

**METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE
TECNOLOGÍAS DE INFORMACIÓN
(VERSIÓN 1.0)**

**CENTRO DE INFORMÁTICA
UNIVERSIDAD DE COSTA RICA**

JUNIO 2016



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 2 de 18



1. OBJETIVO

Establecer un proceso aplicable a la Administración de Riesgos de Tecnologías de Información y Comunicaciones.

2. ALCANCE

Aplica para la Gestión de Riesgos de tecnologías de información y Comunicaciones.

3. RESPONSABILIDADES

Es responsabilidad de cada unidad que gestiona tecnologías en la Universidad de Costa Rica, la aplicación de una metodología de análisis y gestión de riesgos, identificando los riesgos potenciales, los planes de acción y contingencia para los mismos.

La Unidad de Gestión de Riesgos y Seguridad del Centro de Informática, presenta y actualiza ésta metodología de riesgos, propuesta para dicha gestión.

4. DOCUMENTOS RELACIONADOS Y REFERENCIAS

4.1 Modelo de Análisis de Riesgo de Tecnologías de Información (TI) en la Universidad de Costa Rica. Agosto 2011.

4.2 Formulario de Tratamientos y Planes de Acción. Enero 2013.

4.3 Directrices Técnicas de Seguridad de la Información.

5. DEFINICIONES

Administración de riesgo: Proceso donde se identifican, miden, se da monitoreo y seguimiento, y controlan los riesgos (de mercado, operativos o de tecnología de información) a los que se está expuesto.

Administración de riesgo de Tecnologías de Información: proceso de identificación de vulnerabilidades y amenazas a los recursos de información utilizados por la organización, para determinar controles que de ser aplicados reducen el riesgo a un nivel aceptable.

Actividades de control o Controles: Están constituidas por prácticas, políticas, estándares o procedimientos orientados a prevenir o minimizar los riesgos.

Análisis de riesgo: Es el estudio de las causas de las posibles amenazas y probables eventos no deseados, los daños y consecuencias que éstas puedan producir, a partir de la probabilidad y la consecuencia de los eventos identificados.



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 3 de 18



Análisis cualitativo: Valoración descriptiva, para definir la magnitud de las consecuencias potenciales de la materialización de un riesgo y la frecuencia de la probabilidad, con que el nivel de riesgo asociado pudiese presentarse.

Análisis cuantitativo. Valoración numérica, para definir la magnitud de las consecuencias potenciales de la materialización de un riesgo y la frecuencia de la probabilidad, con que el nivel de riesgo asociado pudiese presentarse.

Categorías de riesgo: Agrupación de los diferentes riesgos identificados utilizando un criterio calificador, según sean los daños que pueden provocar su materialización.

Comunicación de riesgo: Etapa del proceso de valoración del riesgo que consiste en la preparación, la distribución y la actualización de información oportuna sobre los riesgos a los sujetos interesados.

Consecuencia: Conjunto de efectos derivados de la ocurrencia de un evento expresado cualitativa o cuantitativamente, sean pérdidas, perjuicios, desventajas o ganancias.

Evaluación de riesgo: Es uno de los pasos que se utiliza en el proceso de administración de riesgos, el cual consiste en la definición de mecanismos de análisis para evaluar el riesgo conforme a los parámetros que lo determinan, la magnitud de la pérdida o daño posible y la probabilidad que dicha pérdida o daño llegue a ocurrir.

Evaluación riesgo absoluto: Análisis de la probabilidad que tiene un sujeto de sufrir un evento a lo largo de cierto tiempo.

Evaluación riesgo controlado: Análisis que persigue como objetivo determinar si el ambiente de control con que cuenta actualmente la TI, permite minimizar la consecuencia y la probabilidad detectadas a través de la evaluación del riesgo absoluto.

Evaluación riesgo tratado: Análisis que persigue como objetivo determinar si una vez concluidas las acciones propuestas para la administración del riesgo, se ha logrado minimizar, a los niveles propuestos, la consecuencia y la probabilidad detectadas a través de la evaluación del riesgo controlado.

Evitar el riesgo: Acción o acciones, que al no ejecutarse las actividades propuestas, pueden materializar riesgos.

Factor de riesgo: Calificador para los riesgos, a través del cual sea posible agrupar éstos, según sean las fuentes u originadores que provocan que el riesgo se materialice.

Identificación de riesgo: Es uno de los pasos que se utiliza en el proceso de administración de riesgos, que consiste en la determinación y la descripción de los



eventos, de índole interno y externo, que pueden afectar de manera significativa el cumplimiento de los objetivos de la Administración.

Medida para la administración de riesgos o tratamiento: Disposición razonada que permite modificar, transferir, prevenir, atender o retener riesgos.

Nivel de riesgo o exposición del riesgo: Grado de exposición al riesgo, que se determina a partir del análisis de la probabilidad de ocurrencia del evento y de la magnitud de su consecuencia potencial, sobre el cumplimiento de los objetivos fijados. Permite establecer la importancia relativa del riesgo.

Nivel de riesgo aceptable: Nivel de riesgo que se está dispuesto y en capacidad de retener, para cumplir con los objetivos, sin incurrir en costos ni efectos adversos ni excesivos, relacionado con los beneficios esperados o incompatibles con las expectativas de los sujetos interesados.

Normativa estándar: Australiano Administración de Riesgos (AS/NZS 4360:1999) Estándar que provee una guía para el establecimiento e implementación del proceso de administración de riesgos.

Normativa ISO 27000. Es un conjunto de estándares desarrollados por ISO(International Organization for Standardization) e IEC(International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Normativa ISO 27001. Contiene los requisitos del sistema de gestión de seguridad de la información.

Normativa ISO 27005. Establece las directrices para la gestión del riesgo en la seguridad de la información.

Normativa ISO 31000. La norma ISO 31000:2009 establece una serie de principios que deben ser satisfechos para hacer una gestión eficaz del riesgo. Esta Norma Internacional recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de trabajo o estructura de soporte (framework) cuyo objetivo es integrar el proceso de gestión de riesgos en el gobierno corporativo de la organización, planificación y estrategia, gestión, procesos de información, políticas, valores y cultura.

Normativa COBIT. El estándar Cobit (Control Objectives for Information and related Technology) ofrece un conjunto de “mejores prácticas” para la gestión de los Sistemas de Información de las organizaciones. El objetivo principal es proporcionar una guía de alto nivel sobre puntos en los que se establecen controles internos con tal de: asegurar el buen gobierno, proteger los intereses de los stakeholders (clientes, accionistas, empleados, etc.), garantizar el cumplimiento normativo del sector al que pertenezca la organización, mejorar la eficacia y eficiencia de los



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 5 de 18



procesos y actividades de la organización y garantizar la confidencialidad, integridad y disponibilidad de la información.

Parámetros de aceptabilidad de riesgo: Criterios que permiten determinar si un nivel de riesgo específico se ubica o no dentro de la categoría de nivel de riesgo aceptable.

Probabilidad de un riesgo: Medida o descripción de la posibilidad de la ocurrencia de un evento.

Reducir Consecuencia: Definición de medidas de administración de riesgos para minimizar la consecuencia.

Reducir Probabilidad: Definición de medidas de administración de riesgos para minimizar la probabilidad.

Retener riesgos. Opción de administración de riesgos que consiste en la no aplicación de otros tipos de medidas como: atención, modificación, prevención o transferencia; y estar en disposición de enfrentar las eventuales consecuencias.

Riesgo: Evento que en caso de presentarse, tendría efectos sobre el cumplimiento de los objetivos de las tecnologías de Información. Su medición se da en términos de consecuencia y probabilidad.

Riesgo Residual: Nivel de riesgo que se acepta retener.

Sujetos interesados: Personas físicas o jurídicas, internas y externas a la Administración, que pueden afectar o ser afectadas directamente por las decisiones y acciones institucionales.

Transferir Riesgo: Definición de medidas de administración de riesgos, a través de las cuales un tercero asume parte o totalidad de los efectos provocados por la materialización del riesgo.

6. DESCRIPCIÓN DEL PROCESO

El proceso para realizar la identificación, evaluación y tratamientos de riesgos se compone de seis (6) pasos, que se indican a continuación:

- 6.1. Definición del catálogo base de Riesgos y Controles para el proceso, proyecto o actividad a evaluar.
- 6.2. Identificación de Riesgos de TI
- 6.3. Análisis del riesgo absoluto
- 6.4. Evaluación de los controles existentes por riesgo
- 6.5. Evaluación del riesgo controlado
- 6.6. Administración de los riesgos relevantes identificados



6.1 Establecer la Definición del catálogo base de Riesgos y Controles

Para iniciar con el proceso es necesario disponer de un catálogo base o inventario de riesgos. Para elaborar dicho inventario se debe de identificar los riesgos del proceso, proyecto o actividad a valorar y se lista en un catálogo con el fin de aplicar la metodología en los que así se determine necesario.

Cabe señalar que el Centro de Informática dispone de un inventario de riesgos, basado en las mejores prácticas de ISO 27001, y recomendaciones de los dominios de COBIT, el cual puede ser utilizado para tal efecto.

Partiendo del inventario de riesgos, llamado “catálogo de riesgos y controles” a partir de éste momento, se adapta al modelo de riesgos que cubre los aspectos relevantes de gestión y seguridad de TI, en esta metodología.

6.2 Identificación de los Riesgos de TI

Consiste en analizar la posibilidad de ocurrencia de un acto o evento (interno o externo) que podría afectar el cumplimiento de los objetivos definidos en el proceso, proyecto o actividad que se está valorando y de esta manera identificar los riesgos asociados a TI.

6.2.1 Valorar los posibles riesgos de TI

Se deben evaluar los posibles riesgos que podrían presentarse en el proceso, proyecto o actividad y que tienen relación con el uso o aplicación de la tecnología de información, así como analizar los factores de riesgo asociados.

Los factores de riesgo se clasifican de la siguiente manera:

Factor de Riesgo	Descripción del Factor
Relaciones Comerciales	Relación entre la Institución y otras organizaciones o proveedores
Condiciones económicas	Circunstancias económicas a nivel de Institución, país o a nivel mundial
Comportamiento Humano	Actitudes de personas, internas o externas, que interaccionan con la Institución.
Eventos Naturales	Eventos de la naturaleza
Disposiciones de Gobierno	Cambios legislativos y factores similares
Ambiente Legal	Cambios de reglamentación interna y externa en los cuales se desarrolla la Institución
Tecnología , Habilidades o Conocimiento	Conjunto de instrumentos tecnológicos, destrezas o capacidades individuales
Medio ambiente	Actividades que genera la Institución que pueden tener un impacto en la naturaleza, degradar el ambiente o el



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 7 de 18



Factor de Riesgo	Descripción del Factor
Responsabilidad Social	Relación con la Institución con la comunidad o sociedad que se ubica cerca de las áreas de influencia de la Institución, considera aspectos sociales, políticos y económicos.

Posteriormente, se deben identificar y priorizar los riesgos relevantes que pueden afectar de manera significativa, total o parcial, el cumplimiento de los objetivos, determinando para ello el tipo de evento que los genera, ya sea interno o externo.

Para determinar el tipo de evento es importante recordar, que un evento es un "Incidente o situación que podría ocurrir en un lugar específico, en un intervalo de tiempo particular", que el mismo puede ser de índole interno (como eventos relacionados con el funcionamiento de los procesos, proyectos y actividades propias de la Institución) o de índole externo (como eventos relacionados con los cambios que pueden ocurrir en el entorno de la Institución).

Como guía para identificar un riesgo relevante, se pueden considerar los siguientes ítems:

- ¿Qué actividades pueden impedir el logro de los objetivos?
- ¿Qué le sucede al proceso, proyecto o actividad y a los objetivos, si existiera una carencia o bien hace falta presupuesto, personal, etc.?
- Establezca la diferencia entre posibles carencias que podrían ser debilidades de control y no riesgos propiamente.
- ¿Qué le sucede al proceso, proyecto o actividad y a los objetivos, si no se ejecuta ese control?
- Establezca la diferencia entre posibles faltas de ejecución de un control y no riesgos propiamente.

6.3 Análisis del Riesgo Absoluto

Los riesgos identificados alrededor del proceso, proyecto o actividad, deberán ser valorados, en primera instancia bajo un enfoque absoluto; es decir, en un escenario donde no existen controles.

Los criterios para la calificación del riesgo absoluto serán la probabilidad y consecuencia de la ocurrencia del mismo.

El responsable del proceso, proyecto o actividad deberá realizar una auto evaluación de consecuencia y probabilidad absoluta, utilizando los criterios establecidos por la Institución y realizando el producto de dichos factores "consecuencia por probabilidad"



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 8 de 18



para obtener el nivel del riesgo absoluto; es decir, la evaluación de riesgo bajo un escenario que no considera la existencia ni efectividad del ambiente de control.

Para realizar la valoración, es importante tener presente la definición de probabilidad y consecuencia de un riesgo, de esta manera el nivel de riesgo absoluto queda establecido por el grado de exposición al riesgo determinado. Este análisis de la probabilidad de ocurrencia del evento y de la magnitud de su consecuencia, sobre el cumplimiento de los objetivos fijados, no considera la existencia, eficiencia y efectividad del ambiente de control: controles existentes en el proceso, proyecto o actividad.

Los criterios definidos para el análisis y evaluación de la consecuencia y probabilidad de un riesgo son los siguientes:

PROBABILIDAD	ESCALA DE PROBABILIDAD	CONSECUENCIA	ESCALA CONSECUENCIA
CASI CERTEZA	5	CATASTRÓFICO	5
PROBABLE	4	MAYOR	4
POSIBLE	3	MODERADO	3
POCO PROBABLE	2	MENOR	2
RARO	1	IN SIGNIFICANTE	1

Definición de los criterios: Probabilidad

Criterio Cualitativo	Descripción	Criterio Cuantitativo
Casi Certeza	La expectativa de ocurrencia se da con una certeza de casi el 100% de las circunstancias	5
Probable	Probabilidad de ocurrencia en la mayoría de las circunstancias	4
Possible	Ocurre en la mitad de los casos	3
Poco Probable	Puede ocurrir algunas veces	2
Raro	Puede ocurrir solo bajo circunstancias excepcionales	1



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 9 de 18



Definición de los criterios: Consecuencia

Criterio Cualitativo	Descripción	Criterio Cuantitativo
Insignificante	No hay daño, pérdida financiera, de imagen o potenciales problemas operativos o de cumplimiento legal bajos	1
Menor	El primer tratamiento de ayuda o de corrección, se realiza inmediatamente, genera pérdidas financieras o de imagen bajas, los procesos críticos y los compromisos de la Entidad hacia los terceros o internamente no se ven comprometidos.	2
Moderado	Requiere tratamiento o corrección inmediata, en las áreas afectadas, los procesos críticos se pueden ver afectados, se requiere de asistencia para la corrección, se presentan pérdidas financieras medias, de imagen y pueden existir debilidades en los procesos operativos y consecuencias legales.	3
Mayor	Daños mayores, pérdidas de capacidad de operación, no se puede cumplir con los objetivos de una manera razonable (eficaz y eficientemente), la Institución se ve expuesta a pérdidas financieras, operativas, de imagen considerables, efectos legales y de cumplimiento pueden perjudicar a la Institución.	4
Catastrófico	No se puede cumplir con los objetivos Institucionales, el no cumplimiento compromete a la Institución, puede ser sancionada, se pueden dar pérdidas financieras muy altas, pérdida de imagen y no cumplimiento de responsabilidades.	5

De acuerdo a la evaluación anterior, se obtiene el “mapa de calor”, el cual ilustra gráficamente la ubicación de los riesgos con respecto al nivel de impacto y probabilidad:

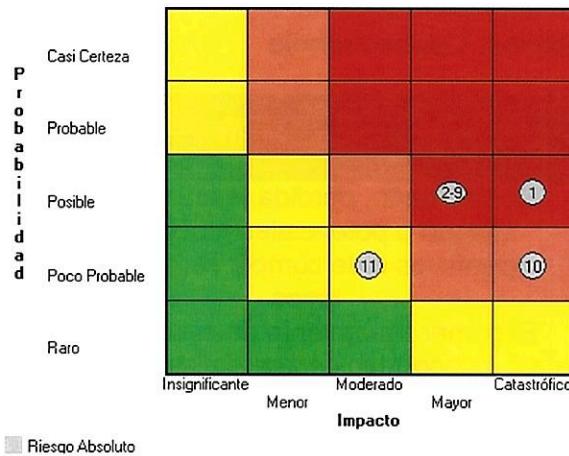


METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 10 de 18



La definición de los niveles de riesgos, se posicionan en los cuadrantes, como se detalla a continuación:

- Nivel de Riesgo Extremo: Cuadrantes Rojos
Los riesgos ubicados en estos cuadrantes, cuentan con altas probabilidades de ocurrencia y consecuencias elevadas para la Administración, en caso de que se materialice, provocando perjuicios extremos en el logro de los objetivos.
- Nivel de Riesgo Alto: Cuadrantes Naranjas:
Estos riesgos cuentan con características de altas probabilidades y consecuencias moderadas o viceversa, su exposición conlleva niveles altos de perjuicio en el logro de los objetivos de la Administración.
- Nivel de Riesgo Moderado: Cuadrantes Amarillos:
Los riesgos ubicados en estos cuadrantes presentan consecuencias y probabilidades moderadas, la materialización de algunos de estos riesgos representará un impacto medio en el logro de los objetivos de la Administración.
- Nivel de Riesgo Bajo: Cuadrantes Verdes
Los riesgos que se encuentran en estos cuadrantes son aquellos que presentan consecuencias y probabilidades bajas, de materializarse alguno impactará de forma mínima el logro de objetivos de la Administración.

Como ejemplo, puede observar en el mapa de calor los riesgos 1, 2 y 9 que se ubican en los cuadrantes rojos, tienen un nivel de riesgo absoluto extremo, el riesgo 10 tiene un nivel de riesgo absoluto alto y el riesgo 11 tiene un nivel de riesgo absoluto moderado.



6.4 Evaluación de los controles existentes por riesgo

Cada responsable del proceso, proyecto o actividad, deberá identificar los controles existentes por cada riesgo y priorizarlo, con el propósito de realizar una auto evaluación de la eficacia y eficiencia de dichos controles. Esta evaluación se realiza sobre los controles actuales que se implementan en el proceso, proyecto o actividad y relacionados con cada riesgo identificado.

Para realizar la evaluación de los controles existentes, es importante recordar que un control es parte de la administración de riesgos que involucra la ejecución de políticas, estándares y procedimientos, para minimizar la probabilidad y consecuencia de los riesgos identificados.

Estos controles se clasifican en:

- Preventivos, son aquellos que actúan para minimizar las consecuencias del riesgo o bien para prevenir su ocurrencia o materialización.
- Correctivos, son aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable y que también permite la modificación de las acciones que propician su ocurrencia.

De igual manera, se deberá determinar si los controles asociados al riesgo, están orientados a la mitigación de la probabilidad o de la consecuencia, evaluada de manera absoluta. Este análisis es importante realizarlo, dado que dependiendo del resultado del mismo, la efectividad de los controles permitirán reducir la consecuencia o la probabilidad absoluta, o ambas.

6.5 Evaluación del riesgo controlado

El análisis de los controles existentes, permitirá identificar el nivel de riesgo alcanzado una vez que haya sido analizada la efectividad del ambiente de control y su efecto en la disminución de los niveles de riesgo absoluto. El análisis del nivel de riesgo controlado es esencial ya que sobre éste se basan los lineamientos para priorizar las medidas de administración de riesgos.

El responsable del proceso, proyecto o actividad, analizará y evaluará el ambiente de control, calificando los controles pertinentes.

Los criterios para la evaluación de los controles se presentan a continuación:



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 12 de 18



Criterio	Descripción	Color de Identificación
Medida de Control Clave	Medidas cuya ejecución adecuada es indispensable para que el riesgo relacionado no se materialice y de hacerlo impacte en un grado mínimo los objetivos de la TIC	ROJO
Medida de Control No Clave	Medidas cuya ejecución, apoya y fortalece la acción de las medidas de control claves	VERDE

Además, se deberá determinar su nivel de ejecución, por lo que considerará, como mínimo los siguientes puntos:

- La ejecución de la medida
- La efectividad con la que esta medida se está realizando

El resultado del análisis anterior a cada uno de los controles revisados, se les asignará alguna de las evaluaciones que se detallan seguidamente en esta tabla:

Criterio de Evaluación	Significado	Color de Identificación
Sin Medida de Control	La medida de control no se está ejecutando	ROJO
Medida de Control Pobre	La medida de control se ejecuta esporádicamente	ANARANJADO
Medida de Control Adecuada	La medida de control se ejecuta sistemáticamente, pero carece de divulgación, formalización y además no ha sido probada por agentes externos	AMARILLO
Medida de Control Fuerte	La medida de control se ejecuta de manera efectiva, ha sido probada, pero carece de un proceso de formalización y divulgación	VERDE OSCURO
Medida de Control Hermética	La medida de control se ejecuta de manera efectiva se encuentra probada, formalizada y divulgada	VERDE CLARO

Cada medida de control identificada y evaluada, contará con la posibilidad de registrar comentarios vinculados con debilidades, mejoras y demás detalles en relación al respectivo control, ingresados por el personal que esté efectuando el proceso de auto-evaluación.



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 13 de 18



Finalizada la clasificación anterior se realizará el siguiente análisis, para cada grupo de controles orientados a la reducción de la probabilidad y los controles que están orientados a la reducción de la consecuencia:

- Si la mayoría de controles claves cuentan con una evaluación "Sin Medida de Control" o "Medida de Control Pobre", significará que el ambiente de control actual no está colaborando en la reducción de la consecuencia o probabilidad del riesgo asociado, según corresponda, por lo que la evaluación absoluta se mantendrá invariable en la evaluación del riesgo controlado.
- Si la mayoría de controles claves cuentan con una evaluación "Medida de Control Adecuada" o "Medida de Control Fuerte", significará que el ambiente de control actual está colaborando en la reducción de la consecuencia o probabilidad del riesgo asociado, según corresponda, por lo que la evaluación absoluta de la consecuencia o de la probabilidad o de ambas se verá disminuida en un nivel en la evaluación de riesgo controlado.
- Si la mayoría de controles claves cuentan con una evaluación "Medidas de Control Herméticas", significará que el ambiente de control actual está colaborando al máximo en la reducción de la consecuencia o probabilidad del riesgo asociado, según corresponda, por lo que la evaluación absoluta de la consecuencia o de la probabilidad o de ambas se verá reducida en dos niveles en la evaluación de riesgo controlado.

Toda la información recopilada en el proceso de evaluación de los controles será documentada, para realizar de manera posterior su respectivo análisis.

Realizada la evaluación de los controles, es importante generar nuevamente un mapa de calor, donde se muestre la evaluación de los riesgos sin la aplicación de medidas de control así como el desplazamiento en los cuadrantes que cada uno obtuvo, como consecuencia de la evaluación del ambiente de control asociado. Este resultado es lo que se define como "Riesgo Controlado".

Lo anterior, permitirá analizar, en un mismo plano, el nivel de riesgo absoluto: definido según la ubicación de la esfera turquesa en el respectivo cuadrante y la disminución del mismo (si fue posible), mediante la evaluación del ambiente de control. De igual manera mostrará, el nivel de riesgo controlado: definido según la ubicación de la esfera gris en el respectivo cuadrante, en éste último se centrará el estudio para determinar si es factible dar por aceptado el riesgo o por el contrario, si se le aplicará el debido proceso de administración del mismo.

Para efectos de ilustración se adjunta el siguiente mapa de calor:

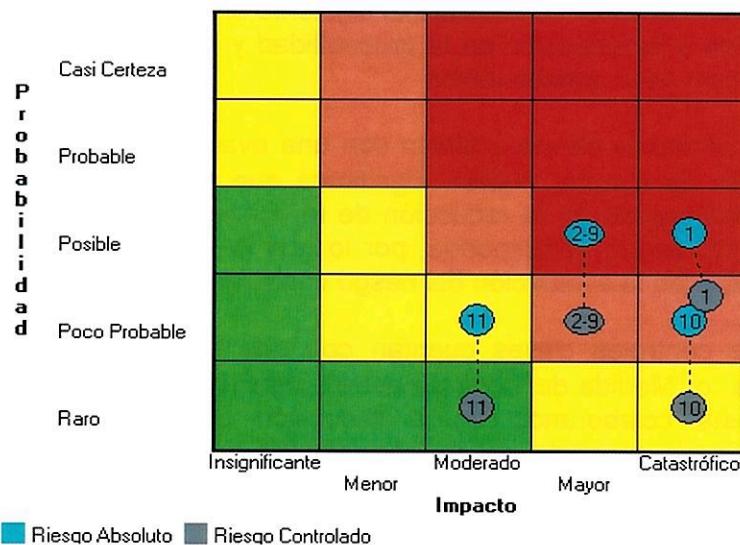


METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 14 de 18



6.6 Administración de los Riesgos relevantes identificados

Una vez identificados los riesgos que no cumplen con los criterios de aceptabilidad, se iniciará para éstos el proceso de administración del riesgo, el cual contempla las siguientes etapas:

- Identificar las medidas para la Administración de Riesgos.
- Evaluar la viabilidad de las medidas para la Administración de Riesgos.
- Preparar los planes para las medidas de Administración de Riesgos.
- Implementación de las medidas para la Administración de Riesgos.

De acuerdo al análisis del "riesgo controlado", un riesgo que no cumple con los criterios de aceptación, se puede identificar de la forma siguiente:

- Riesgos que se ubican en los cuadrantes rojos y naranjas desde el punto de vista del riesgo absoluto.
- Riesgos que se ubican en los cuadrantes rojos y naranjas desde el punto de vista controlado.
- Efectividad de los controles pobres o no existentes.

Para la selección de los riesgos que van a ser administrados se pueden aplicar los siguientes criterios:

- Un riesgo extremo, con un ambiente de control deficiente, ubicado en los cuadrantes rojos o naranja.
- Un riesgo alto, con un ambiente de control deficiente, ubicado en un cuadrante naranja.



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 15 de 18

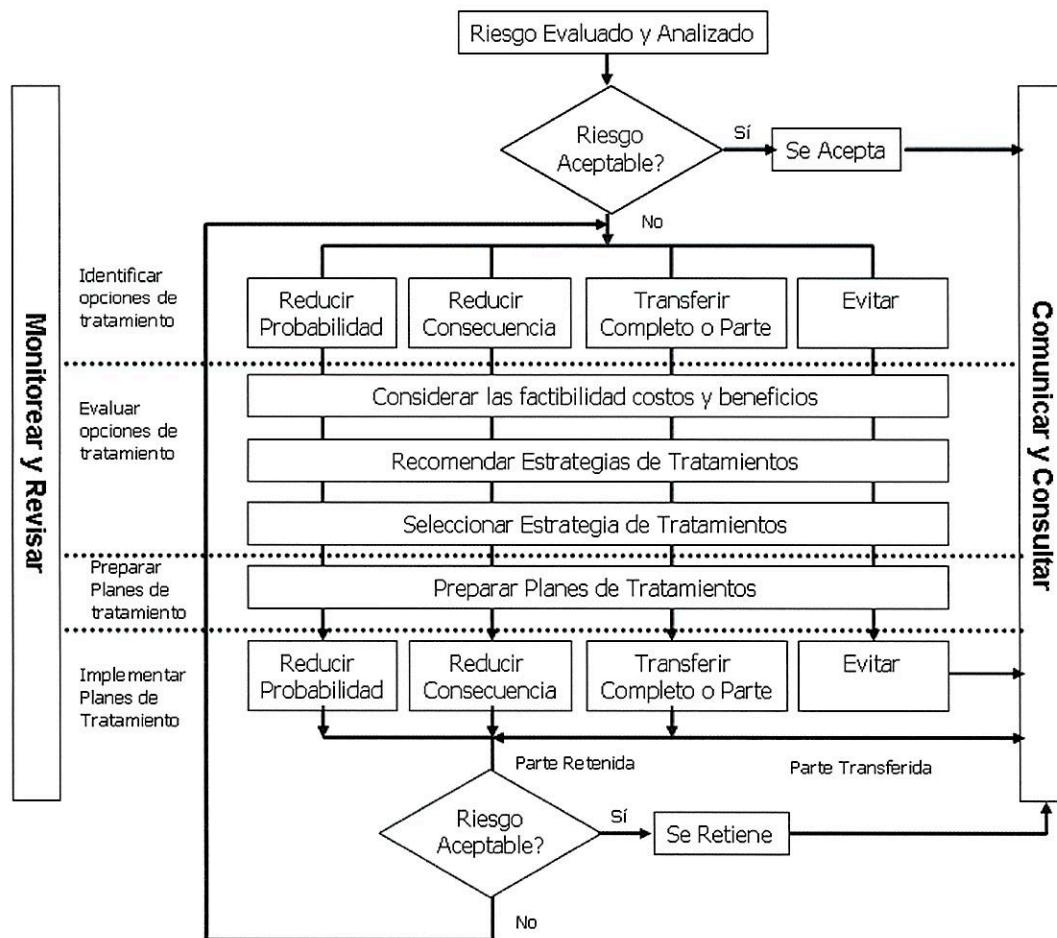


- Así mismo, existe alguna regulación particular, donde se solicita administrar los riesgos asociados a este tipo de objetivos o actividades, ejemplos de ellos son los que se derivan del cumplimiento regulatorio.

La identificación de los riesgos que deberán ser administrados, propone que se establezcan "Tratamientos" y "Planes de Acción", de la siguiente manera:

a. Seleccionar el tipo de tratamiento que se podrá aplicar

Para la selección del tipo de tratamiento que se podrá aplicar tomando en consideración la normativa existente, se deberá aplicar el siguiente diagrama de flujo



b. Identificar las medidas para la Administración de Riesgos

Se definirán, según el orden de priorización determinado durante el proceso de evaluación del riesgo, las diferentes medidas que puedan existir para administrar el riesgo.



Esta definición abarcará al menos uno de los siguientes objetivos:

Evitar el Riesgo:

No ejecutar las acciones que involucran la materialización del riesgo. Esta decisión se debe analizar con mucho cuidado, ya que de no definirse adecuadamente, puede aumentar la exposición de otros riesgos. Todos los riesgos que seleccionen bajo este criterio deben ser adecuadamente documentados e informados a la Administración Superior.

Reducir la Probabilidad:

Definición de medidas que colaboren con la minimización de la probabilidad presentada, a través de la evaluación del riesgo controlado, como revisiones preventivas y condiciones contractuales, entre otros.

Reducir Consecuencia:

Definición de medidas que colaboren con la minimización de la consecuencia presentada a través de la evaluación del riesgo controlado, como planeamiento de contingencia y planes de recuperación, entre otros.

Transferir el Riesgo:

Definir medidas mediante las cuales, terceros asuman parte o la totalidad del riesgo que se desea administrar, por ejemplo, la adquisición de seguros.

Se ejecutará la identificación de las medidas, de forma tal, que éstas traten dentro de un marco aceptable, de abarcar la mayor cantidad de riesgos cuya evaluación no ha sido aceptable y en lo posible, los funcionarios que definen, revisan o evalúan las medidas de administración del riesgo, busquen la integración de las mismas en planes globales de manejo del riesgo.

c. Evaluar la viabilidad de las Medidas para la Administración de Riesgos

Se deberá analizar la viabilidad de cada una de las medidas de administración del riesgo que han sido propuestas, con la finalidad de seleccionar y priorizar las medidas que mejor se ajustan a la ejecución de planes de acción propuestos para cada riesgo tecnológico que se ha identificado.

En este análisis se contemplarán los siguientes criterios de evaluación:

- La relación costo-beneficio de llevar a cabo la recomendación de la medida de mitigación.
- La capacidad e idoneidad de los entes participantes, internos y externos.
- El cumplimiento del interés público y el resguardo de la hacienda pública.
- La viabilidad jurídica, técnica y operacional de las alternativas propuestas para mitigar el riesgo.



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 17 de 18



Las medidas de control para la administración del riesgo se priorizarán con base en aquellas que satisfagan de la mejor manera posible estos criterios de evaluación y permitan asegurar el cumplimiento de los objetivos de los procesos, que se pueden estar viendo afectados por dichos incidentes o riesgos.

En los casos en donde se estime imposible llevar a cabo la ejecución de las medidas identificadas, se deberá valorar cuál es el proceso a seguir para retener el riesgo y definir un mecanismo de monitoreo del mismo para valorar su evolución.

d. Preparar los planes para las Medidas de Administración de Riesgos

Para cada una de las medidas, cuya viabilidad haya sido definida como apropiada, se deberá registrar los acuerdos establecidos como tratamientos y planes de acción que pretendan mitigar los riesgos. Se adjunta el formulario establecido en el Anexo A: CI-URS-F-PAT Formulario de Planes de Acción y Tratamientos de Riesgos, como herramienta de ayuda para dicho registro.

Para rastrear los riesgos identificados, los riesgos residuales y los nuevos riesgos, así como realizar una revisión con el fin de mejorar la gestión del riesgo, se deben de implementar los planes de respuesta al riesgo.

e. Seguimiento y Monitoreo

Debe existir personal de Gestión de Riesgo que realice las auditorías de riesgos para garantizar los resultados de las respuestas a riesgos para que sean eficaces y que los procesos de riesgos se realicen.

Una herramienta técnica que funciona para el proceso de seguimiento y control de los riesgos, es realizar las siguientes actividades:

- a) Gestionar los recursos asignados para Contingencia (lo que se ha gestionado en forma separada para cubrir riesgos relacionados al tiempo y al costo).
- b) Rastrear el conjunto de condiciones (Disparadores) que se asignaron a cada riesgo.
- c) Rastrear el riesgo.
- d) Rastrear el cumplimiento que se definió en el Plan de Gestión de Riesgo.

Para documentar los resultados del proceso del seguimiento y control de los riesgos se puede incluir la siguiente información:

- Para cada riesgo identificado, indicar si este ocurrió (cuándo y cuán frecuente), se deben registrar los datos relevantes como: el impacto, la efectividad de la detección y de la respuesta y cualquier acción no planificada que se llevó a cabo.
- Efectividad de las acciones para evitar o exponer



METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Código: CI-URS-M01

Versión: 1.0

Página 18 de 18



- Efectividad de las acciones de transferencia o compartir
- Riesgos inesperados que ocurrieron
- Efectividad de las acciones de mitigar o mejorar
- Ocurrencia de riesgos u oportunidades aceptadas.

Actividad	Funcionario	Versión	Fecha	Firma
Elaboración	Unidad de Gestión de Riesgo y Seguridad	1.0	27/6/2016	
Validación, Revisión	Ana Cecilia Vargas (URS)	1.0	27/6/2016	
Aprobación	Alonso Castro Mattei (Director CI)	1.0	27/06/16	