GUIA
GESTION DE RIESGOS Y OPORTUNIDADES ODAPAS TECAMAC
(ANEXO 3)

PRINCIPIO: PENSAMIENTO BASADO EN RIESGOS

El concepto de pensamiento basado en riesgos ha estado implícito en ediciones previas de la norma ISO 9001:2015, por ejemplo, mediante requisitos para la planificación, la revisión y la mejora. La norma ISO 9001:2015 especifica requisitos para que la organización entienda su contexto (en 4.1) y determine los riesgos como base para la planificación (en 6.1). Esto representa la aplicación del pensamiento basado en riesgos a la planificación e implementación de los procesos del SGC (en 4.4) y ayudará a determinar la extensión de la información documentada

Uno de los propósitos fundamentales de un SGC es actuar como una herramienta preventiva. El concepto de acción preventiva se expresa mediante el uso del pensamiento basado en riesgos al formular requisitos del SGC

METODOLOGIA GESTION DE RIESGOS

1. IDENTIFICACION DE RIESGOS

La identificación de riesgos se basa en el resultado del análisis del Contexto Estratégico, en el proceso de planeación, partiendo de la claridad de los objetivos estratégicos de la organización para la obtención de resultados

La identificación de los riesgos se realiza a nivel del Componente de “Dirección Estratégica”, identificando los factores internos o externos a la organización, que pueden ocasionar riesgos que afecten el logro de los objetivos

Entender la importancia del manejo del riesgo implica conocer con detalle los siguientes conceptos:

Proceso: Conjunto de actividades mutuamente relacionadas que utilizan las entradas para proporcionar un resultado previsto

Objetivo: Resultado a lograr

Objetivo del proceso: objetivo que se ha definido para el proceso al cual se le están identificando los riesgos

Riesgo: efecto de la incertidumbre, posibilidad de ocurrencia de un evento que puede entorpecer el desarrollo normal de las funciones de la organización o de sus procesos y afectar el logro de sus objetivos

Causas: (**Factores** o **Cuestiones** internos o externos): medios, circunstancias y agentes generadores del riesgo, se pueden clasificar en dos categorías o factores generales:

Factores o Cuestiones Internos:

Situación actual: institucionalización, visión, misión y valores, gestión de la organización, definición de objetivos y estrategias, indicadores, planes y programas, estructura organizacional, capacidad, crecimiento y desarrollo organizacional, logros, éxitos, obstáculos, fracasos, grado de madurez, prestigio, rendición de cuentas ante partes interesadas, planes de contingencia
Humano: capacidad directiva, capacitación, desarrollo y competencia del personal, involucramiento, compromiso
Infraestructura instalaciones, equipos, tecnología
Competitividad: Calidad de productos y servicios, metodologías de operación, cobertura, innovación, eficacia y eficiencia

Capacidad financiera, política de rentabilidad, estructura de ingresos y de gastos, estructura de costos, controles sobre ingresos y egresos, gestión presupuestal, resultados financieros: utilidades, rentabilidad, punto de equilibrio, razones financieras

Factores o Cuestiones externos:

Clientes: requisitos, necesidades y expectativas, fidelidad, retención, comunicación, percepción y retroalimentación
Mercados y competencia: proyección, comportamiento, afectación, posición, participación, estudios de mercado, líderes y principales competidores, agresividad, asociaciones
Proveedores: calidad, capacidad, compromiso, disponibilidad, confiabilidad y mejora, desarrollo de nuevos proveedores
Gobierno y comunidad: políticas y tendencias económicas, sociales, culturales y ambientales, cumplimiento de obligaciones, relaciones con la comunidad, calidad de servicios públicos

Descripción (del riesgo): características generales o formas en que se observa manifiesta el riesgo identificado

Efectos (consecuencias): constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la organización, por ejemplo: daños físicos, fallecimientos, sanciones por incumplimiento de contratos o legislación, pérdidas económicas, de información, de bienes, de imagen y prestigio, de credibilidad y de confianza, interrupción de la producción o del servicio y daño ambiental

Formato de identificación de riesgos

PROCESO:				
Objetivo del proceso	**Causas (Factores o Cuestiones internos y externos, Agente generador)**	**RIESGO**	**DESCRIPCION**	**EFECTOS (CONSECUENCIAS)**

2. CLASIFICACION DEL RIESGO:

Riesgo estratégico: se asocia con la forma en que se gestiona la entidad. La gestión del riesgo estratégico se enfoca a asuntos globales relacionados con la visión, la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la organización por parte de la alta dirección. Su atención requiere acciones del área que lo detecta, de otras instancias de la propia organización, y en su caso de otras instancias externas

Riesgo operativo: comprende los riesgos relacionados tanto con la parte operativa como técnica de la organización, incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos y su estructura, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimientos de los compromisos institucionales, generalmente puede ser atendido por el área o proceso que lo detecta, en algunos casos con el apoyo de otras áreas internas o procesos

Otros tipos de riesgos:

Riesgo financiero: se relacionan con el manejo de los recursos de la organización que incluye la ejecución presupuestal, la elaboración de los estados financieros, los pagos, la cobranza, manejo de excedentes de tesorería y el manejo de los bienes

Riesgo de cumplimiento: se asocian con la capacidad de la organización para cumplir con los requisitos legales, contractuales, éticos, de confidencialidad y en general con su compromiso ante la comunidad

Riesgo de tecnología: se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la entidad y soporte el cumplimiento de la misión

3. ANALISIS DEL RIESGO

Busca establecer la **PROBABILIDAD** de ocurrencia de los riesgos y el **IMPACTO** de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar

Por PROBABILIDAD se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo, número de veces en un tiempo determinado) o de Factibilidad teniendo en cuanta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado

Por IMPACTO se entiende las CONSECUENCIAS que puede ocasionar a la organización la materialización del riesgo

TABLA DE PONDERACIONES PARA ANALISIS DEL RIESGO

PROBABILIDAD DE OCURENCIA	VALOR	GRADO DE IMPACTO	VALOR
ALTA (Recurrente)	3	**CATASTROFICO (influye directamente en el cumplimiento de la misión, pérdida patrimonial, de clientes, sanciones, suspensiones, cancelaciones, interrupciones largas para entregar productos y servicios, deterioro o perdida de la imagen o prestigio)**	3
MEDIA (Posible)	2	**MODERADO (influye de forma importante en el cumplimiento de la misión, pérdida patrimonial, de clientes, sanciones, suspensiones, cancelaciones, deterioro de la imagen, asignación de tiempos importantes para su resolución)**	2
BAJA (inusual o remota)	1	**LEVE (pequeño, nulo o efecto poco significativo al patrimonio, al cumplimiento contractual o legal, o a la operación, se puede corregir de forma inmediata, no afecta a la misión)**	1

4. CALIFICACIÓN DEL RIESGO

Es la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo

Se califican cada uno de los riesgos según la matriz de acuerdo con las siguientes especificaciones: probabilidad alta se califica con 3, probabilidad media con 2 y probabilidad baja con 1, de acuerdo con el número de veces que se presenta o puede presentarse el riesgo. Y el impacto si es leve con 1, si se moderado con 2 y si es catastrófico con 3

5. EVALUACIÓN DEL RIESGO

Permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la organización al riesgo: aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento:

Leve, moderada y catastrófica con relación al impacto y alta, media y baja respecto a la probabilidad

Para la evaluación del riesgo hay que tener en cuenta la posición del riesgo en la matriz, según la celda que ocupa

MATRIZ DE CALIFICACION, EVALUACION Y RESPUESTA A LOS RIESGOS

PROBABILIDAD DE OCURENCIA	**VALOR**			
ALTA	3	3 Zona de riesgo **MODERADO** Evitar el riesgo	6 Zona de riesgo **IMPORTANTE** reducir el riesgo Compartir o transferir	9 Zona de riesgo **INACEPTABLE** Evitar el riesgo Reducir el riesgo Compartir o transferir
MEDIA	2	2 Zona de riesgo **TOLERABLE** Asumir el riesgo Reducir el riesgo	4 Zona de riesgo **MODERADO** Reducir el riesgo Evitar el riesgo Compartir o transferir	6 Zona de riesgo **IMPORTANTE** Reducir el riesgo Evitar el riesgo Compartir o transferir
BAJA	1	1 Zona de riesgo **ACEPTABLE** Asumir el riesgo	2 Zona de riesgo **TOLERABLE** Reducir el riesgo Compartir o transferir	3 Zona de riesgo **MODERADO** Reducir el riesgo Compartir o transferir
	GRADO DE IMPACTO	**BAJO (LEVE)**	**MEDIO (MODERADO)**	**ALTO (CATASTROFICO)**
	VALOR	1	2	3

POLITICAS PARA LA GESTION DE RIESGOS

Permiten estructurar criterios orientadores en la toma de decisiones, respecto al tratamiento de los riesgos y sus efectos dentro de la organización

TRATAMIENTO	POLITICA
Evitar	Se debe eliminar la probabilidad de ocurrencia o disminuir totalmente su impacto. Lo anterior implica eliminar la actividad que genera el riesgo o implementar medidas de protección externas, las cuales implican en algunos casos altos costos
Prevenir	- Inspecciones y pruebas de seguridad en equipos, servicios, maquinaria, etc. - Entrenamiento del personal en cualquier tipo de actividad a desarrollar - Inversión en información para mejorar predicciones y efectuar análisis, pronóstico de precios, estudios de mercado, tasas de cambio - Diversificación de inversiones o al adaptar nuevos proyectos en sectores diferentes - Disminuir el nivel de exposición, reduciendo el nivel de actividad, en situaciones que implican riesgo para la salud - Segregación de funciones, para prevenir fraudes, errores, demoras - Mantenimiento preventivo en equipos y máquinas para evitar fallas, los cuales pueden ocasionar daños en equipos, afectar la salud de las personas, deterioro de productos, etc. - Medicina preventiva y actividades de salud ocupacional, por medio de exámenes de oído, ojos y otros, los cuales si se tratan a tiempo pueden evitar accidentes o disminución de capacidades - Políticas de seguridad, a través del establecimiento de normas internas tendientes a orientar la conducta de los empleados en el desarrollo del trabajo
Proteger o mitigar	Es la acción en el momento del peligro o la presencia del riesgo, para lo cual se debe contar con: - Sistemas automáticos de protección como detectores de humo, activación automática de sirenas para apagar incendios en caso de que suceda, corte de energía en caso de temblores, etc. - Equipos de protección personal, como cascos, gafas, delantales, guantes, calzado, fajas, etc. - Plan de emergencia, de acuerdo con lo establecido en cada organización para las diferentes situaciones - Plan de contingencia, ante situaciones que interrumpan la producción o la prestación del servicio y reducir los efectos negativos que puedan darse, para lo cual es importante identificar los procesos críticos de la organización, tiempo mínimo en que se puede restablecer el servicio, definición de responsable de tomar acciones, etc. - Copias de seguridad y sistemas espejos en el caso de los sistemas, convenios de ayuda mutua con otras instituciones, utilización de medios de comunicación adecuados cuando existen rumores sobre la calidad del servicio de la organización
Aceptar	En ocasiones no es necesario tomar medidas en especial cuando al evaluar el impacto y su probabilidad de ocurrencia no existe un efecto significativo para la organización
Retener	Consiste en afrontar de forma planeada la consecuencia de los riesgos o a través de alternativas que respondan a los riesgos como: creación de fondos en las cuentas de activos, para afrontar situaciones de liquidez, incluir en el presupuesto partidas adicionales para afrontar eventos no previstos, creación de provisiones contables, para el caso de pérdidas de cartera, inventarios, etc.; tener créditos disponibles para cuando se presenta una situación donde se requiera liquidez inmediata en el desarrollo de las actividades de la organización, etc.
Transferir	Involucra a un tercero, el cual podría absorber las pérdidas de la organización por medio de cláusulas en los contratos, transfiriendo ciertas responsabilidades a los contratistas. Transfiriendo el riesgo por medio de seguros, tales como seguros de transporte, seguros patrimoniales, pólizas de manejo, seguro de automóviles, responsabilidad civil, etc.

6. VALORACION DEL RIESGO

La valoración del riesgo es el resultado de confrontar los resultados de la evaluación del riesgo con los controles identificados como parte de la gestión de la organización, con el objetivo de establecer prioridades para su manejo y fijación de políticas

Se hace necesario tener claridad sobre los **puntos de control existentes** en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones

Para realizar la valoración de los controles existentes es necesario recordar que estos se clasifican en:

- Preventivos: aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización
- Correctivos: aquellos que permiten eliminar las causas del riesgo que provocaron su ocurrencia o materialización y que permiten el restablecimiento de la actividad después de haber sido detectado un evento no deseable

Procedimiento para la valoración del riesgo

Establecer si son correctivos o preventivos, respondiendo las siguientes preguntas:

¿los controles están documentados?
¿se está aplicando en la actualidad?
¿es efectivo para minimizar el riesgo?

Realizar la valoración, así:

- calificados y evaluados los riesgos, analícelos frente a los controles existentes en cada riesgo
- pondere según la tabla establecida, teniendo en cuenta las respuestas a las preguntas anteriormente formuladas
- ubique en la matriz de calificación, evaluación y respuesta a los riesgos, el estado final de riesgo, de acuerdo a los resultados obtenidos en la valoración del mismo

TABLA VALORACION DEL RIESGO

CRITERIOS	VALORACION
No existen controles	Se mantiene el resultado de la evaluación antes de controles
Los controles existen, no son efectivos	Se mantiene el resultado de la evaluación antes de controles
Los controles existen, son efectivos pero no están documentados	Cambia el resultado a una casilla inferior de la matriz de evaluación antes de controles (el desplazamiento depende de si el control afecta el impacto o la probabilidad)
Los controles existen, son efectivos y están documentados	Pasa a la escala inferior (el desplazamiento depende de si el control afecta el impacto o la probabilidad)

EJEMPLO:

RIESGO: Pérdida de información debido a la entrada de un virus en la red de información de la organización

PROBABILIDAD: Alta – 3, porque todas las computadoras de la organización están conectadas a la red de internet e intranet

IMPACTO: Alto – 3, porque la pérdida de información conllevaría consecuencias graves para el quehacer de la organización

EVALUACION DEL RIESGO: de acuerdo con la matriz de calificación y evaluación sería de 9 y se encontraría en la zona de riesgo inaceptable

Descripción de los controles existentes:

1. Se hacen Backups o copias de seguridad, semanalmente. Control preventivo
2. Se vacunan todos los programas y equipos diariamente. Control preventivo
3. Se guarda la información mas relevante fuera de la red en un centro de información

Control preventivo:

¿Los controles están documentados? SI
¿Se está aplicando en la actualidad? SI
¿Es efectivo para minimizar el riesgo? SI

DE ACUERDO CON LA TABLA SE ENTIENDE QUE LA VALORACIÓN DEL RIESGO ES: Media y se ubica en la zona moderada 10 debido a la efectividad de los controles existentes, ya que los dos primeros controles apuntan a disminuir la probabilidad y el ultimo a disminuir el impacto, por lo tanto las acciones que se implementen entrarán a reforzar los controles establecidos y a valorar la efectividad de los mismos

Es recomendable elaborar un mapa de riesgos por proceso al final de esta etapa

Con la realización de esta etapa se busca que la organización obtenga los siguientes resultados:

- identificación de los controles existentes para los riesgos identificados y analizados

- priorización de los riesgos de acuerdo con los resultados obtenidos de confrontar la evaluación del riesgo con los controles existentes, a fin de establecer aquellos que puedan causar mayor impacto en la organización en caso de materializarse

- elaborar el mapa o matriz de riesgo para cada proceso

POLITICAS DE GESTION DE RIESGOS

Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de riesgos, permiten tomar decisiones adecuadas y fijar los lineamientos de la Gestión de Riesgos, a su vez transmite la posición de la dirección y establecen las guías de acción necesarias a todos los participantes de la organización

Se deben tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto

1. Evitar el riesgo, tomar las medidas encaminadas a prevenir su materialización, un ejemplo de esto puede ser el control de calidad, el manejo de insumos, el mantenimiento preventivo de equipos, el desarrollo tecnológico, etc.
2. Reducir el riesgo, implica tomar medidas encaminadas a disminuir tanto la probabilidad (medios de prevención), como el impacto (medidas de protección). Se consigue mediante la optimización de los procedimientos y la implantación de controles
3. Compartir o Transferir el riesgo, reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como por ejemplo los contratos con aseguradoras o de conservación de información
4. Asumir el riesgo, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso acepta la pérdida residual probable y elabora planes de contingencia para su manejo

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben de ser factibles y efectivas, tales como: la implementación de políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos, entre otros. La selección de las acciones más convenientes debe considerar la viabilidad jurídica, técnica, institucional, financiera y económica y se puede realizar con base en los siguientes criterios:

- La valoración del riesgo
- El balance entre el costo de la implementación de cada acción contra el beneficio de la misma. Para la ejecución de las acciones se deben identificar las áreas responsables de llevarlas a cabo, definir un cronograma y unos indicadores que permitan verificar el cumplimiento para tomar medidas correctivas cuando sea necesario

Con la realización de esta etapa se busca encauzar el accionar de la entidad hacia el uso eficiente de los recursos, la continuidad en la prestación de los servicios, la protección de los bienes utilizados para servir a la comunidad. Igualmente se busca que la organización tenga claridad sobre las políticas de Gestión de riesgos, las acciones de manejo de riesgos y el compromiso de la Alta dirección y del personal de la organización

7. ELABORACION DEL MAPA O MATRIZ DE RIESGOS POR PROCESO Y EL INSTITUCIONAL

El mapa o matriz de riesgos contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la organización, permitiendo conocer las políticas inmediatas de respuesta ante ellos, tendientes a evitar, reducir, dispersar o transferir el riesgo; o asumir el riesgo residual, y la aplicación de acciones, así como los responsables, el cronograma y los indicadores

Es recomendable elaborar un mapa o matriz de riesgos por cada proceso para facilitar la administración del riesgo, el cual debe elaborarse al finalizar la etapa de valoración del riesgo

RIESGO	IMPACTO	PROBABILIDAD	EVALUACIÓN RIESGO	CONTROLES EXISTENTES	VALORACIÓN RIESGO	OPCIONES DE MANEJO	ACCIONES	RESPONSABLES	CRONOGRAMA	SEGUIM.

Formato Mapa o Matriz de Riesgos

DESCRIPCION DEL MAPA O MATIRZ DE RIESGOS

RIESGO: efecto de la incertidumbre, posibilidad de ocurrencia de un evento que puede entorpecer el desarrollo normal de las funciones de la organización o de sus procesos y afectar el logro de sus objetivos

IMPACTO: CONSECUENCIAS que puede ocasionar a la organización la materialización del riesgo

PROBABILIDAD: entendida como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo, número de veces en un tiempo determinado) o de Factibilidad teniendo en cuanta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado

EVALUACION DEL RIESGO: resultado obtenido en la matriz de calificación, evaluación y respuesta a los riesgos

CONTROLES EXISTENTES: controles que la organización tiene implementados para combatir, minimizar o prevenir el riesgo

VALORACION DEL RIESGO. Es el resultado de determinar la vulnerabilidad de la organización al riesgo, luego de confrontar la evaluación del riesgo con los controles existentes

OPCIONES DE MANEJO: opciones de respuesta ante los riesgos tendientes a evitar, reducir, dispensar o transferir el riesgo, o asumir el riesgo residual

ACCIONES: es la aplicación concreta de las opciones de manejo del riesgo que entrarán a prevenir o a reducir el riesgo y harán parte del plan de manejo de riesgos

RESPONSABLES: son las áreas encargadas de aplicar las acciones propuestas

CRONOGRAMA: son las fechas establecidas para implementar las acciones por parte del grupo de trabajo

SEGUIMIENTO

Una vez desarrollado y validado el plan para gestionar los riesgos, en el mapa o matriz de riesgos, es necesario monitorearlo teniendo en cuanta que estos nunca dejan de representar una amenaza para la organización

El monitoreo debe estar a cargo de los responsables de los procesos y del área de Control interno, su finalidad principal será la de aplicar y sugerir los correctivos y ajustes necesarios para asegurar un efectivo manejo del riesgo

GESTION DE OPORTUNIDADES

IDENTIFICACION

Como parte del análisis del contexto de la organización, se pueden identificar oportunidades. Las oportunidades pueden surgir como resultado de una situación favorable para lograr un resultado previsto, por ejemplo un conjunto de circunstancia que permita a la organización atraer cliente, desarrollar nuevos productos o servicios, reducir residuos o mejorar la productividad. Las acciones para abordar las oportunidades también pueden incluir la consideración de los riesgos asociados. El riesgo es el efecto de la incertidumbre y dicha incertidumbre puede tener efectos positivos o negativos. Una desviación positiva puede que surge de un riesgo puede proporcionar una oportunidad, pero no todos los efectos positivos del riesgo tiene como resultado oportunidades

Formato de identificación de oportunidades

PROCESO:			
Objetivo del proceso	**Causas (Factores o Cuestiones internos y externos, Agente generador)**	**OPORTUNIDAD DESCRIPCION**	**EFECTOS (BENEFICIOS ESPERADOS)**

MATRIZ DE OPORTUNIDADES

OPORTUNIDAD	BENEFICIO ESPERADO	DECISION / VIABILIDAD	ACCIONES	RESPONSABLES	CRONOGRAMA	SEGUIMIENTO

Formato Matriz de Oportunidades

REFERENCIAS:

CONTROL INTERNO Y SISTEMA DE GESTION DE CALIDAD (Ediciones de la U, 2012)
NORMA ISO 9001:2015, ANEXO A

RESPONSABLE DE EMISION: LIC. MAURICIO MORQUECHO ALVAREZ
FECHA DE EMISION / ACTUALIZACION: 6 DE AGOSTO DE 2018