreversibles en la salud con inhabilitación seria, sin pérdida de	Fallas operativas, generando interrupción de 1 o mas procesos entre 3 y 5 días	Afectaciones financieras entre $ 6.058.001.000 y $ 9.465.000.000	Sanciones fiscales o penales a la Institución, por parte de un ente regulador o de control.	• El buen nombre de la Institución está comprometido. • Hechos o situaciones adversos significativos en medios influyentes por varios días.	Alta (4)	Moderado (4)	Moderado (8)	Alto (12)	Alto (16)	Extremo (20)
• Accidente mayor sin incapacidad permanente, afecta el desempeño laboral por largo tiempo, generando ausencia prolongada en el trabajo. • No limita su capacidad para reincorporarse a sus labores diarias dentro de la institución luego de su	Fallas operativas, generando interrupción de 1 o mas procesos entre 1 y 2 días	Afectaciones financieras entre $1.136.001.000 y $ 6.058.000.000.	Demandas a la Institución por agentes externos o internos	• El buen nombre de la Institución podría verse afectado. • Hechos o situaciones adversos puntuales en medios masivos.	Media (3)	Bajo (3)	Moderado (6)	Moderado (9)	Alto (12)	Alto (15)
• Lesión leve o accidente menor, que requiere atención médica. • Genera una posible incapacidad no mayor a 5 día • No afecta el rendimiento laboral.	Fallas operativas, generando interrupción de 2 o mas procesos menor a 1 día	Afectaciones financieras entre $ 252.001.000 y $1.136.000.000.	Quejas o reclamos que puedan derivar en multas o sanciones por un ente regulador o de control.	• La percepción de los grupos de interés, probablemente no tendrá un efecto duradero. • No hay visibilidad en medios.	Baja (2)	Bajo (2)	Moderado (4)	Moderado (6)	Moderado (8)	Alto (10)
• Incidente o suceso que no produce lesiones personales, por lo cual no requiere atención médica. • Requiere medidas de prevención para que no ocurra un accidente por las mismas causas.	Fallas operativas, generando interrupción de 1 proceso menor a 1 día	Afectaciones financieras menores a $252 millones	No se generan investigaciones ni sanciones.	No hay visibilidad en medios.	Insignificante (1)	Bajo (1)	Bajo (2)	Bajo (3)	Moderado (4)	Moderado (5)

Gráfica 5. Mapa de calor Institucional.

Respuesta al riesgo

Con base en la ponderación obtenida del riesgo inherente para los diferentes riesgos asociados al proceso, se debe realizar una evaluación y dar respuesta a cada riesgo, lo cual permite realizar una priorización de los mismos, esta priorización debe ser definida y justificada por los diferentes dueños de los procesos. Para ello se hace preciso analizar los siguientes aspectos:

- **Contexto:** Las respuestas a los riesgos se deben adaptar al contexto en el que se opere (interno y externo).
- **Costo-beneficio:** Se debe evaluar si la implementación o mantenimiento de un control en cuanto a costos, tiempo, personal, es más grande que los beneficios que pueda ofrecer.
- **Obligaciones y expectativas:** La respuesta al riesgo deben ser coherente con los estándares generalmente aceptados, las expectativas de las partes interesadas y la alineación con la misión y visión Institucional.
- **Apetito de riesgo:** La respuesta al riesgo debe alinearse al apetito de riesgo Institucional, procurando no sobrepasarlo.
- **Gravedad o impacto del riesgo:** La respuesta al riesgo debe reflejar el tamaño, alcance, naturaleza e impacto del riesgo en la institución.
- **Priorización del riesgo:** La priorización del riesgo dependerá del análisis de factores como (nivel de riesgo inherente, impacto asociados a la materialización del riesgo y costos de implementación).

Una vez identificados los riesgos y debidamente priorizados, el dueño del proceso debe seleccionar la respuesta adecuada a los mismos, las cuales se encuentran dentro de las siguientes categorías:

Gráfica 6. Respuesta al riesgo.

1.1.3. Actividades de control

Las actividades de control son relevantes en la gestión de riesgos, ya que aseguran que las diferentes causas o fuentes de riesgos están siendo gestionadas por los diferentes líderes de los procesos académicos y administrativos de la Institución, por otra parte, permite que las respuestas a los riesgos sean ejecutadas, de forma apropiada y oportuna. Las actividades de control se llevan a cabo en todos los niveles de la Institución y en las distintas etapas de cada uno de los procesos.

Definición de control

Son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la Alta Dirección para mitigar los riesgos con impacto potencial en los objetivos.

Generalidades

Para la identificación y gestión adecuada de los controles es necesario el establecimiento y aplicación de los aspectos descritos en la siguiente gráfica, que a su vez son indispensables para el diligenciamiento de la matriz de riesgos

Gráfica 7. Generalidades de un control.

1. Definir frecuencia o periodicidad del control

La frecuencia del control permite determinar cada cuanto se ejecuta el mismo, por ende, el dueño del control debe establecer que la periodicidad del control sea la adecuada para cumplir con el objetivo del proceso y evitar la materialización del riesgo. Las periodicidades establecidas para un control son:

- Por evento/ dada vez que se presente
- Diario
- Semanal
- Quincenal
- Mensual
- Bimestral
- Trimestral
- Semestral
- Anual

2. **Definir responsable de su ejecución, revisión y aprobación, describir los pasos detallados en cada rol**

La Universidad establece como responsable de un control aquella persona que realiza las actividades de creación, registro, actualización o eliminación en la ejecución del control, y establece al supervisor del control, como el responsable de realizar las actividades de revisión y aseguramiento del cumplimiento de las actividades de control. Adicionalmente, estos roles deben asegurar la idoneidad y objetividad en la operación de sus actividades.

Es importante mencionar los pasos detallados que se realizan para la ejecución del control, tanto del ejecutor como del revisor, adicional se debe especificar la evidencia física o electrónica que se deja en cada actividad de control, por ejemplo: correo electrónico, documento físico (factura, contrato, documento equivalente), transacciones o aprobaciones en el sistema de información, conciliaciones, confirmaciones, entre otros.

3. **Evidencia de documentación soporte o respaldo tecnológico en la ejecución del control.**

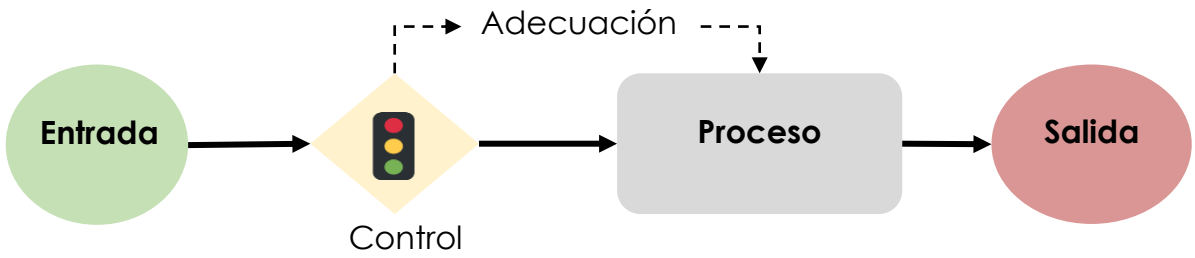
Debido a que es posible la utilización de uno o más sistemas de información al momento de ejecutar un control, es necesario indicar en la redacción del mismo, todos los sistemas de información utilizados, ya sea de gestión, ERP, Bases de Datos, etc.

4. **Asociar tipo de control (preventivo, detectivo, correctivo)**

La clave para la optimización de los procesos y lograr la efectividad y eficiencia de los controles, está en conocer los diferentes tipos de control para poder implementarlos dependiendo del proceso a gestionar, el intervalo de tiempo en el que actuará y su integración con otros controles. Con base en lo anterior, se establecen los siguientes tipos de control:

Preventivos

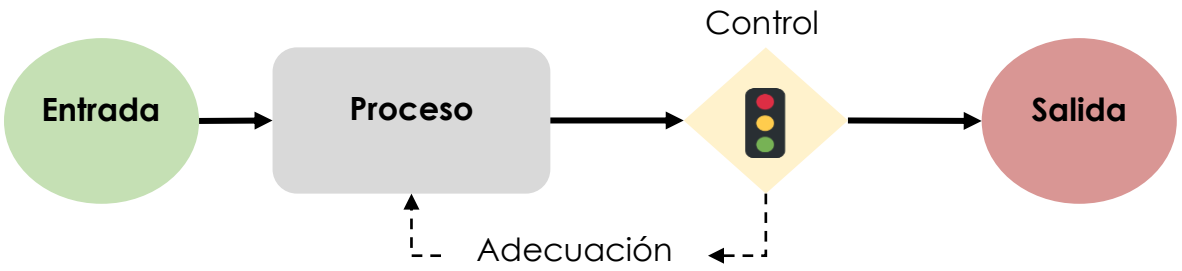
Anticipan eventos no deseados antes de que sucedan, son más rentables, deben quedar incorporados en los sistemas.



Gráfica 8. Controles Preventivos.

Detectivos

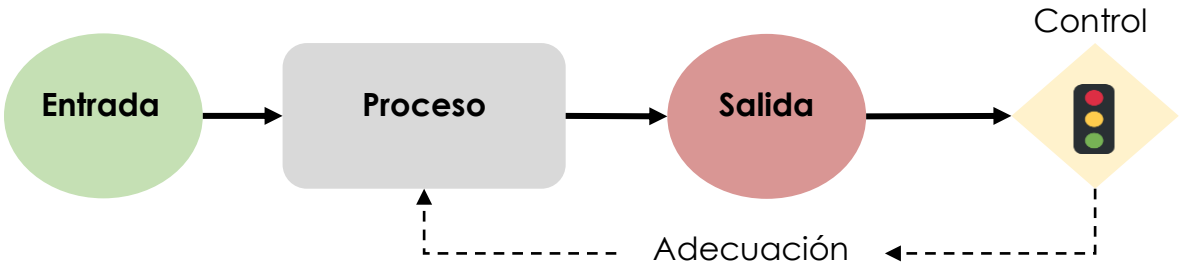
Identifican los eventos en el momento en que se presentan o finalizando el proceso, son más costosos que los preventivos.



Gráfica 9. Controles Detectivos.

Correctivos

Se toman acciones para revertir o remediar un evento no deseado, una vez a finalizado el proceso o se ha establecido el producto final.

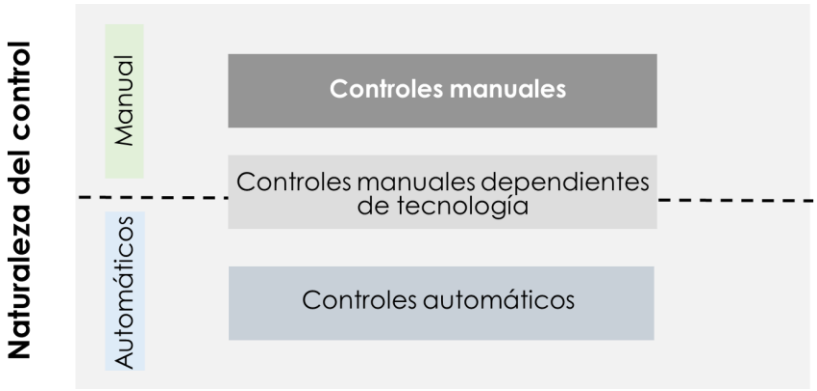


Gráfica 10. Controles Correctivos.

5. Definir la naturaleza del control.

La naturaleza del control (manuales, manuales dependientes de tecnología, automáticos), permite fortalecer el Sistema de Control Interno de cada uno de los procesos Institucionales, en la medida que se puedan implementar controles automáticos o manuales dependientes de tecnología.

La ventaja de un control automático, es que si se cumplen determinadas condiciones en los Controles Generales del Ambiente de Computo (ITGC), podemos garantizar que el control será efectivo en cualquier momento, ya que no dependemos del factor humano para su realización. Estos controles automáticos complementan a los controles manuales que se pueden definir en los diferentes procesos Institucionales.



Gráfica 11. Naturaleza de los controles.

6. Mencionar normativa aplicable

Es importante relacionar la normatividad interna establecida en las políticas, directrices, lineamientos y procedimientos, o la normativa externa establecida en leyes, decretos o resoluciones, que se deben cumplir para la ejecución del control.

7. Definición de control en procedimientos.

Todos los controles propios de cada unidad, deben estar definidos y documentados claramente en sus políticas, directrices, lineamientos o procedimientos internos.

Con la estructuración de los pasos anteriores, definimos el resumen, descripción y actividades de control, las cuales se deben describir de la siguiente forma:

Resumen del control:

Corresponde al objetivo del control y se define de forma breve la periodicidad, responsable y la actividad principal para la ejecución del control. El resumen del control permite a cualquier usuario entender de forma rápida la generalidad del control.

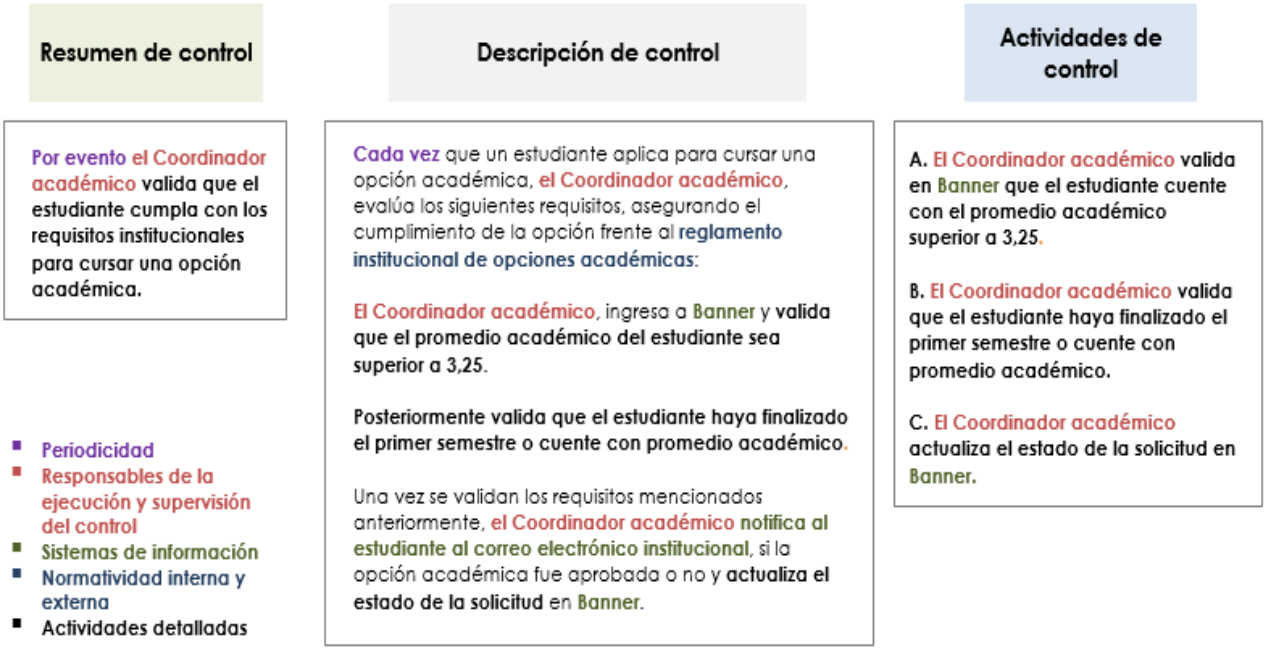
Descripción del control:

La descripción del control está compuesta por todas las actividades mencionadas en la ilustración 14, que se deben realizar para dar cumplimiento al control: definir periodicidad, establecer responsables de la ejecución y supervisión del control, identificar los sistemas de información aplicables, mencionar la normatividad interna y externa e indicar las actividades detalladas con su respectiva evidencia.

Actividades de control:

Son las actividades principales que desprenden de la descripción del control, estas actividades deben contar con un responsable y evidencia física o electrónica para que puedan ser evaluadas correctamente.

Ejemplo redacción del resumen, descripción y actividades de control:



Gráfica 12. Ejemplo Resumen, Descripción y Actividades de control