## TABLA DE CONTENIDO

## 1. OBJETIVO

Establecer los lineamientos para la Administración del Riesgo en la Procuraduría General de la nación – PGN, mediante la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos a los que está expuesta la entidad, con el propósito de generar una cultura de prevención frente a la ocurrencia de hechos o situaciones que puedan afectar o entorpecer la gestión institucional.

## 2. ALCANCE

Esta guía aplica a todos los procesos de la PGN, establecidos en el marco del Sistema de Gestión de Calidad y se hace extensiva a todas las sedes de la PGN en el nivel central, a las Procuradurías delegadas, regionales, distritales y provinciales. Esta guía es establecida por la Alta Dirección en el Comité Institucional de Coordinación de Control Interno, con el fin de garantizar un adecuado conocimiento y control de los riesgos en todos los niveles organizacionales.

## 3. RESPONSABLES

- Comité Institucional de Coordinación de Control Interno
- Líderes y gestores de proceso
- Oficina de Planeación
- Oficina de Control Interno

## 4. DEFINICIONES Y SIGLAS

- **Acción u omisión:** Consiste en realizar algo o dejar de hacerlo intencionalmente para favorecer a un tercero.
- **Activo:** En el contexto de seguridad de la información son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Administración del Riesgo:** Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Apetito al riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los diferentes tipos de riesgos que la entidad debe o desea gestionar.
- **Áreas de impacto:** Es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materialización de un riesgo. Los impactos que aplican son afectación económica o presupuestal y reputacional.
- **Asumir el Riesgo:** Medida de tratamiento del riesgo en la cual se aceptan las consecuencias del riesgo por considerar muy baja la probabilidad de su ocurrencia o leves sus consecuencias.
- **Beneficio particular:** Consiste en la ejecución de las actividades con el fin de un favorecimiento propio o de un tercero
- **Causa:** Factor interno o externo, que sólo o en combinación con otros, puede producir la materialización de un riesgo.
- **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- **Causa raíz:** Causa principal o básica, corresponde a las razones por las cuales se puede presentar un riesgo.
- **Capacidad del riesgo:** Es el máximo valor del nivel del riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería ´posible el logro de los objetivos de la Entidad.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Efecto o situación resultante de la materialización del riesgo que impacta en el proceso, la entidad, sus grupos de valor y/o demás partes interesadas.
- **Contexto del proceso:** Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo de cada proceso.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Control correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.
- **Control detectivo:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control Preventivo:** Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control manual:** controles que son ejecutados por personas
- **Control automático:** controles que son ejecutados por un sistema
- **Descripción del Riesgo:** Narración o explicación de las siguientes preguntas: ¿Qué puede suceder?, ¿cómo puede suceder?, y ¿por qué puede suceder? Debe iniciar con la frase “POSIBILIDAD DE”.
- **Desviación de la gestión de lo público:** Consiste en favorecer a un tercero sin el cumplimiento de requisitos legales o reglamentarios incluidos procedimientos y directrices definidas por la Procuraduría.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Valoración del Riesgo:** Resultado del cruce cuantitativo de la calificación de impacto y probabilidad, para establecer la zona donde se ubicará el riesgo.
- **Factores de riesgo:** Son las fuentes generadoras de los riesgos
- **Frecuencia:** Número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar la organización con respecto al riesgo.
- **Grupo de Valor:** Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad.
- **Identificación del Riesgo:** proceso para encontrar, enumerar y caracterizar los elementos del riesgo.
- **Impacto:** Consecuencias que puede ocasionar a la organización la materialización de un riesgo.
- **Integridad:** La propiedad de salvaguardar la exactitud y complejidad de los recursos
- **Mapa de Riesgos:** Herramienta organizacional que facilita la visualización de las diferentes etapas de la administración del riesgo; esta contempla los riesgos de gestión, corrupción y seguridad de la información
- **Mitigación:** Son todas las medidas que se llevan a cabo para limitar o reducir la materialización de un riesgo. Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó.
- **Monitorear:** Observar, analizar, verificar y evaluar los riesgos identificados, determinando el adecuado desarrollo de cada una de las etapas de administración y el nivel de cumplimiento y aplicación de los controles y acciones definidas.
- **Niveles de aceptación del riesgo:** Decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

- **Objetivos estratégicos**: Identifican la finalidad hacia la cual deben dirigirse los recursos y esfuerzos para dar cumplimiento al mandato legal aplicable a cada Entidad. El cumplimiento de estos objetivos institucionales se materializa a través de la ejecución de la planeación anual de cada entidad y deben desplegarse a los objetivos de los procesos del Sistema de Gestión de Calidad.
- **Objetivo del proceso**: Son los resultados que se espera lograr para cumplir la misión y visión. Determina el cómo logro la política trazada y el aporte que hace a los objetivos institucionales. Un objetivo es un enunciado que expresa una acción, por lo tanto, debe iniciarse con un verbo fuerte como: Establecer, identificar, recopilar, investigar, registrar, buscar. Los objetivos deben ser: medibles, realistas y se deben evitar frases subjetivas en su construcción
- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Parte Interesada:** Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad de la organización.
- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción, que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Política de Administración del Riesgo:** Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO31000 Numeral 2.4). La gestión o Administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.
- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el período de un (1) año.
- **Plan de acción:** acciones tomadas para reducir la probabilidad de ocurrencia del riesgo
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **Reducción del riesgo:** acciones que se toman para disminuir la probabilidad, las consecuencias negativas o ambas, asociadas con un riesgo, por lo general conlleva a la implementación de controles
- **Riesgos de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de corrupción-Soborno:** El soborno o cohecho es el ofrecimiento o solicitud, recibo o entrega, de regalos, préstamos, dinero o cualquier otro tipo de recurso con el propósito de obtener un beneficio particular o ventaja indebidas. El soborno se configura entre un sujeto que recibe o entrega bienes en especie o dineros a cambio de “algo”, y un sujeto que ofrece o solicita su entrega. El delito puede ser cometido por un servidor público en el ejercicio de sus funciones o una empresa o particular que busca un beneficio individual.
- **Riesgo de corrupción-Piratería:** Se refiere a la adopción por negocio de la reproducción, apropiación y distribución con fines lucrativos y a gran escala de distintos medios y contenidos (software, videos, música) de los que no posee licencia o permiso de su autor para su uso. Infracción de los derechos de propiedad intelectual e industrial.
- **Riesgo de corrupción-Fraude:** El fraude se refiere a un acto intencional de una o más personas, dentro de la administración, dirección o con los empleados o terceros, que involucra el uso del engaño para obtener una ventaja. Alteración intencional o deliberada de información, con el objeto de lograr una ventaja injusta sobre otro. Cualquier acto u omisión diseñado para engañar, que resulte en pérdidas para la victima y/o ganancias para el perpetrador.
- **Riesgo Inherente:** Nivel de riesgo propio de la entidad. Es aquel al que se enfrenta una entidad en ausencia de acciones de control para modificar su probabilidad o impacto. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo residual:** Resultado de aplicar la efectividad de los controles al riesgo inherente.

- **Riesgos de seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **Riesgo de gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias
- **Riesgo – Ejecución y administración de procesos:** Pérdidas derivadas de errores en la ejecución y administración de procesos.
- **Riesgo – Fraude externo:** Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
- **Riesgo – Fraude interno:** Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos, abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos un (1) participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
- **Riesgo – Fallas tecnológicas:** Errores de hardware, software, telecomunicaciones, interrupción de servicios básicos.
- **Riesgo – Relaciones laborales:** Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
- **Riesgo – Usuarios, productos y prácticas:** Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a estos.
- **Riesgo – Daños a activos fijos / eventos externos:** Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos / eventos externos como atentados, vandalismo, orden público
- **Uso del poder:** Consiste en aprovechar la autoridad que tiene una persona para tomar decisiones que favorezcan a un tercero.
- **Tolerancia al riesgo:** El valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

## 5. CONTENIDO

### 5.1. ALINEACIÓN CON EL MARCO ESTRATÉGICO DE LA PGN

La Política de Administración del Riesgo se encuentra alineada con el direccionamiento estratégico y la planeación institucional de la entidad, dado que se armoniza con la misión, la visión y los objetivos estratégicos.

Los riesgos se definen a nivel de cada uno de los procesos que conforman el Sistema de Gestión de Calidad - SGC de la PGN, los cuales se encuentran alineados a los objetivos estratégicos según el PLAN ESTRATÉGICO INSTITUCIONAL 2021 – 2024, cuya correlación se muestra a continuación:

**Tabla 1. Alineación Marco Estratégico PGN**

| PERSPECTIVA | OBJETIVO ESTRATEGICO | PROCESO ASOCIADO |
|---|---|---|
| **Sociedad y estado** | SE1. Optimizar la gestión de la PGN como una entidad referente por su actuación anticipatoria y vital para la efectiva gestión pública | Preventivo |
| | SE2. Aumentar la satisfacción de los usuarios respecto a los servicios que presta la PGN mediante su actuación oportuna y transparente. | Atención al ciudadano<br>Preventivo<br>Disciplinario<br>Intervención – Conciliación<br>Tecnologías de la información |

| PERSPECTIVA | OBJETIVO ESTRATEGICO | PROCESO ASOCIADO |
|---|---|---|
| | SE3. Contribuir a la garantía efectiva de derechos y preservación del patrimonio público | Preventivo<br>Disciplinario<br>Intervención |
| **Misional** | M1. Consolidar el trabajo colaborativo de las funciones misionales teniendo como enfoque la creación de valor para tener una actuación más anticipatoria y prestar un servicio de calidad a los ciudadanos | Preventivo<br>Disciplinario<br>Intervención - Conciliación |
| | M2. Afianzar la articulación interinstitucional del Ministerio Público y otras entidades del Estado para prestar una oferta de servicios integrada y oportuna a la ciudadanía. | Conocimiento e innovación<br>Tecnologías de la información<br>Atención al ciudadano |
| | M3. Acercar la PGN a la ciudadanía para el reconocimiento de su propósito misional. | Atención al ciudadano<br>Preventivo<br>Disciplinario |
| **Capacidades institucionales** | CI1. Consolidar y apropiar el modelo de gestión del conocimiento y la innovación para incrementar la productividad institucional y adaptarse a los cambios del entorno | Conocimiento e innovación<br>Tecnologías de la información |
| | CI2. Consolidar el gerenciamiento del talento humano para incentivar el cumplimiento de las funciones institucionales en cada área de la entidad | Talento humano |
| | CI3. Fomentar la cultura organizacional para mejorar la coordinación intrainstitucional y promover el sentido de apropiación institucional. | Direccionamiento y planeación institucional<br>Talento humano<br>Conocimiento e innovación |
| | CI4. Implementar el modelo de direccionamiento estratégico basado en riesgos de la gestión pública para contribuir al alcance de resultados y efectos institucionales | Direccionamiento y planeación institucional<br>Mejoramiento continuo<br>Evaluación institucional |
| **Recursos físicos y financieros** | RFF1. Asegurar la disponibilidad de las soluciones tecnológicas para funcionarios y grupos de interés que facilite la actuación de los servicios de la PGN. | Tecnologías de la información |
| | RFF2. Mejorar la planificación administrativa y financiera para el suministro oportuno y adecuado de bienes y servicios institucionales | Direccionamiento y planeación institucional<br>Administración de recursos y seguridad<br>Adquisición de bienes y servicios<br>Financiera |
| | RFF3. Fortalecer la gestión documental para acceder oportunamente a la información producida institucionalmente. | Documental<br>Tecnologías de la información |

Para la identificación de los riesgos de cada uno de los procesos, se toma como insumo:

- Acontecimientos potenciales que, de ocurrir, afectarían a la entidad.
- La probabilidad de corrupción que pueda afectar la adecuada gestión institucional.
- El contexto interno y externo de la entidad definido en el proceso “Direccionamiento y planeación institucional”, lo que permite que se tomen medidas en cumplimiento de las funciones institucionales.

## 5.2. POLÍTICA DE RIESGOS

La Política de Administración de Riesgos hace referencia al propósito de la Alta Dirección de gestionar el riesgo. Esta política debe estar alineada con la planificación estratégica de la entidad, con el fin de garantizar la eficacia de las acciones planteadas frente a los riesgos de corrupción, gestión y seguridad de la información identificados. Dentro del mapa institucional y de política de administración del riesgo de la Procuraduría General de la Nación deberán contemplarse los riesgos para que a partir de ahí se realice un monitoreo a los controles establecidos para los mismos.

***"La Procuraduría General de la Nación, con el liderazgo de la alta dirección, y la participación del Comité Institucional de Coordinación de Control Interno y con el apoyo de los líderes de procesos y sus equipos de trabajo gestionará, orientará, implementará y fortalecerá las etapas de administración de todo tipo de riesgos (gestión, corrupción, seguridad de la información), que impidan el logro de los objetivos estratégicos, institucionales y de procesos con base en las orientaciones establecidas en la Guía de Administración del riesgo definida por la PGN para el tratamiento, manejo y seguimiento de los mismos".***

.

## 5.3. ROLES Y RESPONSABILIDADES

**Figura 1. Roles y responsabilidades frente a la administración del riesgo a partir de las líneas de defensa**


El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen, de acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión, a partir de la estructuración de las líneas de defensa:

**Tabla 2. Roles y Responsabilidades Gestión del Riesgo**

| LINEAS DE DEFENSA | REPRESENTANTES | RESPONSABILIDADES |
|---|---|---|
| **Línea Estratégica** | Comité Institucional de Coordinación de Control Interno<br><br>Procurador(a) | Define el marco general y su control para la gestión del riesgo y supervisa su cumplimiento.<br><br>Así mismo, la Alta Dirección y el equipo directivo, a través del Comité Institucional de Coordinación de Control Interno, deben evaluar y dar línea sobre la administración de los riesgos al Comité Institucional de Gestión y |

| LINEAS DE DEFENSA | REPRESENTANTES | RESPONSABILIDADES |
|---|---|---|
| | General de la Nación.<br><br>Viceprocurador(a) General de la Nación. | Desempeño a través de las siguientes actividades:<br><br>▪ Revisar los cambios en el Contexto Estratégico y como estos pueden generar nuevos riesgos.<br>▪ Aprobar las directrices para la administración del riesgo en la Entidad, materializadas en la política de administración de riesgos y definidas en la presente guía.<br>▪ Establecer los recursos técnicos, financieros y de talento humano necesarios para llevar a cabo la implementación de la Política de Administración del Riesgo, con base en los reportes de la primera y segunda línea.<br>▪ Coordinar la revisión anual de la Política de Administración del Riesgo.<br>▪ Hacer seguimiento al menos una vez al año y cuando se considere necesario en el Comité Institucional de Coordinación de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo, los resultados de las evaluaciones realizadas por la Oficina de Control Interno o quien haga sus veces y a los eventos de riesgos que se hayan materializado en la entidad, incluyendo los riesgos de corrupción.<br><br>La Alta Dirección, representada en el Comité Institucional de Coordinación de Control Interno es la responsable de la aprobación de la política de administración del riesgo. |
| **Primera Línea** | Los líderes, sus equipos y/o responsables de los procesos. | Controla la gestión del riesgo de su proceso a través de su identificación, análisis, valoración, monitoreo e implementación de acciones de mejora.<br><br>De igual manera, los líderes o responsables de los procesos deben realizar el seguimiento del cumplimiento de los objetivos institucionales y sus procesos a través de las siguientes actividades:<br><br>▪ Dar a conocer a su equipo de trabajo los lineamientos determinados en la Política de Administración del Riesgo.<br>▪ Realizar la identificación, análisis, evaluación y valoración de los riesgos de sus respectivos procesos en el formato establecido para tal fin.<br>▪ Determinar y aprobar los contenidos de los mapas de riesgos de los procesos a su cargo.<br>▪ Realizar la socialización y divulgación de su mapa de riesgo por proceso al interior de sus respectivos equipos de trabajo, lo anterior contando con el apoyo de los gestores en cada proceso.<br>▪ Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en el Sistema de Gestión de Calidad.<br>▪ Revisar cada cuatro meses la ejecución de sus controles y el cumplimiento de las acciones complementarias al control.<br>▪ Actualizar su mapa de riesgos (para incluir, reformular o eliminar riesgos) considerando la dinámica de la entidad.<br>▪ Notificar a la Oficina de Planeación las actualizaciones del mapa de riesgos en el marco de la revisión cuatrimestral, para la modificación de este.<br>▪ Informar a la Oficina de Planeación cualquier inquietud o inconveniente presentado en el desarrollo de la administración de sus riesgos.<br>▪ Supervisar los controles del día a día.<br><br>Adicionalmente los gestores deberán:<br>▪ Informar a la oficina de planeación (segunda línea) y la Oficina de control |

| LINEAS DE DEFENSA | REPRESENTANTES | RESPONSABILIDADES |
|---|---|---|
| | | interno (tercera línea) sobre los riesgos materializados.<br>▪ Apoyar en la identificación, análisis, valoración y administración de los riesgos de los procesos en los cuales la dependencia interviene.<br>▪ Apoyar en la definición de las acciones correctivas o de mejora para mitigar los riesgos que sean responsabilidad del proceso.<br>▪ Proporcionar evidencias dentro de los plazos establecidos para el reporte de la información a la Oficina de planeación y la Oficina de control interno. |
| **Segunda Línea** | Oficina de Planeación con apoyo de los gestores de procesos | Controla que la gestión del riesgo implementado por parte de la primera línea de defensa esté diseñada apropiadamente y funcione según lo preestablecido.<br>▪ Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones del caso.<br>▪ Esta oficina evaluará la eficacia tanto para los controles como para planes de acción; cuatrimestralmente el registro del monitoreo que hace como segunda línea de defensa.<br>▪ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento de los objetivos.<br><br>Por otra parte, la Oficina de Planeación realizará las siguientes actividades:<br>▪ Generar la metodología para la administración del riesgo de la Entidad, y a su vez liderar, coordinar y capacitar en su aplicación.<br>▪ Anualmente revisará la Política de Administración del Riesgo y la actualizará en caso de requerirse para su respectiva presentación y aprobación ante la Alta Dirección a través del Comité Institucional de Coordinación de Control Interno.<br>▪ Divulgar y socializar la Política de Administración del Riesgo y la Metodología Integrada de Administración del Riesgo.<br>▪ Asesorar técnicamente a los procesos, en los casos que se requiera, en la formulación de los mapas de riesgos. Esta asesoría debe ser entendida como la orientación en la aplicación de la metodología establecida.<br>▪ Asesorar a la línea estratégica en el análisis del contexto interno y externo.<br>▪ Monitorear los riesgos cada cuatro meses en el marco del Plan Anticorrupción y Atención al Ciudadano -PAAC e informar los resultados a la Oficina de Control Interno.<br>▪ Solicitar a la primera línea de defensa el plan de tratamiento de los riesgos materializados, el cual debe ser informado a la tercera línea de defensa. |

| LINEAS DE DEFENSA | REPRESENTANTES | RESPONSABILIDADES |
|---|---|---|
| **Tercera Línea** | Oficina de Control Interno - OCI | La OCI debe proveer la evaluación de manera independiente y objetiva sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades a través de las siguientes actividades:<br>▪ Apoyar, en coordinación con la Oficina de Planeación, en la difusión y la implementación de la Política de Administración del Riesgo en toda la entidad fortaleciendo la cultura de prevención.<br>▪ Apoyar a los líderes de procesos facilitando la aclaración de términos o técnicas para el diligenciamiento de los mapas de riesgo en cada una de sus etapas, en cumplimiento del rol de enfoque hacia la prevención.<br>▪ Analizar, dentro de sus procesos de auditoría, el diseño, idoneidad y efectividad de los controles, determinando si son o no adecuados para prevenir o mitigar los riesgos de los procesos.<br>▪ Hacer evaluación y seguimiento al cumplimiento de la política, al menos una vez al año.<br>▪ Adelantar el seguimiento al Mapa de Riesgos de Corrupción y gestión cada cuatro meses bajo la metodología seleccionada. Esta evaluación se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.<br>▪ Informar sobre la efectividad de la Gestión de Riesgos al Comité Institucional de Coordinación de Control Interno.<br>▪ Evaluar la eficacia de los planes de mejoramiento como resultado de las auditorias efectuadas, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.<br>▪ Hacer seguimiento a los planes de tratamiento de aquellos riesgos materializados.<br>▪ Recomendar mejoras sobre la política de gestión del riesgo. |

Para los riesgos de seguridad de la información, la Entidad designará un responsable el cual debe pertenecer a un área que haga parte de la Ata Dirección o línea Estratégica, cuyas funciones frente a la gestión del riesgo de Seguridad de la información son:

- Definir el procedimiento para la identificación y valoración de activos.
- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, análisis, evaluación y tratamiento).
- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos.
- Apoyar en el seguimiento a los planes de tratamiento de riesgos definidos.
- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.

Responsabilidades generales de los servidores públicos y contratistas:

- Participar de manera directa en la identificación, análisis y valoración de los riesgos asociados a su gestión.
- Implementar los controles requeridos para la gestión del riesgo asociados a los procesos en los que participa.
- Desarrollar las acciones de tratamiento para la mitigación de los riesgos identificados.
- Efectuar el monitoreo de los controles de acuerdo con las funciones que realiza, en los tiempos estipulados.

- Informar a su superior inmediato o responsable de proceso sobre la posibilidad de generación de nuevos riesgos o la materialización de un riesgo identificado.
- Participar en los ejercicios de sensibilización sobre la Política de Administración.

### 5.4. FORMULACIÓN Y/O ACTUALIZACIÓN DEL MAPA DE RIESGOS Y OPORTUNIDADES

Para la identificación, valoración, monitoreo y seguimiento del riesgo se relacionan a continuación las instrucciones generales para el diligenciamiento del Mapa de riesgos de cada proceso del SGC de la PGN.

En relación con la identificación de oportunidades, estas se tratarán según lo definido en el procedimiento “MC-P-02 Gestión de acciones correctivas, preventivas y oportunidades de mejora”.

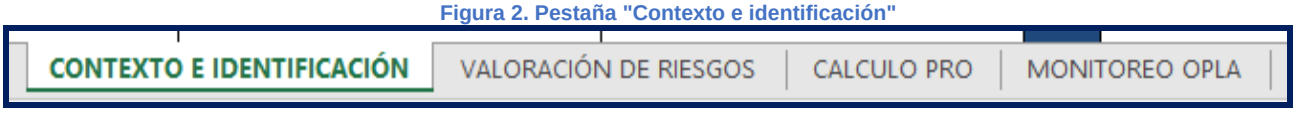
#### 5.4.1. Identificación del riesgo

La identificación del riesgo estará asociada a aquellos eventos o situaciones que pueden influir negativa o positivamente en el normal desarrollo de los objetivos del proceso. Para diligenciar el mapa de riesgos de cada proceso, se diligenciarán los siguientes campos dentro de la herramienta, así:

##### 5.4.1.1. Establecimiento del Contexto

El primer paso para iniciar el proceso de identificación de riesgos en la PGN es el establecimiento del contexto, para lo cual, en la herramienta de mapa de riesgos se ha dispuesto la pestaña “Contexto e identificación”, como se observa en la siguiente figura:

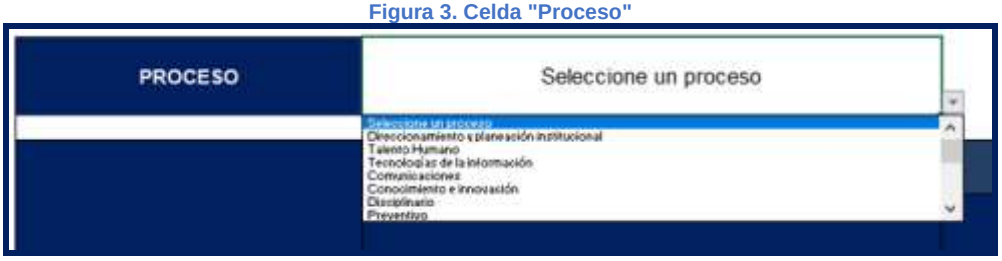
**Figura 2. Pestaña "Contexto e identificación"**




**A. Proceso**

Teniendo en cuenta el mapa de procesos de la PGN, se debe seleccionar en la celda denominada “PROCESO”, el nombre del proceso de la lista desplegable (Ver Figura 3) para el cual se identificarán los riesgos, así:

**Figura 3. Celda "Proceso"**

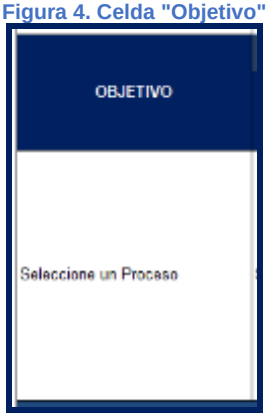



Es importante resaltar que todos los procesos institucionales formalmente definidos para la PGN deben contar con la formulación de su mapa de riesgos.

**B. Objetivo del Proceso**

Una vez se haya seleccionado el proceso sobre el cual se identificarán los riesgos, automáticamente la herramienta establecerá el objetivo correspondiente, el cual ha sido documentado previamente en la caracterización del proceso, en la celda que se denomina “Objetivo”. (Ver Figura 4)

**Figura 4. Celda "Objetivo"**

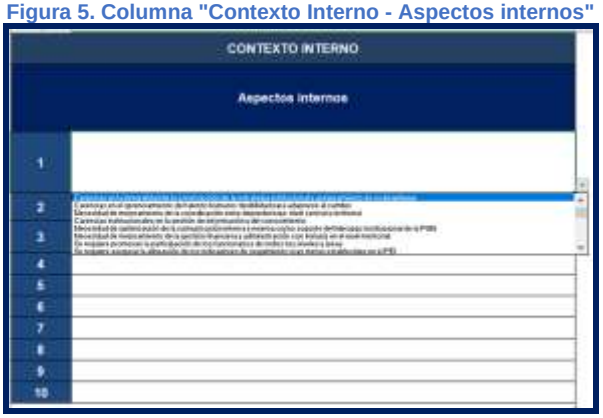



**C. Contexto Interno y Externo**

Posteriormente, para definir el contexto interno y externo del proceso, se debe tomar en consideración el Contexto Estratégico analizado e incluido dentro del Plan Estratégico Institucional vigente, en donde se pueden identificar tanto aspectos internos como externos de la PGN, de esta manera, en la herramienta se presentan dos columnas denominadas así:

- **Columna “Contexto interno”:** En esta se ha dispuesto una lista desplegable a partir de la cual se podrán seleccionar cada uno de los aspectos internos relevantes para el proceso, así como complementar los que se consideren importante incluir, analizando y determinando las características y aspectos esenciales del proceso tales como estructura organizacional, funciones, responsabilidades, políticas, objetivos, estrategias implementadas, recursos y conocimientos con que se cuenta. (Ver Figura 5)

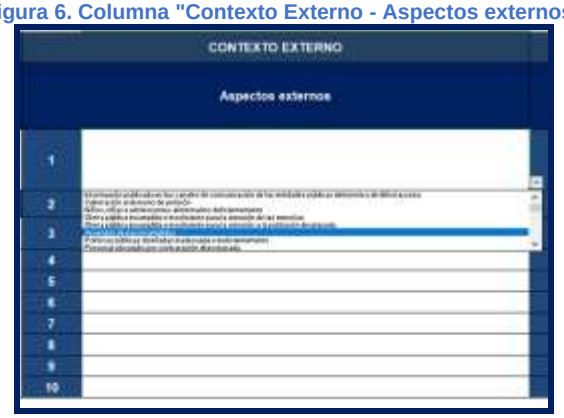
**Figura 5. Columna "Contexto Interno - Aspectos internos"**




- **Columna “Contexto externo”:** En esta se ha dispuesto una lista desplegable a partir de la cual se podrán seleccionar cada uno de los aspectos externos relevantes para el proceso, así como complementar los que se consideren importante incluir, analizando y determinando las características y aspectos esenciales del

proceso tales como factores económicos, medioambientales, políticos, sociales, tecnológicos y de comunicación externa. (Ver Figura 6)

**Figura 6. Columna "Contexto Externo - Aspectos externos"**



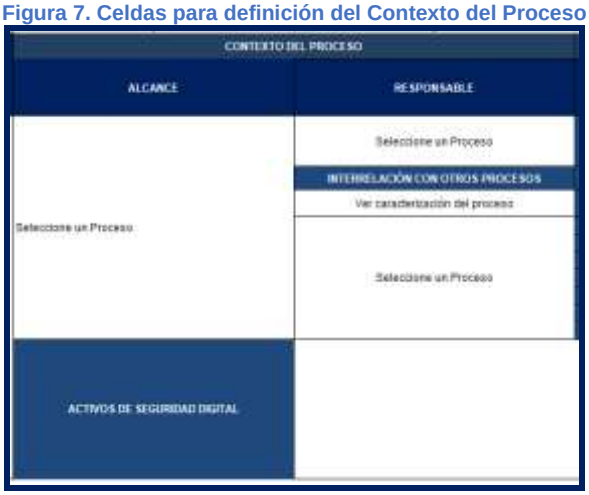

**D. Contexto del Proceso**

De igual manera, al escoger el proceso sobre el cual se efectuará la identificación, automáticamente la herramienta establece la información contextual del mismo, permitiendo analizar y considerar las características o aspectos de este, así como sus interrelaciones con factores como (Ver Figura 7):

- **Alcance:** Conforme a la caracterización del proceso se define automáticamente en este campo el texto correspondiente a la definición de la actividad inicial y final en concordancia con el objetivo del proceso, por lo cual, este campo no requiere edición adicional.

- **Responsable:** De igual forma que para el punto anterior, la herramienta define automáticamente en este campo al líder(es) del proceso, es decir, el cargo de quien tiene la autoridad para la toma de decisiones en el proceso, así como la aprobación de la versión final del mapa de riesgos.
- **Interrelación con otros procesos:** En este campo encontraremos la frase “Ver caracterización del proceso”, así como el enlace de acceso a la misma, la cual se diligencia de forma automática, conforme a los factores anteriores.
- **Activos de seguridad de la información:** En este campo se diligenciará lo correspondiente a los activos de información de cada proceso, cuyos datos se encuentran disponible en el enlace presentado.

**Figura 7. Celdas para definición del Contexto del Proceso**




**E. Identificación de factores de riesgo**

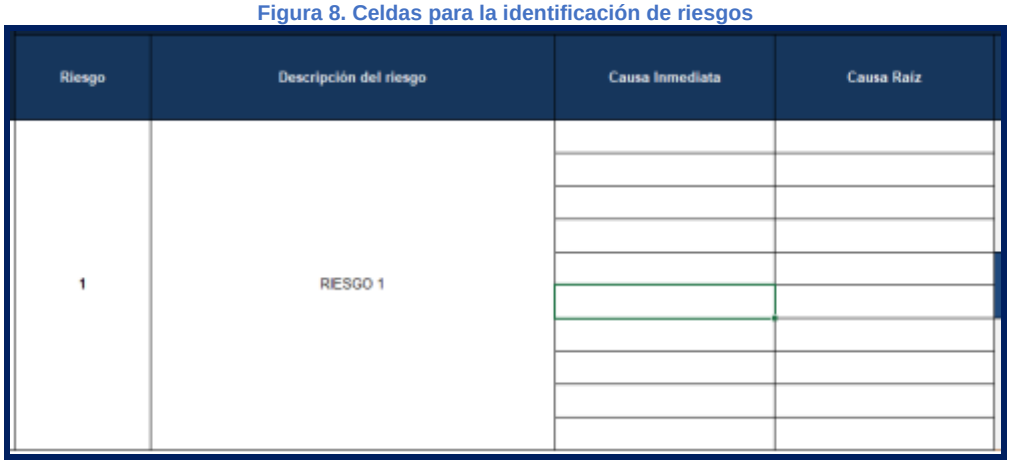
Una vez finalizado el análisis del establecimiento del contexto del proceso, se pasa a la pestaña “Valoración de riesgos”, donde se inicia el proceso de identificación de los riesgos y oportunidades, que impactan el cumplimiento del objetivo del proceso y que se pueden articular con las acciones de control ejecutadas a través de las actividades o procedimientos existentes en el mismo.

Así pues, al momento de identificar y redactar los riesgos para el proceso, se deben considerar las siguientes premisas:

- No describir como riesgos omisiones ni desviaciones del control. **Ejemplo:** errores en la liquidación de la nómina por fallas en los procedimientos existentes.
- No describir causas como riesgos. **Ejemplo:** inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
- No describir riesgos como la negación de un control. **Ejemplo:** retrasos en la prestación del servicio por no contar con digiturno para la atención.
- No existen riesgos transversales, lo que pueden existir son causas transversales. Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes. **Ejemplo:** pérdida de expedientes.

**Nota:** si durante el establecimiento de los riesgos del proceso se identifican oportunidades de mejora, se deberán seguir los lineamientos dictados en el procedimiento MC-P-02. Gestión de acciones correctivas, preventivas y de mejora.

**Figura 8. Celdas para la identificación de riesgos**



| Riesgo | Descripción del riesgo | Causa Inmediata | Causa Raíz |
|---|---|---|---|
| 1 | RIESGO 1 | | |

Así pues, en el marco del proceso se debe iniciar analizando y respondiendo las preguntas que orientan la identificación de los riesgos, así:

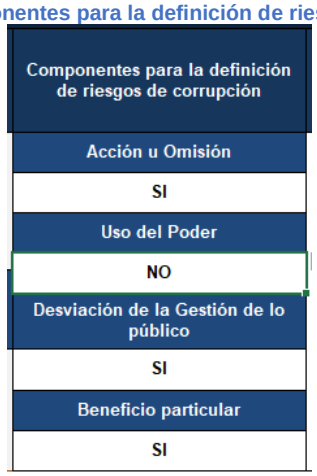
- **Descripción del Riesgo:** Se debe iniciar con la pregunta "¿Qué puede suceder?", donde se parte del análisis sobre los posibles eventos que pueden ocasionar el incumplimiento del objetivo del proceso, toda vez que a través de la resolución de esta pregunta se define a su vez el área de impacto, es decir la consecuencia económica (presupuestal) o reputacional a la cual se ve expuesta la PGN. En esta celda se registrará la redacción del riesgo, donde se concatenan las causas inmediatas y las causas raíz, así:

  - Para riesgos de gestión y de seguridad de la información, conforme a la estructura propuesta por el DAFP, se debe iniciar con la frase "Posibilidad de afectación económica/reputacional (…)", continúa con la palabra "por", describiendo en este punto el ¿cómo?, que hace referencia a la afectación definida en la primera pregunta. Así mismo, específicamente para los riesgos de seguridad de la información se deberá indicar el activo de información sobre el cual se genera la afectación. Y la redacción finaliza con la palabra "debido a", describiendo en este punto el ¿por qué?, que hace referencia a la afectación definida en la primera pregunta.


  - Para riesgos de corrupción, es necesario que su redacción exprese los componentes de su definición: acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado. Por lo anterior, se establece en la herramienta las celdas que presentan los componentes mencionados (Ver Figura 9); en cada uno de ellos se despliega una lista donde se elige "SI" o "NO" en el caso de que aplique en la definición del riesgo.

Cuando un riesgo cumple con los cuatro componentes precisados, se clasificará automáticamente como un riesgo de corrupción; si no, corresponde a un riesgo de gestión o seguridad de la información. Es necesario que su redacción finalice con la frase "*para beneficio propio o de un tercero*".

**Figura 9. Celdas "Componentes para la definición de riesgos de corrupción"**




- **Causa Inmediata:** en esta columna se identifican las circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las cuales no constituyen la causa principal o base para que se presente el riesgo. Se puede orientar el ejercicio de identificación respondiendo las preguntas ¿Por qué puede suceder? y ¿Mediante qué puede suceder? Dichas respuestas se registrarán en las celdas denominadas "Causa Inmediata", conforme a lo expuesto para cada tipología de riesgos (Ver Figura 8).

- **Causa Raíz:** en esta columna se identifican las causas principales que pueden generar el riesgo y son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa y cada causa tendrá su respectivo control. Dichas respuestas se registrarán en las celdas denominadas "Causa Raíz", conforme a lo expuesto para cada tipología de riesgos (Ver Figura 8).

### 5.4.2. Valoración del riesgo

Una vez finalizado el proceso de identificación del riesgo, en la misma pestaña se continuará la valoración del riesgo, para lo cual se diligenciarán los siguientes campos:

#### 5.4.2.1. Clasificación

En la celda denominada "Clasificación", se deberá seleccionar la tipología del riesgo que ha sido identificado, conforme a tres categorías: gestión, corrupción o seguridad de la información. (Ver Figura 10).

**Figura 10. Celda "Clasificación"**


**Nota:** una vez definida la clasificación del riesgo, en la herramienta se activará la tipología de riesgo correspondiente.

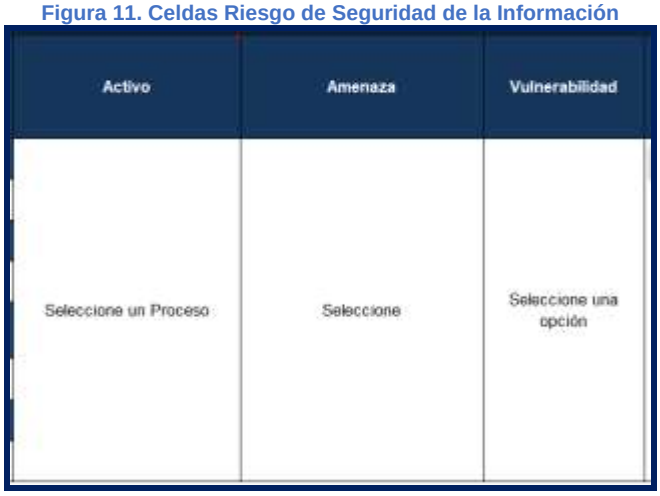
- **Tipo:** Al seleccionar la clasificación del riesgo, se deben considerar las definiciones presentados en el numeral 4. “Definiciones y siglas” de la presente guía, la cual es consistente con la identificación preliminar del mismo. De esta manera, conforme a esta tipología los riesgos cuentan con las siguientes opciones:

**Tabla 3. Tipologías de riesgo**

| CLASIFICACIÓN | TIPO |
|---|---|
| Gestión | ▪ Ejecución y administración de proceso<br>▪ Fraude externo<br>▪ Fraude interno<br>▪ Fallas tecnológicas<br>▪ Relaciones laborales<br>▪ Usuarios, productos y prácticas<br>▪ Daño a activos fijos/Eventos externos |
| Corrupción | ▪ Soborno<br>▪ Piratería<br>▪ Fraude |
| Seguridad de la información | ▪ Pérdida de confidencialidad<br>▪ Pérdida de integridad<br>▪ Pérdida de disponibilidad |

- **Celdas Riesgo de Seguridad de la Información:** si el riesgo identificado es clasificado como riesgo de seguridad de la información, se deberán diligenciar las celdas “Activo”, “Amenaza” y “Vulnerabilidad”, con el fin de determinar el activo afectado, la situación que puede ocasionar el daño y las situaciones asociadas a la amenaza que se activan y que pueden ocasionar el daño al activo. En caso de no corresponder a esta tipología, se seleccionará la opción “No aplica”.

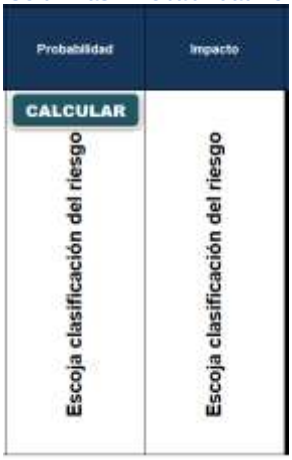
**Figura 11. Celdas Riesgo de Seguridad de la Información**




### 5.4.2.2. Valoración Zona de riesgo inherente

Para estimar la zona de riesgo inicial o de riesgo inherente es necesario establecer la probabilidad y el impacto del riesgo identificado, para lo cual la herramienta cuenta con dos columnas denominadas “Probabilidad” e “Impacto”, donde se dirige el ejercicio hacia los campos de cálculo programados y que deberán ser desarrollados como se explica a continuación. (Ver Figura 12)

**Figura 12. Columnas "Probabilidad" e "Impacto"**



Así pues, se entiende por "Probabilidad" como la posibilidad de su ocurrencia del riesgo y por "Impacto" como el efecto ocasionado por la ocurrencia del riesgo, que al confrontarse permiten calcular la Zona de Riesgo Inherente. Esta valoración se calcula de acuerdo con la tipología del riesgo, así:

**A. Riesgos de gestión y seguridad de la información**

- **Probabilidad**

Para esta tipología de riesgos, la probabilidad corresponde al número de veces que puede presentarse el riesgo durante el periodo de un (1) año, teniendo como criterios para definir el nivel de probabilidad los siguientes:

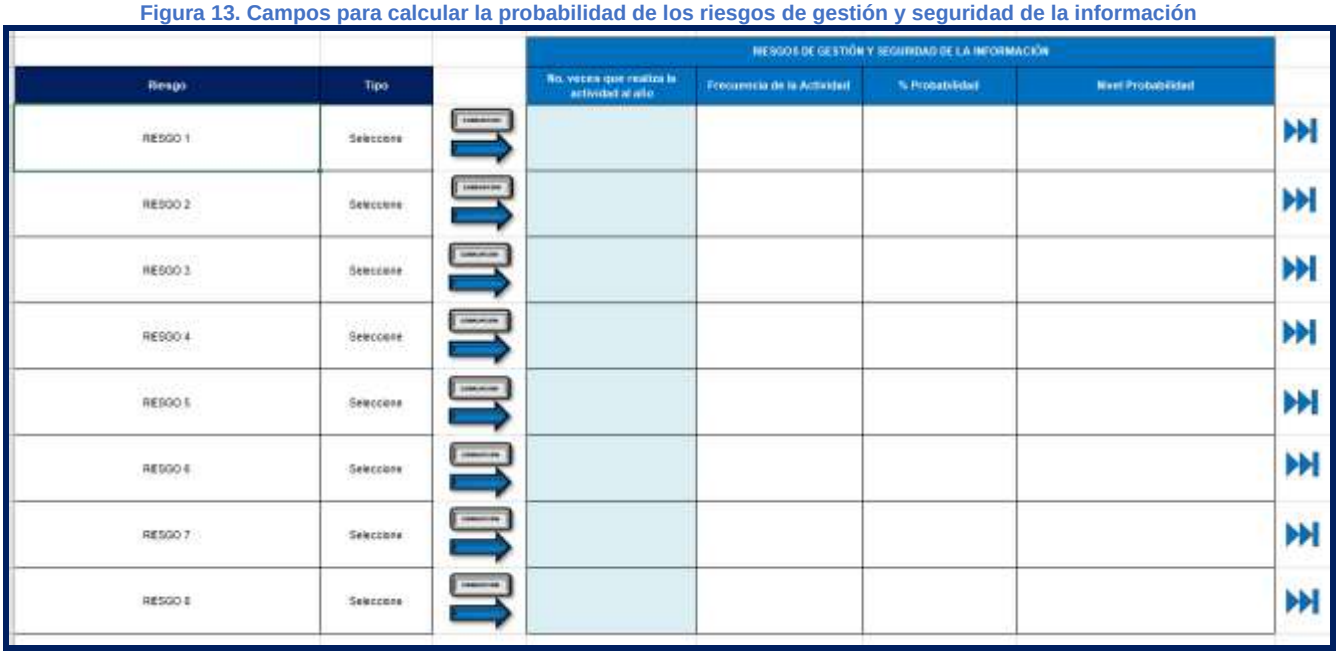
**Tabla 4. Criterios para definir el nivel de probabilidad - Riesgos de gestión y seguridad de la información**

| NIVEL | FRECUENCIA DE LA ACTIVIDAD | PROBABILIDAD |
|---|---|---|
| Muy Baja | La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año | 20% |
| Baja | La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año | 40% |
| Media | La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año | 60% |
| Alta | La actividad que conlleva el riesgo se ejecuta mínimo 501 veces al año y máximo 5.000 veces por año | 80% |
| Muy Alta | La actividad que conlleva el riesgo se ejecuta más de 5.001 veces por año | 100% |

**Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5. DAFP. Diciembre de 2020**

Para establecer la probabilidad del riesgo identificado, dé clic en el botón CALCULAR, el cual lo dirigirá a una tabla con los siguientes campos:

**Figura 13. Campos para calcular la probabilidad de los riesgos de gestión y seguridad de la información**



Así pues, teniendo en cuenta las columnas presentadas en la figura 13, se diligenciarán de la siguiente forma:

- **Riesgo:** corresponde a la descripción del riesgo identificado, este campo es diligenciado automáticamente por la herramienta.
- **Tipo:** corresponde a la clasificación del riesgo identificado, este campo es diligenciado automáticamente por la herramienta
- **N° veces que realiza la actividad al año:** teniendo en cuenta la explicación anterior, se debe establecer un número entero (sin decimales), a partir del cual la herramienta calcula el nivel de probabilidad.
- **Frecuencia de la actividad:** conforme al número registrado en la columna "*N° veces que realiza la actividad al año*", la herramienta diligencia este campo automáticamente, por lo cual no requiere edición adicional.
- **% probabilidad:** conforme al número registrado en la columna "*N° veces que realiza la actividad al año*", la herramienta diligencia este campo automáticamente, por lo cual no requiere edición adicional.
- **Nivel probabilidad:** conforme al número registrado en la columna "*N° veces que realiza la actividad al año*", la herramienta diligencia este campo automáticamente, por lo cual no requiere edición adicional.

Este nivel de probabilidad se verá reflejado en la columna "Probabilidad" de la pestaña "Valoración de riesgos" de forma automática, por lo cual, no requiere un diligenciamiento adicional. Una vez se haya efectuado la calificación de la probabilidad del riesgo, se debe dar clic en el botón ⏭, para continuar con el ejercicio de valoración de impacto.

➢ **Impacto**

Para esta tipología de riesgos, el impacto se define bajo dos variables principales: impactos económicos e impactos reputacionales, teniendo como criterios para definir el nivel de impacto los siguientes:

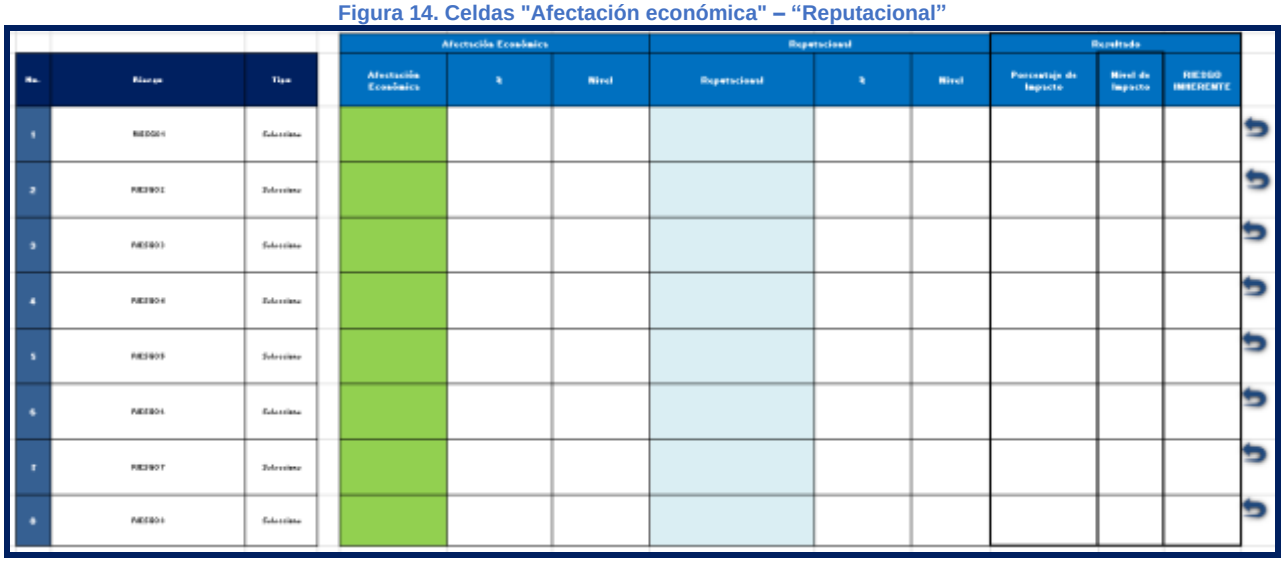
**Tabla 5. Criterios para definir el nivel de impacto - Riesgos de gestión y seguridad de la información**

| NIVEL | % IMPACTO | AFECTACIÓN_ECONÓMICA | REPUTACIONAL |
|---|---|---|---|
| Leve | 20% | Menor a 10 SMLMV | El riesgo afecta la imagen de algún área de la organización. |
| Menor | 40% | Entre 10 y 50 SMLMV | El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores. |
| Moderado | 60% | Entre 51 y 100 SMLMV | El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos. |
| Mayor | 80% | Entre 101 y 500 SMLMV | El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal. |
| Catastrófico | 100% | Mayor a 500 SMLMV | El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país |

**Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5. DAFP. Diciembre de 2020**

Para establecer el impacto del riesgo identificado, una vez se haya efectuado la calificación de la probabilidad, se debe dar clic en el botón ⏭, que te dirigirá a los siguientes campos:

**Figura 14. Celdas "Afectación económica" – "Reputacional"**



Así pues, teniendo en cuenta las columnas presentadas en la figura 14, se diligenciarán de la siguiente forma:

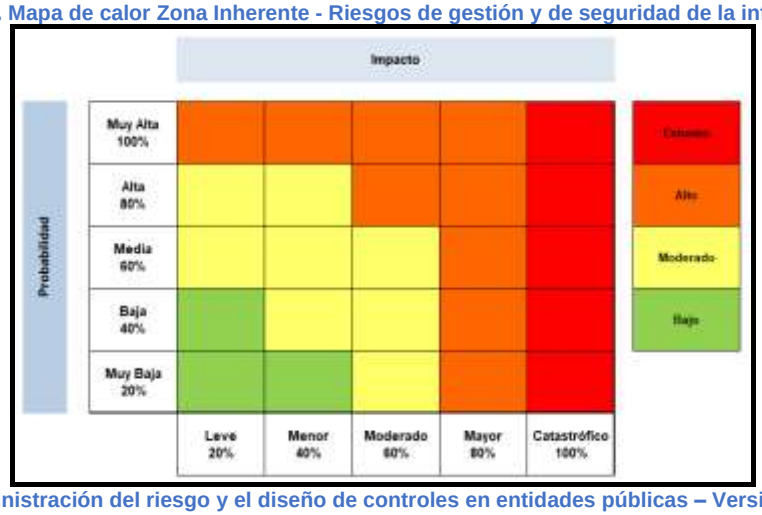
- **Afectación económica:** teniendo en cuenta los criterios establecidos en la Tabla 5, se debe seleccionar de la lista desplegable el nivel de afectación conforme al análisis efectuado.
- **"%" y "Nivel":** conforme a la afectación seleccionada en la columna "*Afectación económica*", la herramienta diligencia este campo automáticamente, por lo cual no requiere edición adicional.
- **Reputacional:** teniendo en cuenta los criterios establecidos en la Tabla 5, se debe seleccionar de la lista desplegable la afectación reputacional conforme al análisis efectuado.
- **"%" y "Nivel":** conforme a la afectación seleccionada en la columna "*Reputacional*", la herramienta diligencia este campo automáticamente, por lo cual no requiere edición adicional.

Este nivel de impacto se verá reflejado en la columna "Impacto" de la pestaña "Valoración de riesgos" de forma automática, por lo cual, no requiere un diligenciamiento adicional.

- **Zona de riesgo inherente:**

Es importante ilustrar como se estima la zona de riesgo inicial o inherente en los riesgos de gestión y de seguridad de la información, para lo cual, los valores de la probabilidad y del impacto se combinan definiendo cuatro (4) zonas de severidad en la matriz de calor así:

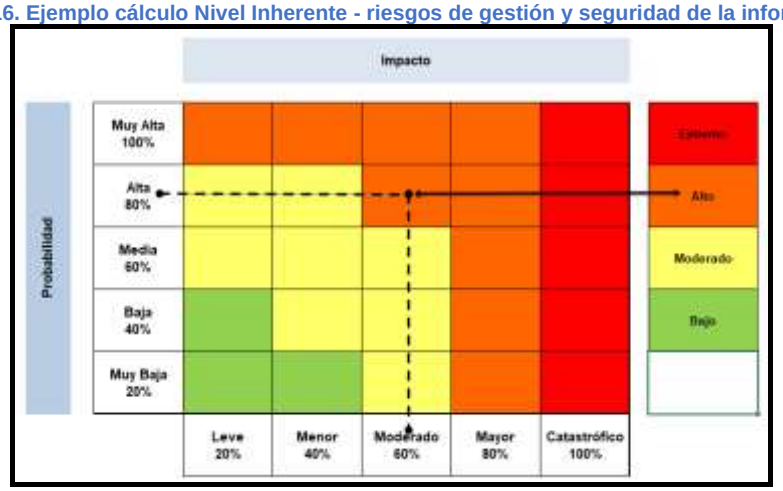
**Figura 15. Mapa de calor Zona Inherente - Riesgos de gestión y de seguridad de la información**




**Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5. DAFP. Diciembre de 2020**

Así pues, con al análisis previo referente a la determinación de la probabilidad y el impacto, la herramienta calculará el nivel del riesgo efectuando el cruce entre estos dos resultados, así:

**Figura 16. Ejemplo cálculo Nivel Inherente - riesgos de gestión y seguridad de la información**




De esta manera, una vez se haya efectuado la calificación de la probabilidad del riesgo, la herramienta automáticamente calcula conforme al mapa de calor la zona de riesgo inherente en que este se valora y lo registra en el campo correspondiente.

**B. Riesgos de corrupción**

Para efectuar el análisis, la probabilidad de ocurrencia puede ser medida con criterios de frecuencia si se ha materializado el riesgo y, en caso contrario, debe ser medida con criterios de factibilidad, existiendo cinco (5) niveles representados así:

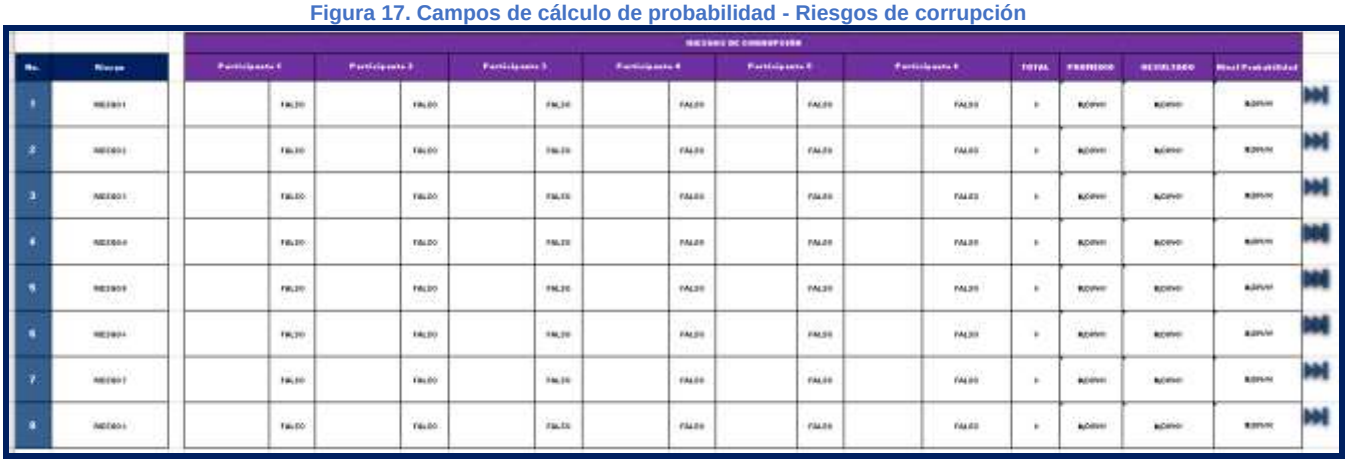
**Tabla 6. Niveles de probabilidad - Riesgos de corrupción**

| NIVEL | FRECUENCIA DE LA ACTIVIDAD | FRECUENCIA |
|---|---|---|
| Rara vez | El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales) | No se ha presentado en los últimos cinco años |
| Improbable | El evento puede ocurrir en algún momento | Al menos una vez, en los últimos cinco años |
| Posible | El evento podrá ocurrir en algún momento | Al menos una vez en los últimos dos años |
| Probable | Es viable que el evento ocurra en la mayoría de las circunstancias | Al menos una vez en el último año |
| Casi seguro | Se espera que el evento ocurra en la mayoría de las circunstancias | Más de una vez al año |

**Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018. DAFP.**

Para establecer la probabilidad del riesgo identificado, dé clic en el botón  , el cual lo dirigirá a una tabla con los siguientes campos:

**Figura 17. Campos de cálculo de probabilidad - Riesgos de corrupción**



Así pues, teniendo en cuenta las columnas presentadas en la figura 17, se diligenciarán de la siguiente forma:

- **Riesgo:** corresponde al riesgo sobre el cual se encuentra efectuando la actividad de valoración, por lo cual se define de forma automática en la herramienta y no requiere edición.
- **Columnas "Participante":** se encuentran ubicados los espacios para la participación de seis (6) integrantes del proceso, cada uno elegirá una columna donde, conforme a la lista desplegable, elegirá el nivel de frecuencia de la actividad y se establecerá un puntaje automáticamente en la herramienta. Con el promedio de dichos puntajes propuestos por los participantes, se determina la probabilidad del riesgo. (Ver Tabla 6).

Este nivel de probabilidad se verá reflejado en la columna “Probabilidad” de la pestaña “Valoración de riesgos” de forma automática, por lo cual, no requiere un diligenciamiento adicional. Una vez se haya efectuado la calificación de la probabilidad del riesgo, se debe dar clic en el botón ⏭, para continuar con el ejercicio de valoración de impacto.

- **Impacto**

En esta tipología de riesgo, para establecer el impacto de este, el respectivo análisis se realiza teniendo en cuenta los siguientes niveles:

**Tabla 7. Niveles de impacto - Riesgos de corrupción**

| CATEGORÍA | NIVEL DE RIESGO |
|---|---|
| 3 | Moderado |
| 4 | Mayor |
| 5 | Catastrófico |

**Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018. DAFP.**

Así pues, una vez se haya efectuado la calificación de la probabilidad, se debe dar clic en el botón ⏭, que lo dirigirá a la resolución del siguiente cuestionario correspondiente (Ver Figura 18), así:

- ¿Afecta al grupo de funcionarios del proceso?
- ¿Afectar el cumplimiento de metas y objetivos de las dependencias?
- ¿Afectar el cumplimiento de la misión de la entidad?
- ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?
- ¿Genera pérdida de confianza de la entidad, afectando su reputación?
- ¿Genera pérdida de recursos económicos?
- ¿Afecta la generación de productos o la prestación de servicios?
- ¿Da lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o los recursos públicos?
- ¿Generar pérdida de información de la entidad?
- ¿Generar intervención de los órganos de control, de la fiscalía u otro Ente?
- ¿Dar lugar a procesos sancionatorios?
- ¿Dar lugar a procesos disciplinarios?
- ¿Dar lugar a procesos fiscales?
- ¿Dar lugar a procesos penales?
- ¿Generar pérdida de credibilidad de la entidad?
- ¿Generar pérdida de credibilidad del sector?
- ¿Ocasionar lesiones físicas o pérdida de vidas humanas?
- ¿Afectar la imagen regional?
- ¿Afectar la imagen nacional?
- ¿Generar daño ambiental?

Una vez sea diligenciado el cuestionario, la herramienta calculará automáticamente el impacto del riesgo, así:

- Responder afirmativamente de una (1) a cinco (5) preguntas genera un impacto “Moderado”
- Responder afirmativamente de seis (6) a once (11) preguntas genera un impacto “Mayor”
- Responder afirmativamente de doce (12) a veinte (20) preguntas genera un impacto “Catastrófico”

**Figura 18. Campos de cálculo de impacto - Riesgos de corrupción**

**Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018. DAFP**

Este nivel de impacto se verá reflejado en la columna “Impacto” de la pestaña “Valoración de riesgos” de forma automática, por lo cual, no requiere un diligenciamiento adicional.

- **Zona de riesgo inherente:**

Para estimar la zona inicial o inherente en los riesgos de corrupción, los valores de la probabilidad y del impacto se multiplicarán para establecer el nivel de severidad de acuerdo con la siguiente matriz de calor así:

**Figura 19. Mapa de calor Zona Inherente - Riesgos de corrupción**


**Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018. DAFP**

Es importante destacar que los riesgos de corrupción nunca podrán ser calificados en una zona de riesgo inherente baja, debido a su naturaleza, por esta razón, como se observa en la Figura 19, no se efectúa el cruce para dichas categorías.

De esta manera, una vez se haya efectuado la calificación de la probabilidad del riesgo, la herramienta automáticamente calcula conforme al mapa de calor la zona de riesgo inherente en que este se valora y lo registra en el campo correspondiente.

**5.4.2.3. Acciones de control**

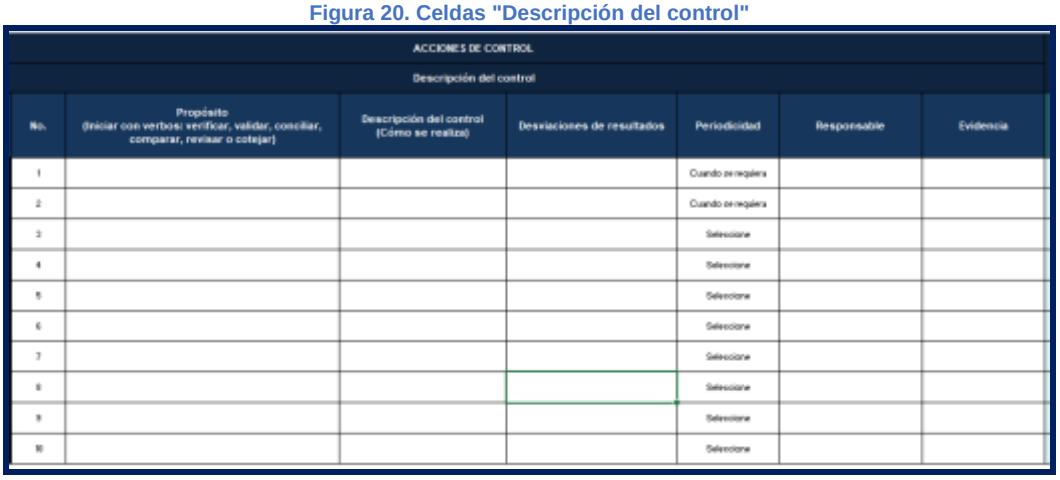
En primer lugar, para adelantar esta etapa se hace necesario tener en cuenta los puntos de control (controles) existentes en los diferentes procedimientos del proceso con el fin de analizar su aplicabilidad y efectividad.

Para establecer los controles, la herramienta cuenta con una sección denominada "*Acciones de control",* donde se establecen las columnas para identificar y registrar hasta diez (10) controles asociados a las causas identificadas en la pestaña de "Contexto e identificación".

Cabe anotar que cada causa debe tener su respectivo control, de manera separada. En caso tal de que un control puede mitigar dos o más causas, se repite el control, asociado de manera independiente a la causa especifica.

Para la definición de controles se debe establecer los siguientes componentes (Ver Figura 20):

**Figura 20. Celdas "Descripción del control"**



| ACCIONES DE CONTROL | | | | | | |
|---|---|---|---|---|---|---|
| Descripción del control | | | | | | |
| No. | Propósito (Iniciar con verbos: verificar, validar, conciliar, comparar, revisar o cotejar) | Descripción del control (Cómo se realiza) | Desviaciones de resultados | Periodicidad | Responsable | Evidencia |
| 1 | | | | Cuando se requiera | | |
| 2 | | | | Cuando se requiera | | |
| 3 | | | | Seleccione | | |
| 4 | | | | Seleccione | | |
| 5 | | | | Seleccione | | |
| 6 | | | | Seleccione | | |
| 7 | | | | Seleccione | | |
| 8 | | | | Seleccione | | |
| 9 | | | | Seleccione | | |
| 10 | | | | Seleccione | | |

- **Propósito del control:** El control debe tener un propósito que indique para qué se realiza y que conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo. Considere que establecer un procedimiento o contar con una política por sí sola, no va a prevenir las causas o detectar la materialización del riesgo.

- **Descripción del control:** El control debe indicar el "cómo se realiza", "quien lo realiza", "cuando lo realiza", "que evidencia queda de la acción" y para los casos que aplique, debe reflejar la segregación de funciones. Para los procesos que integran varios componentes, deben especificar en este campo la aplicabilidad del control.

- **Desviaciones de resultados:** Se hace referencia al plan alternativo con el que cuenta el proceso para la aplicación del control, es decir, si como resultado de un control preventivo se observan diferencias o aspectos que no se cumplen, la actividad no debería continuarse hasta que se subsane la situación o si es

un control que detecta una posible materialización de un riesgo, deberían gestionarse de manera oportuna los correctivos o aclaraciones a las diferencias presentadas.

- **Periodicidad:** El control debe tener una periodicidad específica para su realización (cuando se requiera, diario, semanal, mensual, trimestral, anual), la cual deberá seleccionarse de la lista desplegable establecida y su ejecución debe ser consistente y oportuna para la mitigación del riesgo. Por lo que en la periodicidad se debe evaluar si este previene o se detecta de manera oportuna el riesgo.

- **Responsable:** Se debe indicar el cargo asignado para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutarlo dentro del proceso. Se recomienda que sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas.

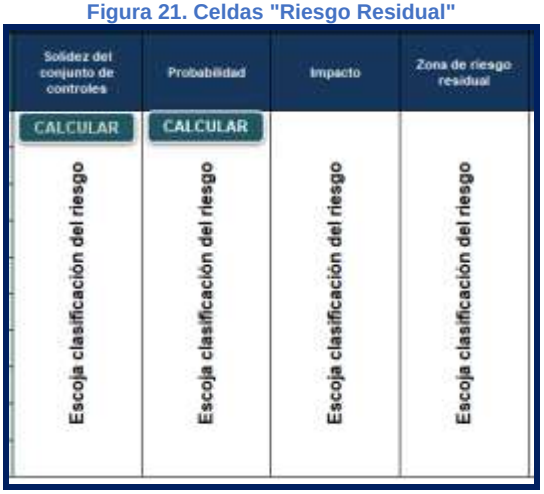
- **Evidencias:** El control debe contar con la evidencia que soporte su ejecución. Esta evidencia ayuda a que se pueda revisar la misma información por parte de un tercero y llegue a la misma conclusión de quien ejecutó el control, y posteriormente, permita evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos y descritos anteriormente.

  Así mismo, en el proceso de monitoreo por parte de la segunda línea de defensa (OPLA) y seguimiento por parte de la tercera línea de defensa (OCI) únicamente se tomará como evidencia aquella que se encuentre documentada en esta sección.

### 5.4.2.4. Valoración Zona de Riesgo Residual

Corresponde al nivel de riesgo resultante de aplicar los controles y se establece de forma posterior a la calificación tanto de la solidez del diseño de controles, para el caso de los riesgos de corrupción, como para la efectividad de los controles, para el caso de los riesgos de gestión y seguridad de la información. De acuerdo con lo anterior, la herramienta registrará el resultado de la zona de riesgo residual de forma automática en la celda correspondiente. (Ver Figura 21)

**Figura 21. Celdas "Riesgo Residual"**



**A. Análisis y evaluación de los controles**

Con el fin de establecer la efectividad de los controles propuestos por el proceso y el cálculo posterior de la Zona de Riesgo Residual, se debe efectuar su evaluación conforme a cada tipología del riesgo así:

A continuación, se precisa el proceso para cada una de estas tipologías.

- **Tipología de controles**

Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan los controles tenemos:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

**B. Para riesgos de gestión y seguridad de la información**

Para analizar los atributos de los controles establecidos, se deben tener en cuenta las características relacionadas con la eficiencia y la formalización, como se observa en la siguiente tabla:

**Tabla 8. Atributos para la evaluación del control - Riesgos de gestión y seguridad de la información**

| CARACTERÍSTICAS | | | DESCRIPCIÓN | PESO |
|---|---|---|---|---|
| Eficiencia | Tipo | Preventivo | Va hacia las causas del riesgo, aseguran el resultado final esperado. | 25% |
| | | Detectivo | Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos. | 15% |
| | | Correctivo | Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación. | 10% |
| | Implementación | Automático | Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización. | 25% |
| | | Manual | Controles que son ejecutados por una persona, tiene implícito el error humano. | 15% |
| Informativos | Documentación | Documentado | Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso. | - |
| | | Sin documentar | Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso. | - |
| | Frecuencia | Continua | El control se aplica siempre que se realiza la actividad que conlleva el riesgo. | - |

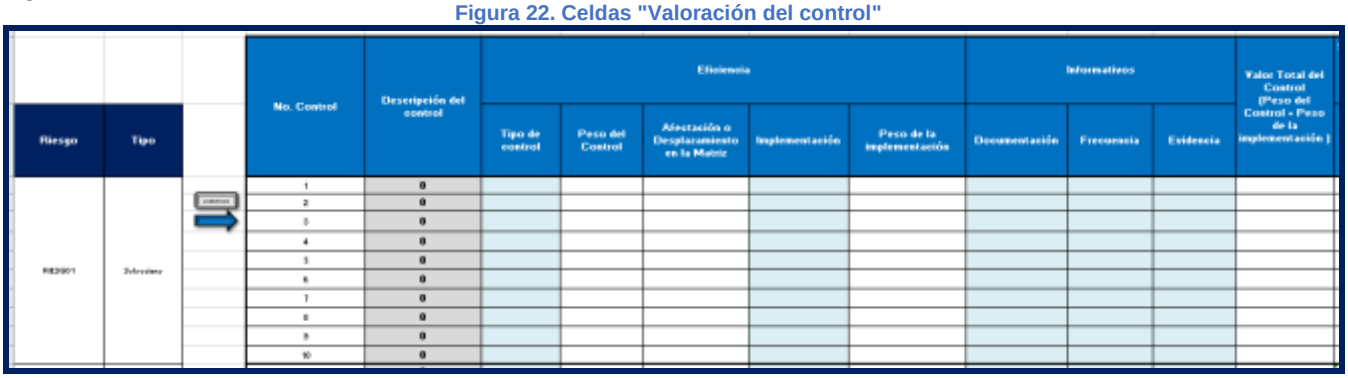
| CARACTERÍSTICAS | | | DESCRIPCIÓN | PESO |
|---|---|---|---|---|
| | | Aleatoria | El control se aplica aleatoriamente a la actividad que conlleva el riesgo. | - |
| | Evidencia | Con Registro | El control deja un registro permite evidencia la ejecución del control. | - |
| | | Sin Registro | El control no deja registro de la ejecución del control. | - |

**Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5. DAFP. Diciembre de 2020**

Teniendo en cuenta que, a partir estos atributos, se dará el movimiento en la matriz de calor, se debe dar clic sobre el botón CALCULAR que se encuentra en la columna “Probabilidad” de la sección Riesgo Residual, como se observa en la figura 21.

Posteriormente, la herramienta presentará la sección “Valoración del control”, donde se diligenciarán las siguientes celdas:

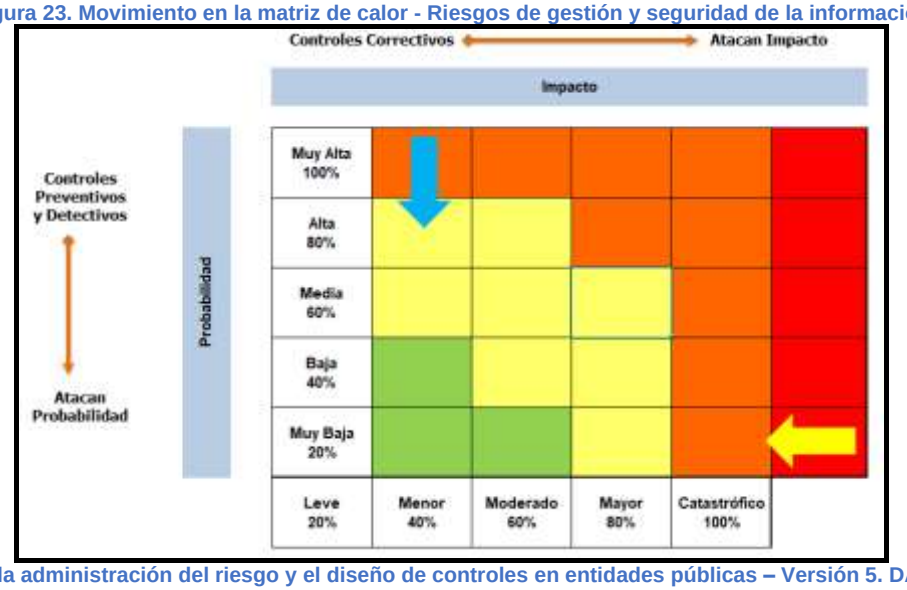
**Figura 22. Celdas "Valoración del control"**




- **Riesgo, Tipo, N° y Descripción del control:** estas celdas son diligenciadas automáticamente por la herramienta, considerando la información registrada en la pestaña “Valoración del riesgo”.
- **Tipo de control:** conforme a lo explicado en la Tabla 8, se debe seleccionar de la lista desplegable la opción considerada para el control.
- **Peso del control – Afectación o Desplazamiento en la Matriz:** estas celdas son diligenciadas automáticamente por la herramienta, considerando la información registrada en “Tipo de control”.
- **Implementación:** conforme a lo explicado en la Tabla 8, se debe seleccionar de la lista desplegable la opción considerada para el control.
- **Peso de implementación:** esta celda es diligenciada automáticamente por la herramienta, considerando la información registrada en la columna “Implementación”.
- **Documentación - Frecuencia - Evidencia:** conforme a lo explicado en la Tabla 8, se debe seleccionar de la lista desplegable la opción considerada para el control.
- **Valor Total del control:** teniendo en cuenta los valores escogidos en las columnas anteriores, la herramienta calcula automáticamente el valor total, efectuando la suma entre el peso del control y el peso de implementación.

De acuerdo con los resultados de la evaluación de los controles se establece una calificación del desplazamiento en la zona de riesgo que la herramienta calcula de forma automática, que es el resultado de aplicar la efectividad de los controles al riesgo inherente, teniendo en cuenta que estos mitigan de forma acumulativa, conforme la clasificación de los controles se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto, así:

**Figura 23. Movimiento en la matriz de calor - Riesgos de gestión y seguridad de la información**




**Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 5. DAFP. Diciembre de 2020**

Para mayor claridad, en la siguiente tabla se presenta un ejemplo donde se observan los cálculos requeridos para la aplicación de los controles:

| RIESGO | DATOS DE PROBABILIDA E IMPACTO INHERENTES | | DATOS VALORACIÓN DE CONTROLES | | CÁLCULOS REQUERIDOS |
|---|---|---|---|---|---|
| Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos. | Probabilidad inherente | 60% | Valoración control 1 preventivo | 40% | 60% x 40% = 24%<br>60% - 24% = 36% |
| | Valor probabilidad para aplicar 2º control | 36% | Valoración control 2 detectivo | 30% | |
| | Probabilidad residual | 25.2% - Baja | | | |
| | Impacto inherente | 80% | | | |
| | No se tiene controles para aplicar al impacto | N/A | N/A | N/A | N/A |
| | Impacto residual | 80% - Mayor | | | |

Para este caso, si bien el riesgo disminuye en el nivel de probabilidad de ocurrencia, al combinar este valor con el nivel de impacto residual, la Zona de riesgo Residual se ubica como Alto en el mismo mapa de calor.

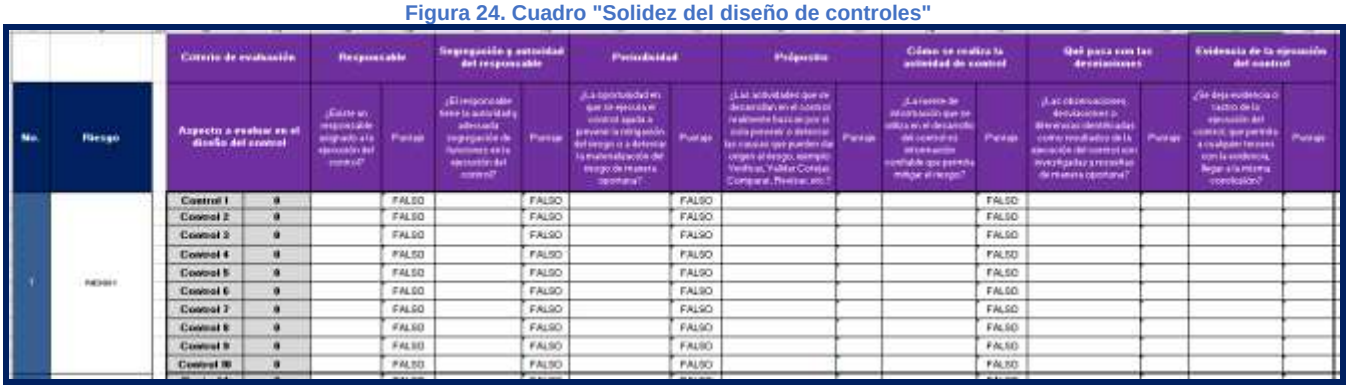
**Nota:** en caso de no contar con controles correctivos (atacan el impacto), este es el mismo calculado para la zona inherente o inicial y no será posible su movimiento en la matriz para el impacto.

### C. Para riesgos de corrupción

Teniendo en cuenta que, a partir estos atributos, se dará el movimiento en la matriz de calor, se debe dar clic sobre el botón CALCULAR que se encuentra en la columna “Solidez del conjunto de controles” de la sección Riesgo Residual, como se observa en la figura 21.

Así pues, la solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo, para lo cual la herramienta presenta el siguiente cuadro:

**Figura 24. Cuadro "Solidez del diseño de controles"**




Como se observa en la figura 24, se establecen siete (7) criterios para evaluar el diseño de los controles pertenecientes a los riesgos de corrupción, para esto se debe seleccionar en la casilla correspondiente para cada control, la respuesta a la pregunta formulada en la columna “Aspecto a evaluar en el diseño de control”, así:

**Tabla 9. Criterios de valoración solidez de controles - Riesgos de corrupción**

| CRITERIO DE EVALUACIÓN | ASPECTO A EVALUAR | OPCIONES DE RESPUESTA |
|---|---|---|
| **Responsable** | ¿Existe un responsable asignado a la ejecución del control? | Asignado |
| | | No asignado |
| **Segregación y autoridad del responsable** | ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control? | Adecuado |
| | | Inadecuado |
| **Periodicidad** | ¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna? | Oportuna |
| | | Inoportuna |
| **Propósito** | ¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar, Cotejar, Comparar, Revisar, ¿etc.? | Prevenir |
| | | Detectar |
| | | No es un control |
| **Cómo se realiza la actividad de control** | ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo? | Confiable |
| | | No confiable |
| **Qué pasa con las desviaciones** | ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna? | Se investigan y resuelven oportunamente |
| | | No se investigan ni se resuelven oportunamente |
| | | No se ha ejecutado el control |

| CRITERIO DE EVALUACIÓN | ASPECTO A EVALUAR | OPCIONES DE RESPUESTA |
|---|---|---|
| | | No se han presentado desviaciones en la ejecución del control |
| **Evidencia de la ejecución del control** | ¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión? | Completa |
| | | Incompleta |
| | | No existe |
| | | No se ha ejecutado el control |

**Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP. 2018.**

Una vez se dé respuesta a las preguntas, la herramienta realiza de forma automática la calificación del control como: “Débil”, “Moderado” o “Fuerte”, teniendo en cuenta el peso asignado, el cual es un valor numérico del 0 al 100, por lo anterior, cada control debe ser evaluado de forma individual y la herramienta ponderará el resultado, que se reflejará en la correspondiente casilla automáticamente.

Posteriormente, se debe dar clic en el botón ⏭, para llegar a las celdas donde se calcula el desplazamiento en el mapa de calor; es importante resaltar que, tratándose de riesgos de corrupción **únicamente hay desplazamiento en el nivel de probabilidad, es decir, para el impacto no opera el desplazamiento debido a la naturaleza de estos riesgos**.

**Figura 25. Celdas para evaluar el desplazamiento - Riesgos de corrupción**

- **Columnas Impacto y Riesgo Inherente:** corresponden a los datos de cálculo para la probabilidad, impacto y zona de riesgo inicial que la herramienta diligencia de forma automática, por lo cual no requiere edición adicional.
- **Solidez Control:** corresponde al cálculo ponderado obtenido con la evaluación de las preguntas y los criterios para el diseño de los controles, el cual es diligenciado de forma automática por la herramienta, por lo cual no requiere edición adicional.
- **Disminución:** se debe seleccionar de la lista desplegable la opción correspondiente al conjunto de controles, considerando si estos disminuyen de forma directa, indirecta o no disminuyen la probabilidad de ocurrencia del riesgo.

- **Riesgo Residual - Probabilidad:** conforme a la opción seleccionada en la columna “Disminución”, esta disminuirá dos (2) niveles si disminuye directamente, un (1) nivel si disminuye indirectamente o se mantendrá igual si no disminuye, este cálculo lo efectúa la herramienta de forma automática.
- **Riesgo Residual – Impacto:** considerando las premisas dadas, este valor se mantiene igual para el riesgo inherente.
- **Resultado:** en esta celda la herramienta presenta de forma automática el cruce del desplazamiento conforme al mismo mapa de calor usado para la zona de riesgo inicial, por lo cual no requiere edición adicional.

### 5.4.3. Acciones de tratamiento – Plan de acción

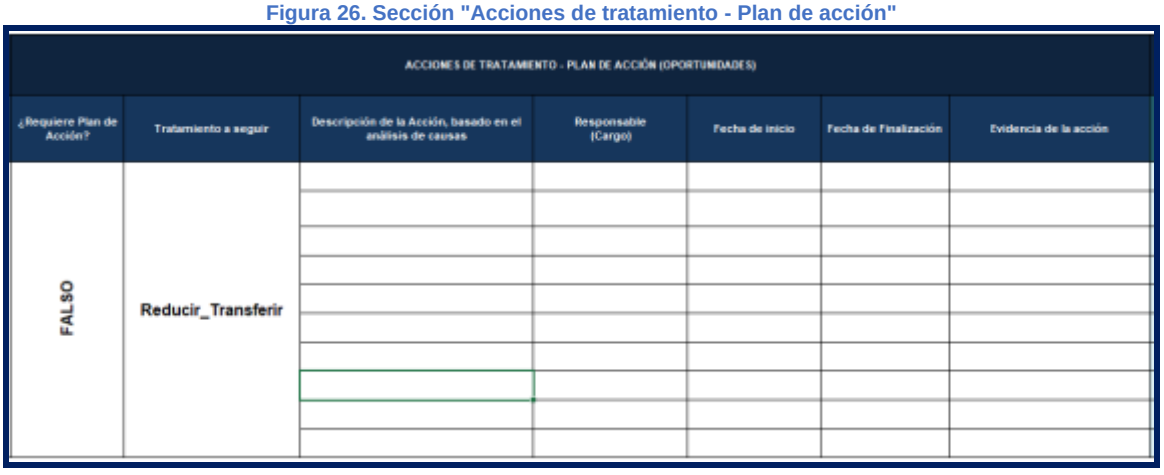
Teniendo como referencia la zona de riesgo residual establecida anteriormente, la herramienta identifica de forma automática la opción de tratamiento del riesgo, la cual se asigna considerando las alternativas que contempla la zona donde se ubica el riesgo, como se muestra en la siguiente tabla:

**Tabla 10. Matriz de tratamiento del riesgo**

| ZONA DE RIESGO RESIDUAL | NIVEL DE ACEPTACIÓN | TRATAMIENTO DEL RIESGO RESIDUAL |
|---|---|---|
| Extrema | No Aceptable* | ▪ Evitar el riesgo decidiendo no iniciar o continuar la actividad que lo originó, definiendo acciones para mejorar los controles o acciones complementarias que contribuyan a la no materialización del riesgo.<br>▪ Reducir el riesgo mediante acciones adicionales tendientes a automatizar los controles.<br>▪ Reducir el riesgo mediante acciones asociadas a mejorar el control.<br>▪ Si la causa es atribuible a un tercero, transferir el riesgo y eventualmente efectuar mejoras en el control o en el proceso.<br>▪ Compartir el riesgo: reducir su efecto compartiéndolo con uno o varios procesos.<br>Nota: si se decide compartir el riesgo, es necesario contar con la aceptación del proceso con el que se va a compartir el riesgo y debe identificarse el riesgo en los mapas de los procesos que lo van a compartir. |
| Alta | | |
| Moderada | | |
| Baja | Aceptable | ▪ Asumir el riesgo para lo cual se debe mantener el control, en caso de existir, y gestionarlo. Por tal motivo, no es necesario definir un plan de tratamiento para estos riesgos. |

Considerando la tabla anterior, todos los riesgos que cuenten con zonas de riesgo residual “Extrema”, “Alta” y “Moderada”, requerirán del establecimiento de un plan de acción, para lo cual, la herramienta dispone de las siguientes celdas:

**Figura 26. Sección "Acciones de tratamiento - Plan de acción"**



Cabe resaltar que este campo se habilitará única y exclusivamente para aquellos riesgos cuyo tratamiento se definió como Reducir – Mitigar, para estos casos, se debe diligenciar los siguientes campos:

- **Descripción de la acción, basado en el análisis de causas:** registrar la actividad que se va a realizar para evitar que el riesgo se materialice y se debe definir el fin para el cual se realiza dicha actividad; por ejemplo: automatizar la lista de chequeo contractual con el fin de optimizar tiempos y disminuir márgenes de error.
- **Responsable:** registrar el nombre y cargo de la persona que realizara dicha actividad; por ejemplo: Leonidas León – Asesor contratación
- **Fecha de inicio y fecha de finalización:** registrar el periodo de tiempo durante el cual se va a desarrollar la acción.
- **Evidencia de la acción:** registrar cual sería el documento que soportaría la ejecución de la acción; por ejemplo: lista de chequeo automatizada.

### 5.4.4. Monitoreo de la gestión del riesgo

#### 5.4.4.1. Monitoreo por parte del líder del proceso a la aplicación de controles

El monitoreo al Mapa de Riesgos del proceso implica reportar la ejecución de cada uno de los controles establecidos para cada riesgo, por parte de los líderes de proceso como primera línea de defensa.

El reporte del monitoreo se debe realizar cuatrimestralmente así:

- Primer monitoreo con corte a abril de la vigencia, cuyo monitoreo debe reportarse hasta 20 de abril.
- Segundo monitoreo con corte a agosto de la vigencia, cuyo monitoreo debe reportarse hasta 20 de agosto.
- Tercer monitoreo con corte a diciembre de la vigencia, cuyo monitoreo debe reportarse hasta 20 de diciembre.

El monitoreo realizado por la primera línea de defensa implica diligenciar el análisis cualitativo y cargar las evidencias en la carpeta compartida de SharePoint, dispuesta para tal fin.

Lo anterior, teniendo en cuenta los siguientes pasos:

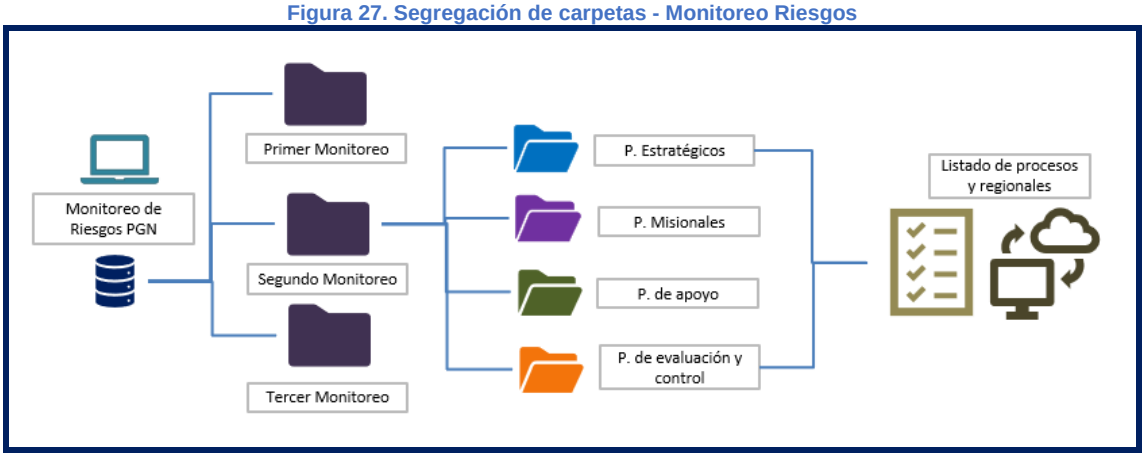
- **Paso 1:** Ingresar a la carpeta en SharePoint creada para los monitoreos a realizar en la vigencia, la cual se encuentra en el grupo “Monitoreo Riesgos – PGN”; esta será compartida por parte de la OPLA con líderes y gestores de proceso tanto a nivel central como territorial.

- **Paso 2.** Identificar el periodo de monitoreo correspondiente primer monitoreo, segundo monitoreo o tercer monitoreo.

- **Paso 3.** Ubicar la clasificación de proceso correspondiente (Procesos estratégicos, misionales, de apoyo y de evaluación y control).

- **Paso 4.** Ubicar la carpeta correspondiente al proceso del SGC. (Ver Figura 50)

**Figura 27. Segregación de carpetas - Monitoreo Riesgos**




- **Paso 5.** Ingresar al mapa de riesgo del proceso y diligenciar los campos correspondientes conforme al periodo que se está reportando (columna U, V y W) tal como lo indica la siguiente figura:

**Figura 28. Monitoreo por parte del líder del proceso**

| Monitoreo por parte del Lider del Proceso | | |
|---|---|---|
| Monitoreo 1 (Con corte 15 de abril)<br>Fecha de reporte: Entre 16 y 20 abril | Monitoreo 2 (Con corte 15 de agosto)<br>Fecha de reporte: Entre 16 y 20 agosto | Monitoreo 3 (Con corte 15 de diciembre)<br>Fecha de reporte: Entre 16 y 20 diciembre |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

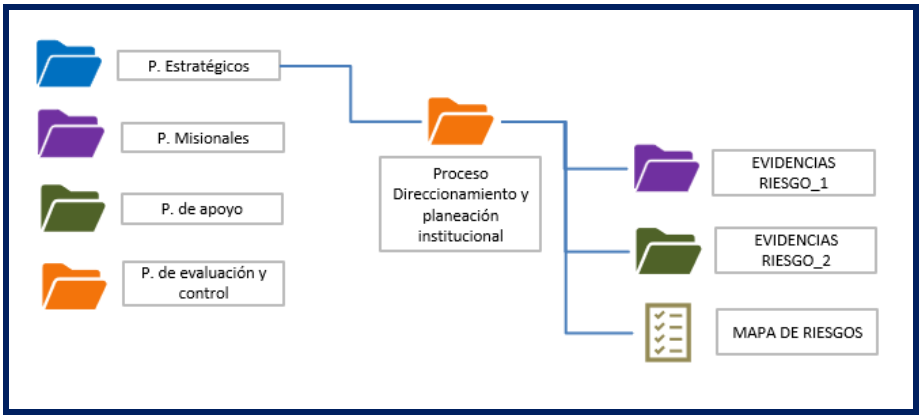
**Nota:** es importante aclarar que, para el reporte cualitativo de cada control, este debe dar respuesta a cada uno de los campos definidos en las acciones de control (Descripción del control – ¿Cómo se realiza?, desviación de resultados, periodicidad, responsable, y evidencia); es decir su redacción debe plasmar la ejecución de estos;

por ejemplo:

*"El servidor designado diligencio la lista de chequeo contractual para 35 procesos que se desarrollaron en el cuatrimestre. Para este periodo no aplico desviación de resultados".*

- **Paso 6.** Cargar evidencias de la aplicación del control en la carpeta correspondiente (La OPLA dispondrá una carpeta para que el líder del proceso cargue las evidencias según la aplicación del control y lo registrado en el monitoreo cualitativo para el periodo correspondiente) (Ver Figura 29)

**Figura 29. Evidencias Monitoreo Primer Línea de defensa**




- **Paso 7.** Comunicar a la Oficina de Planeación mediante correo electrónico el reporte del monitoreo y cargue de evidencias.

### 5.4.4.2. Monitoreo por parte del Líder del Proceso al Plan de acción

Este monitoreo debe ser registrado en la columna correspondiente según el cuatrimestre a evaluar. De igual manera que en el literal 5.4.4.1 – "Monitoreo por parte del líder del proceso a la aplicación de controles", el líder o gestor del proceso debe realizar el registro de información cualitativa (describir el avance y ejecución de la acción) y debe cargar la respectiva evidencia que soporte la ejecución de la acción en la carpeta dispuesta dentro de cada riesgo como "Evidencia plan de acción". (Ver Figura 29)

La información cualitativa debe registrarse en las columnas AJ, AK y AL; según corresponda el periodo a evaluar.

**Figura 30. Monitoreo por parte del Líder del Proceso al Plan de acción**

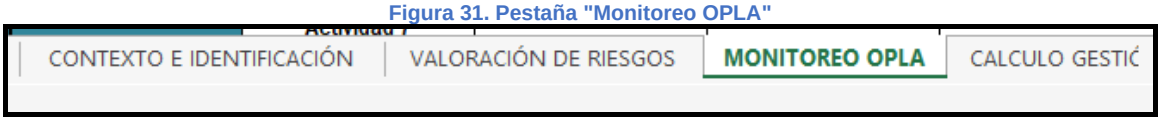
Una vez se haya registrado el reporte cualitativo y se haya cargado la evidencia correspondiente se debe definir el estado de la acción, información que debe diligenciarse en la columna “Estado”. Se establecen las siguientes categorías:

- **Sin iniciar**, cuando la acción no se haya iniciado
- **En proceso**; cuando la acción se haya realizado parcialmente
- **Cerrado**, cuando la acción se haya realizado totalmente según lo preestablecido
- **Vencido,** cuando la acción no se ha finalizado y ya se ha cumplido su periodo de ejecución establecido.

### 5.4.4.3. Monitoreo por parte de la Oficina de Planeación

Esta información debe registrarse cuatrimestralmente en la pestaña denominada “Monitoreo OPLA” y dicho reporte debe realizarse hasta el último día hábil de cada cuatrimestre.

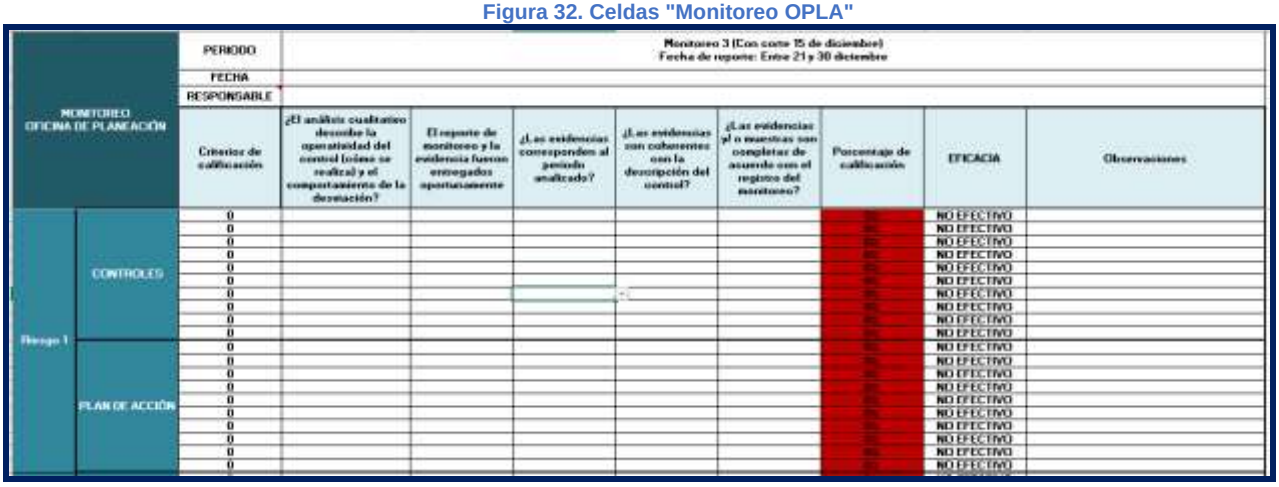
**Figura 31. Pestaña "Monitoreo OPLA"**




De acuerdo con lo anterior, el seguimiento se realiza teniendo en cuenta los siguientes criterios (Ver Figura 56):

- **¿El análisis cualitativo describe la operatividad del control (cómo se realiza) y el comportamiento de la desviación?**, se revisa si el reporte cualitativo da respuesta a la aplicación de las acciones de control predefinidas, tal como se proporciona ejemplo en el acápite “Monitoreo por parte del líder del proceso a la aplicación de controles” de este documento.
- **¿El reporte de monitoreo y la evidencia fueron entregados oportunamente?;** se revisa que el correo electrónico por medio del cual el líder o gestor del proceso comunica a OPLA la disponibilidad de monitoreo se haya realizado dentro del tiempo estipulado según lo definido en el acápite “Monitoreo por parte del líder del proceso a la aplicación de controles” de este documento.
- **¿Las evidencias corresponden al periodo analizado?,** se revisa que las evidencias que suministra el líder o gestor del proceso se hayan realizado dentro del cuatrimestre evaluado
- **¿Las evidencias son coherentes con la descripción del control?,** se revisa que la evidencia suministrada corresponda a la preestablecida en las acciones de control, es decir, por ejemplo, si en las acciones de control se definió como evidencia una lista de chequeo, el proceso no puede suministrar un acta de una reunión
- **¿Las evidencias y/ o muestras son completas de acuerdo con el registro del monitoreo?,** se revisa que las evidencias establecidas en el monitoreo sean las mismas suministradas por el proceso; es decir, si el proceso en el monitoreo dice que se realizaron 35 listas de chequeo, se hayan cargado como evidencias ese mismo número de listas de chequeo.

**Figura 32. Celdas "Monitoreo OPLA"**




El cumplimiento de los anteriores aspectos determina una calificación al monitoreo, que se presenta en la herramienta a través del siguiente semáforo:

| N° CRITERIOS CUMPLIDOS | PORCENTAJE DE CALIFICACIÓN | |
|---|---|---|
| 5 | 100% | |
| 4 | 80% | |
| 3 | 60% | |
| 2 | 40% | |
| 1 | 20% | |
| 0 | 0% | |

**Nota:** Con relación al monitoreo de OPLA para las acciones establecidas en el Plan de acción, se tendrán en cuenta los mismos criterios que los establecidos para los controles.

- **EFICACIA**

Como se observa en la figura 32, en la columna “EFICACIA” la herramienta registra automáticamente si el control es eficaz, cuando se establece un cumplimiento mayor al 80%, donde se considera el cumplimiento de lo planeado, de forma oportuna, coherente y completa, respecto al monitoreo, evidencias aportadas y plazos establecidos para efectuar tanto el monitoreo como la ejecución de los controles.

### 5.5. MATERIALIZACIÓN DEL RIESGO

En caso de identificar la materialización de un riesgo en un proceso, el líder de proceso debe documentar las acciones de contingencia, incluyendo criterios de oportunidad, en el plan de mejoramiento del proceso, con el fin de evitar en lo posible el daño sobre el proceso y la repetición del evento. Además, se precisa que este efectúe el reporte correspondiente a la Oficina de Planeación con copia a la Oficina de Control Interno, a través de correo electrónico institucional, con plazo máximo de 10 días hábiles una vez se notifique la materialización de riesgo.

### 5.6. APROBACIÓN O ACTUALIZACIÓN DEL MAPA DE RIESGOS POR PROCESOS

Una vez registrada toda la información en la herramienta del Mapa de Riesgos, esta debe ser aprobada por el líder del proceso y remitidos a la Oficina de Planeación para su respectiva publicación, según lo definido en el procedimiento MC-P-01. Gestión de la información documentada. Asimismo, en caso de que se requiera crear, modificar o eliminar un riesgo, se debe solicitar mediante el formato MC-F-01. Solicitud de actualización documental.

Adicionalmente, en relación con lo anterior, se realiza la consolidación y actualización de los riesgos de corrupción de acuerdo con lo consignado en el Plan Anticorrupción y Atención al Ciudadano.

## 6. CONTROL DE CAMBIOS

| FECHA (Diligencie la fecha en la OPLA aprueba la actualización documental) | VERSIÓN DEL DOCUMENTO QUE MODIFICA (Diligencie el número de la versión del documento que se va a modificar) | DESCRIPCIÓN DEL CAMBIO (Describir de manera detallada las modificaciones realizadas al documento) |
|---|---|---|
| 08/06/2020 | 1 | Creación de la Política de Administración del Riesgo |
| 07/12/2021 | 2 | 1. Este documento se encontraba codificado en el proceso de Administración del riesgo con el código GUI-AR-00-001. Así mismo, esta guía se traslada al proceso de Mejoramiento Continuo.<br>2. Se actualizan todos los componentes de la gestión del riesgo, conforme a la nueva versión de la Guía de Administración del Riesgo emitida por el Departamento Administrativo de la Función Pública – DAFP, versión 5 de diciembre de 2020. |
| 26/09/2022 | 3 | 1. Se actualizan objetivos estratégicos según lo aprobado en Comité Institucional de Gestión y desempeño del 30 de junio de 2022.<br>2. Se incluyen ejemplos de redacción de riesgos de corrupción Se incluye el tratamiento de oportunidades y la evaluación de la eficacia tanto para controles como para planes de acción. |
| 31/03/2023 | 4 | 1. Se actualiza la guía conforme a la actualización de la herramienta de mapa de riesgos.<br>2. Se incluye la información de la efectividad incluida en la herramienta. |

*Para el diligenciamiento del presente formato, es necesario tener en cuenta las directrices definidas en el numeral 5.1. Condiciones generales de la MC-G-01 Guía "Elaboración de la información documentada"; este formato se desarrolla dependiendo de la necesidad, puede incluir tablas, dibujos, diagramas, etc. y su tamaño varía de acuerdo con lo requerido.*