INTRODUCCION

El plan de riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todas las entidades en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; enfatiza en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y da lineamientos sencillos y claros para su adecuada gestión.

OBJETIVOS

GENERAL

Establecer los conceptos básicos y metodológicos para una adecuada administración de riesgos a partir de su identificación, manejo y seguimiento.

ESPECIFICOS

- Involucrar y comprometer a todos los funcionarios en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

ALCANCE

Este plan, proporcionará una metodología establecida por la Entidad para la administración y gestión de los riesgos a nivel interno; orienta sobre las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis y valoración de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

DIRECCIONAMIENTO ESTRATEGICO

LINEA ESTRATEGICA

A la hora de garantizar la seguridad en cualquier entorno, además de tener las medidas técnicas y legales adecuadas es de vital importancia el factor humano, ya que con frecuencia los mayores problemas de seguridad se presentan por errores o descuidos en el hacer diario del personal, por este motivo se debe capacitar al personal que tiene acceso a la información digital y física de la institución, para minimizar y eliminar el riesgo de pérdida o daño, parcial o total de la información.

GESTION DE RIESGO EN LA SEGURIDAD INFORMATICA

La Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

En su forma general contiene cuatro fases

ANALISIS

Determina los componentes de un sistema que requieren protección, sus vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el resultado de revelar su grado de riesgo

CLASIFICACION

Determina si los riesgos encontrados y los riesgos restantes son aceptables.

REDUCCION

Define e implementa las medidas de protección. Además, sensibiliza y capacita los usuarios conforme a las medidas.

CONTROL

Analiza el funcionamiento, la efectividad y el cumplimiento de las medidas, para determinar y ajustar las medidas deficientes y sanciona el incumplimiento.

Todo el proceso está basado en las llamadas políticas de seguridad, normas y reglas institucionales, que forman el marco operativo del proceso, con el propósito de potenciar las capacidades institucionales, reduciendo la vulnerabilidad y limitando las amenazas con el resultado de reducir el riesgo.

Orientar el funcionamiento organizativo y funcional.

Garantizar corrección de conductas o prácticas que nos hacen vulnerables.

METODOLOGIA DE EVALUACIÓN DEL RIESGO

Es el primer paso hacia la gestión de riesgos. Necesita definir las reglas para llevar a cabo la gestión de riesgo, ya que querrá que toda la empresa lo haga de la misma forma, el principal problema del plan de tratamiento de riesgos de seguridad de la información es que la organización lo ejecute de diferente forma en distintas partes de la organización.

IDENTIFICACION DEL RIESGO

La finalidad de esta fase es descubrir, reconocer y registrar los riesgos. Este proceso incluye la identificación de las causas y el origen de los riesgos, los sucesos o situaciones que pueden tener un impacto en los objetivos de la organización

METODOS DE IDENTIFICACION DEL RIESGO PUEDEN INCLUIR

Métodos basados en evidencias como pueden ser, las listas de verificación y las revisiones de datos históricos.

Enfoques sistemáticos de equipos, como los grupos de expertos que siguen un método con una sistemática estructurada de preguntas para identificar los riesgos.

ANALISIS DEL RIESGO

Esta fase implica una comprensión del riesgo, es decir, determinar sus consecuencias y probabilidades, teniendo en cuenta la presencia y la eficacia de los controles existentes.
Los métodos que se utilizan para este análisis de riesgos pueden ser cualitativos, semicuantitativos o cuantitativos.

La apreciación cualitativa se suele expresar con niveles del tipo “alto”, “medio” y “bajo” para definir las consecuencias, las probabilidades o el nivel de riesgo.
Los métodos semicuantitativos utilizan escalas de valoración numérica lineales o logarítmicas principalmente.
El análisis cuantitativo trabaja con valores numéricos realistas y obtiene el mismo tipo de resultados. El problema suele ser que, en ocasiones, junto a estos valores deben tenerse en cuenta otros factores difícilmente cuantificables o simplemente que faltan datos.

EVALUACIÓN DEL RIESGO

En la fase de evaluación se toman las decisiones sobre las acciones futuras basadas en el conocimiento del riesgo que se ha obtenido durante la fase de análisis.
En la mayoría de las ocasiones, el criterio para tomar la decisión de, si se debe tratar el riesgo y cómo hacerlo, depende de los costos/beneficios de aceptar el riesgo y/o de implantar los controles pertinentes.
El criterio de “tan bajo como razonablemente sea posible” es un clásico de este enfoque de criterio

SELECCIÓN DE LAS TECNICAS DE APRECIACION DEL RIESGO

Llega el momento clave de ver que técnica/herramienta vamos a elegir. Los principales factores a tener en cuenta son:

- La disposición de recursos adecuados en tiempo y experiencia, así como el presupuesto con el que contamos.
- La naturaleza y el grado de la incertidumbre, que depende de la calidad, cantidad e integridad de los datos e información disponible sobre los riesgos considerados.
- La complejidad de los riesgos.

COMPONENTES DE LA IDENTIFICACION DEL RIESGO

CAUSAS DEL RIESGO

Son las causas, uno de los aspectos a eliminar o mitigar para que el riesgo no se materialice; esto se logra mediante la definición de controles efectivos. Para realizar

el análisis de las causas existen varias técnicas que serán analizadas a continuación.

LLUVIA DE IDEAS

Usualmente se utiliza la técnica de lluvia de ideas para identificar todo aquello que puede ser considerado dentro del análisis de riesgos y para que esta sea eficaz, se debe considerar que:

- Debe haber un moderador que tome nota y que organice las exposiciones de todos los participantes, indicando el tiempo que cada cual tiene para presentar sus ideas.
- Es más importante la cantidad de ideas que la calidad de las mismas. Todas las ideas son valiosas para el proceso de recopilación de información.
- No se deben calificar las ideas como buenas o malas, son simplemente puntos de vista que capitalizados pueden brindar alternativas no consideradas.
- Es importante soportarse en las ideas de los otros. Es decir, agregar valor a las apreciaciones de otros o considerar situaciones a partir de las mismas.
- El análisis de las ideas se debe realizar al final, por el moderador, quien las organizará y las expondrá a manera de resultado.
- Todos deben participar de manera equitativa, es importante no fijar la atención en pocos participantes, ni mantenerse en la palabra sin dar la oportunidad a otro de expresar sus ideas

CONSECUENCIAS

Son los efectos que se generan o pueden generarse con la materialización del riesgo sobre los objetivos de los procesos y de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.
Se deben determinar las consecuencias del riesgo en escala ascendente; definiendo cual podría ser el efecto menor que puede causar la materialización del riesgo hasta llegar al efecto mayor generado.

CLASIFICACION DE LOS RIESGOS

Durante la etapa de identificación, se realiza una clasificación del riesgo, según sus características, con el fin de orientar la formulación de un tratamiento adecuado que posibilite la mitigación del riego mediante la definición de controles y planes de manejo:

Clases de riesgo	Definición
Estratégico	Son los riesgos relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
Operativo	Relacionados con el funcionamiento y operatividad de los sistemas de información de la entidad: definición de procesos, estructura de la entidad, articulación entre dependencias.
Financieros	Relacionados con el manejo de los recursos de la entidad: ejecución presupuestal, elaboración estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes.
Cumplimiento	Capacidad de cumplir requisitos legales, contractuales, ética pública y compromiso con la comunidad.
Tecnología	Capacidad para que la tecnología disponible satisfaga las necesidades actuales y futuras y el cumplimiento de la misión.
Imagen	Tienen que ver con la credibilidad, confianza y percepción de los usuarios de la entidad.

Escala para calificar la probabilidad del riesgo		
Nivel	**Concepto**	**Frecuencia**
Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
Improbable	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
Moderado	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.

Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
Casi certeza	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Escala para calificar el impacto del riesgo							
Tipos de efecto o impacto		**a) Estratégico**	**b) Operativo**	**c) Financieros**	**d) Cumplimiento**	**e) Tecnología**	**f) Imagen**
INSIGNIFICANTE	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos o bajos sobre la institución	Afecta el cumplimiento de algunas actividades	Genera ajustes a una actividad concreta	La pérdida financiera no afecta la operación normal de la institución	Genera un requerimiento	Afecta a una persona o una actividad del proceso	Afecta a un grupo de servidores del proceso
MENOR	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la institución	Afecta el cumplimiento de las metas del proceso	Genera ajustes en los procedimientos	La pérdida financiera afecta algunos servicios administrativos de la institución	Genera investigaciones disciplinarias, y/o fiscales y/o penales	Afecta el proceso	Afecta a los servidores del proceso
MODERADO	Si el hecho llegara a presentarse tendría medianas consecuencias o efectos sobre la Institución	Afecta el cumplimiento de las metas de un grupo de procesos	Genera ajustes o cambios en los procesos	La pérdida financiera afecta considerablement e la prestación del servicio	Genera interrupciones en la prestación del bien o servicio	Afecta varios procesos de la institución	Afecta a todos los servidores de la institución
MAYOR	Si el hecho llegara a presentarse tendría altas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas de la institución	Genera intermitencia en el servicio	La pérdida financiera afecta considerablement e el presupuesto de la institución	Genera sanciones	Afecta a toda la entidad	Afecta el sector
CATASTRÓFICO	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la institución	Afecta el cumplimiento de las metas del sector y del gobierno	Genera paro total de la institución	Afecta al presupuesto de otras entidades o a de la del departamento	Genera cierre definitivo de la institución	Afecta al Departamento	Afecta al Departamento, Gobierno, Todos los usuarios de la institución

VALORACION DE LOS RIESGOS

Es el producto de confrontar la evaluación del riesgo y los controles (preventivos o correctivos) de los procesos. La valoración del riesgo se realiza en tres momentos: primero, identificando los controles (preventivos o correctivos) que pueden disminuir la probabilidad de ocurrencia o el impacto del riesgo; luego, se deben evaluar los controles, y finalmente, con base en los resultados de la evaluación de los controles, determinar la evaluación del riesgo residual y definir la opción de manejo del riesgo. Lo anterior de acuerdo con los formatos de Identificación y evaluación de controles y Valoración del riesgo.

IDENTIFICACION DE CONTROLES

Los controles son las acciones orientadas a minimizar la probabilidad de ocurrencia o el impacto del riesgo; estos, deben estar directamente relacionados con las causas o las consecuencias identificadas para el riesgo y eliminarlas o mitigarlas. La administración del riesgo contribuirá a la gestión de la entidad, en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos.

A continuación, se presentan las características mínimas que se deben tener en cuenta para la definición de los controles:

Característica	Descripción
Objetivos	No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener
Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo
Realizables	Se deben definir controles que la entidad o el proceso esté en capacidad de llevar a cabo
Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad
Periódicos	Tienen frecuencia de aplicación en el tiempo

Efectivos	Eliminan o mitigan las causas o consecuencias y evitan la materialización del riesgo
Asignables	tienen responsables definidos para su ejecución

ETAPAS PARA LA ADMINISTRACION DEL RIESGO

A continuación, se presenta cada una de las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

- **Contexto estratégico:** determinar los factores externos e internos del riesgo.
- **Identificación:** identificación de causas, riesgo, consecuencias y clasificación del riesgo.
- **Análisis:** Calificación y evaluación del riesgo inherente.
- **Valoración:** identificación y evaluación de controles; incluye la determinación del riesgo residual.
- **Manejo:** determinar, si es necesario, acciones para el fortalecimiento de los controles.
- **Seguimiento:** evaluación integral de los riesgos

SEGUIMIENTO DE RIESGOS

Cada año realizará seguimiento a todo el componente de administración de riesgos y verificará aspectos como:

Cumplimiento de las políticas y directrices para la administración del riesgo: metodología de Administración del Riesgo (diseño y funcionamiento).
Administración de los riesgos por proceso e institucionales: calificación y evaluación, efectividad de los controles y cumplimiento de las acciones.

Los resultados de la evaluación y las observaciones de la persona que haga las veces de auditor deben ser presentados, para que se tomen las decisiones pertinentes que garanticen la sostenibilidad de la Administración del Riesgo en la organización.