Tabla de contenido

1. Objetivo

Establecer la metodología para la administración de riesgos, por parte de los responsables de los procesos en la toma de decisiones respecto al tratamiento de los riesgos y sus impactos en la Comisión Nacional del Servicio Civil o sus grupos de interés, con el fin de cumplir con los objetivos institucionales y de proceso.

2. Alcance

El presente documento está basado en la guía para la administración del riesgo y el diseño de controles en entidades públicas, vigente del Departamento Administrativo de la Función Pública y es aplicable a todos los procesos y las dependencias de la Comisión Nacional del Servicio Civil – CNSC, permitiendo su gestión desde la identificación hasta su monitoreo y revisión de controles eficaces.

La CNSC a través del presente documento establece:

- ✓ Política
- ✓ Identificación de riesgos
- ✓ Administración del riesgo de seguridad de la información
- ✓ Administración del riesgo de corrupción
- ✓ Niveles de aceptación del riesgo
- ✓ Conservación de los resultados de la gestión

3. Diccionario Conceptual

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenaza:** Cosa que constituye una posible causa de riesgo o perjuicio para el proceso o parte de él en el cumplimiento de su objetivo, así incluye toda aquella acción o situación que aprovecha una vulnerabilidad para atacar o invadir un sistema. El origen de las amenazas suele ser externo o ajeno al control de la Entidad.
- **Apetito de 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 distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Capacidad de riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección consideran que no sería posible el logro de los objetivos de la entidad.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden 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 la cuales se puede presentar el riesgo.
- **Capacidad de riesgo:** Es el máximo valor del nivel de 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.
- **CNSC:** sigla para referirse a la Comisión Nacional del Servicio Civil.
- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Criterio de frecuencia:** criterio para medir la probabilidad de ocurrencia, analizando el número de eventos en un periodo determinado, los hechos que se han materializado y el historial de situaciones o eventos asociados al riesgo.
- **DAFP:** sigla para referirse al Departamento Administrativo de la Función Pública.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Evaluación del riesgo:** proceso utilizado para determinar las prioridades de la administración del riesgo, comparando el nivel de un determinado riesgo con respecto a un estándar determinado.
- **Factor de riesgo:** Son las fuentes generadoras de riesgos.
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** propiedad de exactitud y completitud.
- **Modelo de líneas de defensa:** modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad. Este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.
- **Monitoreo:** comprobación, supervisión, observación, o registro de la forma en que se lleva a cabo una actividad con el fin de identificar sus posibles cambios.
- **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. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- **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.
- **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 periodo de 1 año.
- **Respuestas a riesgos:** los medios a través del cual se decide gestionar riesgos individuales. Las principales categorías son: tolerar el riesgo; tratar el mismo reduciendo su impacto o posibilidad; transferirlo a otra organización o terminar la actividad que lo origina. Los controles internos son una forma de tratar un riesgo.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

  Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo 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 gestión:** posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos.
- **Riesgo 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. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo aceptado:** la cuantía, más amplia del riesgo, que la Comisión Nacional del Servicio Civil –CNSC- está dispuesta a asumir para realizar su misión o su visión.
- **Riesgo inherente:** Nivel de riesgo propio de la actividad. 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:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Seguridad de la información:** conjunto de técnicas y métodos encaminados a la preservación de la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, medios de almacenamiento y/o difusión (ISO 27000:2014 Numeral 2.33. Information security).

- **Seguridad informática:** es una disciplina tecnológica que se encarga de proteger la integridad y la privacidad de la información contenida o gestionada mediante sistemas informáticos.
- **SIG:** sigla para referirse al Sistema Integrado de Gestión Institucional de la CNSC.
- **Tolerancia al riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
- **Vulnerabilidad:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas. El origen de las vulnerabilidades suele ser interno y en la potestad de gestión por parte de la Entidad.

4. Desarrollo

Contexto institucional

La CNSC, en el desarrollo de sus actividades y en función de su objeto social, se enfrenta constantemente a factores internos y externos que pueden crear incertidumbre sobre el logro de sus objetivos, constituyendo un riesgo. Por tal motivo, la administración del riesgo proporciona información que permite a la Comisión aumentar la probabilidad de alcanzar sus objetivos estratégicos y reducir la ocurrencia de eventos que pueden afectar el cumplimiento de tales objetivos.

A la vez, la administración del riesgo ayuda al conocimiento y mejoramiento de la CNSC en general, contribuye a elevar la productividad y a garantizar la eficiencia y la eficacia en los procesos, permitiendo la definición de acciones de mejoramiento continuo, brindándole un manejo sistémico a la entidad.

En este orden de ideas, la administración del riesgo debe ser incorporada al interior de la CNSC como una política de gestión por parte de la Dirección y contar con la participación y respaldo de todos los servidores públicos, involucrándolos y comprometiéndolos en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.

Desde la perspectiva del Control Interno, el modelo COSO1, adaptado para Colombia por el ICONTEC mediante la Norma Técnica NTC-ISO 31000, interpreta que el propósito principal del control es la reducción de los riesgos, garantizando que los objetivos de la entidad van a ser alcanzados. También establece que la administración del riesgo es un proceso efectuado por la Dirección de la entidad y por todo el personal, para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

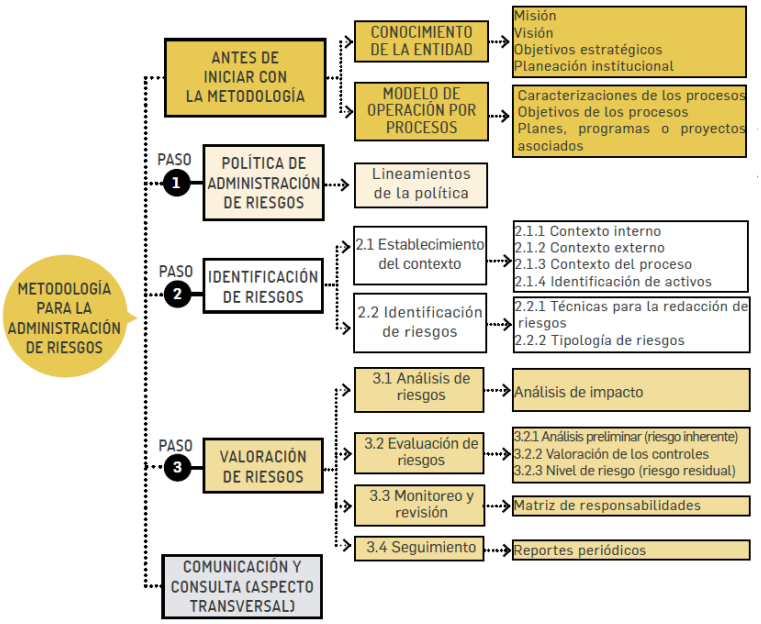
Metodología

El insumo que permitirá analizar y adaptar la información a los criterios exigidos por las normas técnicas, en especial a lo referido a la administración del riesgo y a los aspectos del nuevo modelo de operación por procesos de la CNSC, serán los mapas de riesgos elaborados por las

[1] COSO: Committee on Sponsoring Organizations of the Treadway Commission

dependencias. De acuerdo con la metodología del Departamento Administrativo de la Función Pública, el ejercicio de administración del riesgo consiste en establecer la Política de Administración de Riesgos, identificar los riesgos y valorarlos.

Esquema 1. Metodología para la administración del riesgo recomendada por el Departamento Administrativo de la Función Pública en su Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 de octubre de 2018.



Fuente: Elaboración DAFP 2020

4.1 Política

La Política de Administración de Riesgos de la Comisión Nacional del Servicio Civil se ha concebido bajo un enfoque estratégico que tiene como objetivo generar valor agregado para la gestión institucional a partir de la prevención de amenazas, el aprovechamiento de oportunidades y mitigación de impactos negativos derivados de la exposición a los riesgos.

La gestión de riesgos establece las directrices que permiten atención de aquellos eventos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales desde el desarrollo de los procesos de la Entidad.

Desde la Alta Dirección se promueve y fortalece la gestión del riesgo mediante la asignación de los recursos necesarios para su desarrollo, generando espacios de participación y de construcción colectiva y propiciando la comunicación e interacción efectiva a nivel interno y con nuestro contexto organizacional.

Para la adecuada gestión del riesgo se adelantan acciones y prácticas de trabajo para:

- La identificación y documentación de riesgos de gestión, de corrupción y de seguridad de la información en los procesos.
- El establecimiento de acciones de carácter preventivo para evitar la materialización de los riesgos identificados.
- La actuación correctiva y oportuna ante la materialización de los riesgos identificados.
- La aplicación de buenas prácticas derivadas de las metodologías establecidas para la gestión de riesgos en la administración pública.

Los lineamientos para la gestión del riesgo se desarrollan en esta guía, denominada “Guía Institucional para la Administración y Gestión del Riesgo en la CNSC”, la cual considera la estructura metodológica, los niveles de aceptación o tolerancia, las acciones de tratamiento, y el seguimiento, entre otros aspectos.

4.1.1 Lineamientos de la política

Para la implementación de la guía se consideran lineamientos los siguientes elementos:

- Que la administración del riesgo en la Comisión Nacional del Servicio Civil – CNSC sea una herramienta estratégica usada como elemento para la toma de decisiones de todos sus procesos institucionales.
- Que la gestión eficaz del riesgo sea considerada por los directores como un factor esencial para el logro de los objetivos de la Comisión.
- Que la gestión del riesgo cree y proteja el valor y aborde explícitamente la incertidumbre que se pueda presentar sobre los objetivos organizacionales.
- Que la administración del riesgo en la Comisión sea una actividad transparente e inclusiva, que actúa dinámicamente, y que sea permanentemente receptiva al cambio.
- Que la responsabilidad de los Comisionados, Directores, Jefes de Oficina, Asesores y Coordinadores de Grupo sea explícita, como encargados de implementar la metodología para administrar el riesgo, elaborar y actualizar los mapas y planes de administración de los riesgos en sus dependencias, así como de la calidad, completitud y veracidad de los ejercicios administración del riesgo de cada uno de sus procesos.
- Que la Oficina Asesora de Planeación cumpla un papel de facilitador para el adecuado desarrollo de esta guía y acompañante metodológico para todos los procesos institucionales.
- Que la administración del riesgo en la CNSC, usa como marcos de referencia herramientas de implementación, el ciclo Deming (o ciclo PHVA) para su gestión, las recomendaciones de la metodología del Departamento Administrativo de la Función Pública – DAFP y la Norma Técnica Colombiana NTC-ISO 31000 en la versión que se encuentra vigente a la fecha de su aplicación.

- Que el proceso con alcance a la planeación institucional y el direccionamiento estratégico lidere la implementación y administración del riesgo en la Comisión, efectuando una revisión y ajuste a la planeación de actividades y objetivos al menos una vez al año.
- Que el resultado de esta revisión a la planificación se comunique a todos líderes de los procesos institucionales.
- Que se cuente con un plan de tratamiento específico, que incluya actividades concretas para contribuir a la contención de posibles eventos de materialización del riesgo, para todos los riesgos con impacto negativo, cuyo valor después de la aplicación de los controles sea “Alto” o “Extremo”.
- Que los resultados de la identificación de los riesgos, su valoración, la aplicación y evaluación de los controles, los planes de tratamiento formulados, las acciones de atención, casos de materialización de los riesgos y los riesgos residuales sean reconocidos y aceptados por cada uno de los propietarios de los riesgos.
- Que el riesgo residual sea documentado y sea sometido a monitoreo, revisión, y a tratamiento adicional cuando sea pertinente.
- Que los riesgos que se hayan identificado con posible afectación a la seguridad de la información sean registrados en las matrices correspondientes y la materialización de ellos sea reportada según lo indicado en el procedimiento de gestión de incidentes de seguridad de la información para ser reportados a las autoridades o instancias respectivas que el gobierno disponga cuando corresponda.
- Que se realicen las actualizaciones de las matrices de riesgos siguiendo los lineamientos de esta guía, cada vez que se presenten cambios significativos en el direccionamiento estratégico de la entidad, en las características de ejecución de las actividades de los procesos institucionales o ante posibles materializaciones de riesgos no identificados inicialmente.

4.2 Identificación de riesgos

En la CNSC la identificación de los riesgos se realiza determinando cuales están o no bajo el control de la organización, para ello tenemos en cuenta el contexto estratégico en el que opera la entidad, las caracterizaciones de proceso dentro del Modelo de Operación por Procesos y que contemplan su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

La Oficina Asesora de Planeación debe realizar reuniones por proceso, contando con la participación del responsable de este y las personas de las diferentes dependencias u oficinas que estén involucradas en la ejecución del proceso específico, con el fin de realizar un inventario de los riesgos y estructurarlos de la siguiente manera:

Misión	Visión	Objetivo Estratégico	Objetivo de Proceso
Garantizar a través del mérito, que las	Ser reconocida en el 2022 como la Entidad que en el	1. Incrementar la capacidad técnica de la CNSC para ejecutar el plan de vacantes definido con las entidades públicas.	Todos los objetivos de proceso se relacionan en la

Misión	Visión	Objetivo Estratégico	Objetivo de Proceso
entidades públicas cuenten con servidores de carrera competentes y comprometidos con los objetivos institucionales y el logro de los fines del Estado.	Estado colombiano garantiza de manera efectiva la Carrera Administrativa, con adecuada capacidad institucional y posiciona como la autoridad técnica en la materia.	2. Completar, depurar y mantener actualizado el Registro Público para la debida administración de la Carrera Administrativa. 3. Validar la EDL para determinar la permanencia y el retiro de los servidores de Carrera Administrativa y su contribución al logro de las metas institucionales. 4. Incrementar la cobertura y oportunidad de la vigilancia y control de la Carrera Administrativa para garantizar el cumplimiento de las normas de carrera.	administración de riesgos Sistema Integrado de Gestión (SIG) | CNSC

Fuente: Elaboración propia en la CNSC

4.2.1 Tipos de Riesgo

A partir de la tipología descrita en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, emitida por el Departamento Administrativo de la Función Pública, la Comisión Nacional del Servicio Civil identifica los siguientes tipos de riesgo:

- **Riesgo estratégico:** posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad. Se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
- **Riesgos operativos:** posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad. Incluye riesgos provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.
- **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.
- **Riesgos financieros:** posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc. Incluye la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad.
- **Riesgos de cumplimiento**: posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal, las obligaciones contractuales, la ética pública y, en general, a su compromiso ante la comunidad.
- **Riesgos tecnológicos:** posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad, y

la capacidad de la CNSC para que la tecnología disponible satisfaga sus necesidades actuales y futuras y soporte el cumplimiento de misión.

- **Riesgos de imagen:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas. Es el desprestigio de la Entidad que trae como consecuencia la pérdida de credibilidad y confianza del público por fraude, insolvencia, conducta irregular de los empleados, rumores, errores cometidos en la ejecución de alguna operación por falta de capacitación del personal o deficiencia en el diseño de los procedimientos.
- **Riesgos de seguridad de la información:** posibilidad de combinación de amenazas y vulnerabilidades en el entorno de la seguridad de la información. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales.

4.3 Valoración de los riesgos

4.3.1 Análisis de riesgos

Consiste en establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (también conocido como riesgo inherente).

Probabilidad de ocurrencia del riesgo

Es la posibilidad de ocurrencia del riesgo, que puede ser medida con criterios de frecuencia o factibilidad. Para la CNSC, se adopta el criterio de frecuencia, realizando el análisis con base en la estimación del número de veces que se ha presentado o se puede llegar a presentar el evento en un tiempo determinado. En caso de no contar con un historial de situaciones o eventos asociados al riesgo, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

Para la CNSC se toman como referencia los siguientes niveles, en orden ascendente según la probabilidad de ocurrencia basada en el criterio de frecuencia:

Nivel de probabilidad	Descriptor	Descripción	Frecuencia
1	Raro	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos cinco (5) años.
2	Poco Probable	El evento puede ocurrir en algún momento.	Se ha presentado al menos 1 vez en los últimos cinco (5) años.

Nivel de probabilidad	Descriptor	Descripción	Frecuencia
3	Posible	El evento podría ocurrir en algún momento.	Se ha presentado al menos 1 vez en los últimos dos (2) años.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Se ha presentado al menos 1 vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Se ha presentado más de 1 vez al año.

Fuente: Elaboración propia en la CNSC

Impacto del riesgo

Es la consecuencia que puede ocasionar la materialización del riesgo a la entidad. La CNSC ha adaptado y adoptado los siguientes criterios para calificar el impacto de sus riesgos:

Nivel de impacto	Descriptor	Afectación operativa	Afectación económica	Afectación de imagen	Afectación a la seguridad de la información
1	Leve	El evento materializado impide el normal funcionamiento de la Presidencia y/o alguno de los Despachos de los Comisionados y/o en las Oficinas Asesoras y/o las Direcciones de la Comisión por un tiempo transcurrido entre tres (3) y ocho (8) horas durante la jornada laboral normal.	El evento materializado produce una pérdida de dinero o un sobrecosto menor a dos (2) salarios mínimos mensuales legales vigentes.	El evento materializado produce una reclamación de menos de diez (10) ciudadanos. No se afecta la imagen institucional de forma significativa.	No aplica
2	Menor	El evento materializado impide el normal	El evento materializado produce una pérdida de	El evento materializado produce una reclamación de	No aplica

Nivel de impacto	Descriptor	Afectación operativa	Afectación económica	Afectación de imagen	Afectación a la seguridad de la información
		funcionamiento de la Presidencia y/o alguno de los Despachos de los Comisionados y/o en las Oficinas Asesoras y/o las Direcciones de la Comisión por un tiempo transcurrido entre tres (3) y doce (12) horas durante el periodo de cierre de convocatorias.	dinero o un sobrecosto calculado entre dos (2) y hasta cinco (5) salarios mínimos mensuales legales vigentes.	entre once (11) y veinticinco (25) ciudadanos. Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.	
3	Moderado	El evento materializado impide el normal funcionamiento de la Presidencia y/o alguno de los Despachos de los Comisionados y/o en las Oficinas Asesoras y/o las Direcciones de la Comisión por un tiempo transcurrido entre doce horas y un minuto (12:01) hasta treinta y seis (36) horas durante la jornada laboral normal.	El evento materializado produce una pérdida de dinero o un sobrecosto calculado entre cinco (5) y hasta diez (10) salarios mínimos mensuales legales vigentes.	El evento materializado produce una reclamación de más de veintiséis (26) ciudadanos y/o una (1) entidad pública. Reproceso de actividades y aumento de carga operativa. Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. Investigaciones penales,	Un evento materializado puede afectar de alguna forma la confidencialidad, integridad o disponibilidad por: (i) causar una degradación del 25% en la capacidad operativa de los procesos misionales, sin embargo, la organización puede realizar sus funciones principales, pero la efectividad de las funciones se reduce. (ii) resultar en una pérdida financiera menor, calculada entre dos (2) y hasta cinco (5) salarios mínimos mensuales legales vigentes

Nivel de impacto	Descriptor	Afectación operativa	Afectación económica	Afectación de imagen	Afectación a la seguridad de la información
				fiscales o disciplinarias.	(iii) derivar en un riesgo bajo para las personas, de acuerdo con los peligros y valoraciones establecidas por el sistema de seguridad y salud en el trabajo.
4	Mayor	El evento materializado impide el normal funcionamiento de la Presidencia y/o alguno de los Despachos de los Comisionados y/o en las Oficinas Asesoras y/o las Direcciones de la Comisión por un tiempo transcurrido entre doce horas y un minuto (12:01) hasta treinta y seis (36) horas durante el periodo de cierre de convocatorias. Incumplimiento en las metas y objetivos institucionales.	El evento materializado produce una pérdida de dinero o un sobrecosto calculado entre diez (10) y hasta veinticinco (25) salarios mínimos mensuales legales vigentes.	El evento materializado produce una reclamación de más de dos (2) entidades públicas y/o una institución de educación superior y/o un ente de control externo. Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. Sanción por parte del ente de control u otro ente regulador. Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.	El evento materializado significa la pérdida de confidencialidad, integridad o disponibilidad por: (i) causar una degradación entre el 26% y el 50% en la capacidad operativa de los procesos misionales, y la organización pueda realizar parcialmente sus funciones principales, pero la efectividad de estas reduce considerablemente. (ii) resultar en una pérdida financiera significativa, calculada entre cinco (5) y hasta diez (10) salarios mínimos mensuales legales vigentes. (iii) derivar en un riesgo medio para las personas, de acuerdo con los peligros y valoraciones establecidas por el sistema de seguridad y salud en el trabajo. (iv) Se ven afectados dos criterios de seguridad de la

Nivel de impacto	Descriptor	Afectación operativa	Afectación económica	Afectación de imagen	Afectación a la seguridad de la información
					información, de forma simultánea.
5	Catastrófico	El evento materializado impide el normal funcionamiento de la Presidencia y/o alguno de los Despachos de los Comisionados y/o en las Oficinas Asesoras y/o las Direcciones de la Comisión por un tiempo mayor a treinta y seis horas y un minuto (36:01) sin considerar el periodo en que se presente	El evento materializado produce una pérdida de dinero o un sobrecosto calculado mayor a veinticinco (25) salarios mínimos mensuales legales vigentes. Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.	El evento materializado produce una reclamación de más de dos (2) instituciones de educación superior y/o un ente de control externo y/o el Congreso de la República. Intervención por parte de un ente de control u otro ente regulador. Pérdida de información crítica para la entidad que no se puede recuperar. Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.	El evento materializado inminentemente produce la pérdida de confidencialidad, integridad o disponibilidad que puede: (i) causar una degradación mayor al 51% en la capacidad operativa de los procesos misionales, y la organización presenta dificultades para realizar sus funciones principales, pero la efectividad de estas reduce severamente. (ii) resultar en una gran pérdida financiera, calculada en más de diez (10) salarios mínimos mensuales legales vigentes. (iii) derivar en un riesgo alto para las personas, de acuerdo con los peligros y valoraciones establecidas por el sistema de seguridad y salud en el trabajo. (iv) Se ven afectados los tres criterios de seguridad de la información, de forma simultánea.

Fuente: Elaboración propia en la CNSC

Sin dejar de lado las consideraciones de impacto expuestas anteriormente, es posible que los riesgos tengan además una potencial afectación de la seguridad de la información, razón por la cual, se adoptan los siguientes criterios para que sean consideradas al valorar su impacto:

Tabla: Valoración de impacto potencial para cada criterio de seguridad de la información

Criterio de Seguridad	Moderado (3)	Mayor (4)	Catastrófico (5)
Confidencialidad	Podría esperarse que la revelación no autorizada de información tenga un efecto adverso **limitado** sobre las operaciones de la organización, los activos de la organización o los individuos.	Podría esperarse que la divulgación no autorizada de información tenga un efecto adverso **grave** en las operaciones de la organización, los activos de la organización o las personas. También, cuando de forma simultánea se vea afectada la integridad **o** la disponibilidad de la información.	Se puede esperar que la divulgación no autorizada de información tenga un efecto **severo o catastrófico** en las operaciones de la organización, los activos de la organización o las personas. También, cuando de forma simultánea se vea afectada la integridad **y** la disponibilidad de la información.
Integridad	Se puede esperar que la modificación o destrucción no autorizada de la información tenga un efecto adverso **limitado** en las operaciones de la organización, los activos de la organización o las personas.	Se puede esperar que la modificación o destrucción no autorizada de la información tenga un efecto adverso **grave** en las operaciones de la organización, los activos de la organización o las personas. También, cuando de forma simultánea se vea afectada la confidencialidad **o** la disponibilidad de la información.	Se puede esperar que la modificación o destrucción no autorizada de la información tenga un efecto adverso **severo o catastrófico** en las operaciones de la organización, los activos de la organización o las personas. También, cuando de forma simultánea se vea afectada la confidencialidad **y** la disponibilidad de la información.

Criterio de Seguridad	Moderado (3)	Mayor (4)	Catastrófico (5)
Disponibilidad	La interrupción del acceso o uso de la información o un sistema de información podría tener un efecto adverso **limitado** en las operaciones de la organización, los activos de la organización o las personas.	Se puede esperar que la interrupción del acceso o uso de la información o de un sistema de información tenga un efecto adverso **grave** en las operaciones de la organización, los activos de la organización o las personas. También, cuando de forma simultánea se vea afectada la confidencialidad **o** la integridad de la información.	Se puede esperar que la interrupción del acceso o uso de la información o de un sistema de información tenga un efecto adverso **severo o catastrófico** en las operaciones de la organización, los activos de la organización o las personas. También, cuando de forma simultánea se vea afectada la confidencialidad **y** la integridad de la información.

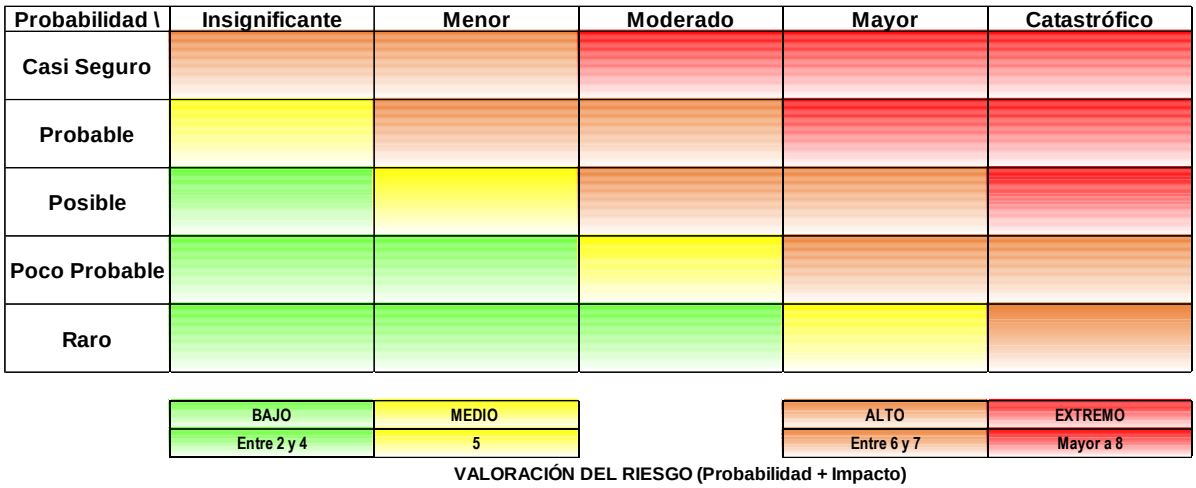
Fuente: Elaboración propia en la CNSC

Finalmente, en caso de requerir precisión en la valoración, es conveniente convocar a una mesa de trabajo en la que participe el dueño del riesgo, un representante del Sistema de Gestión de Seguridad de la Información y un representante del Sistema Integrado de Gestión, sin cerrar la posibilidad de convocar a otros expertos técnicos para apoyar los temas que sean pertinentes.

Valoración de exposición del riesgo

Para la CNSC, la forma en que calcula el valor de exposición del riesgo será la suma del nivel de probabilidad de ocurrencia y del nivel de impacto. Este valor se ubica en el siguiente mapa de calor:

MAPA DE CALOR DE LOS RIESGOS DE LA CNSC



Fuente: Elaboración propia en la CNSC

El eje X (horizontal) muestra el impacto y el eje Y (vertical) la probabilidad de ocurrencia. La intersección corresponde al nivel de riesgo inicial o inherente. Los colores hacen visible qué tan crítico es el riesgo en términos cualitativos, ubicando la intersección en verde si es **bajo**, amarillo si es **medio**, naranja si es **alto** o rojo si es **extremo.**

Por ejemplo, para un riesgo determinado, se obtiene la siguiente valoración, en términos de probabilidad de ocurrencia, e impacto:

Criterio de valoración	Valoración	Nivel
Probabilidad de ocurrencia	Poco probable	2
Impacto	Moderado	4

Fuente: Elaboración propia en la CNSC

El valor de exposición de este riesgo es seis (6), porque es la suma del nivel de probabilidad de ocurrencia (2) y del nivel de impacto (4). En el mapa de calor, esta intersección particular indica que el riesgo es alto.

Esta valoración del riesgo se hace con el fin de establecer prioridades para su manejo y tomar decisiones en cuanto a su tratamiento.

La forma de llevar a cabo esta valoración consistirá en invitar a un ejercicio participativo de en donde deben participar los servidores que por su grado conocimiento o experiencia respecto al proceso se consideren expertos. Se presentarán inicialmente los riesgos identificados, es decir la descripción del riesgo, las causas y sus potenciales consecuencias, para que revisen detalladamente esta información. A continuación, el servidor otorgará valores de probabilidad de ocurrencia para cada una de las causas y un valor de impacto general para el riesgo, según su experticia.

Las valoraciones realizadas por cada servidor serán consolidadas, como un promedio simple redondeado a un entero, calculando de esta forma el valor inherente del riesgo que será consignado en el mapa de riesgos.

A modo de ejemplo: dos servidores expertos del proceso Registro Público de Carrera Administrativa realizan el análisis y valoración para el mismo riesgo:

Riesgo	Causa	Consecuencia
Adulteración de la información del Sistema de control RPCA.	Ausencia de controles en la información Bajo compromiso y ética profesional	Declaración de derechos no constituidos en los términos establecidos por la ley

Fuente: Elaboración propia en la CNSC

Valoran la probabilidad de ocurrencia y el impacto, así:

Ejemplo de valoración por parte del servidor A.

Causa	Consecuencia	Probabilidad de ocurrencia	Impacto
Ausencia de controles en la información	Declaración de derechos no constituidos en los términos establecidos por la ley	1	3
Bajo compromiso y ética profesional		2	

Fuente: Elaboración propia en la CNSC

Ejemplo de valoración por parte del servidor B.

Causa	Consecuencia	Probabilidad de ocurrencia	Impacto
Ausencia de controles en la información	Declaración de derechos no constituidos en los términos establecidos por la ley	2	3
Bajo compromiso y ética profesional		3	

Fuente: Elaboración propia en la CNSC

En este caso, se suman las **valoraciones de probabilidad** de ambos servidores (1+2+2+3=8) y se divide por el número total de valoraciones para este criterio (2 valoraciones por 2 causas=4). Entonces, la valoración de este grupo de servidores equivale a 8 dividido entre 4, es decir, **2**.

De forma análoga se calcula la **valoración de impacto** para este grupo de servidores. La suma de las valoraciones (3+3=6), al dividirse entre el número total de valoraciones para este criterio (2 valoraciones por 1 riesgo=2) equivale a 6 dividido entre 2, es decir, **3**.

Como conclusión del ejercicio realizado por el grupo de servidores expertos, se obtiene una valoración de probabilidad de 2 (poco probable) y una valoración de impacto de 3 (moderado), por tanto, el valor de exposición para el riesgo del ejemplo equivale a **5**, se muestra en el mapa de calor en color **amarillo** y cualitativamente es **medio**.

4.3.2 Evaluación de riesgos

A partir del análisis del riesgo inicial, se identifica e implementa una o más acciones específicas, denominadas controles, que contribuyan a modificar la exposición al riesgo desde la primera línea de defensa, ya sea en la valoración de probabilidad de impacto o en la valoración de impacto.

Para la CNSC, los controles se encuentran en alguna de las siguientes categorías:

- **Preventivos:** aquellos que actúan para eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.

- **Correctivos:** aquellos que permiten el restablecimiento de la actividad, después de ser detectado un evento no deseable. También permiten la modificación de las acciones que propiciaron su ocurrencia.

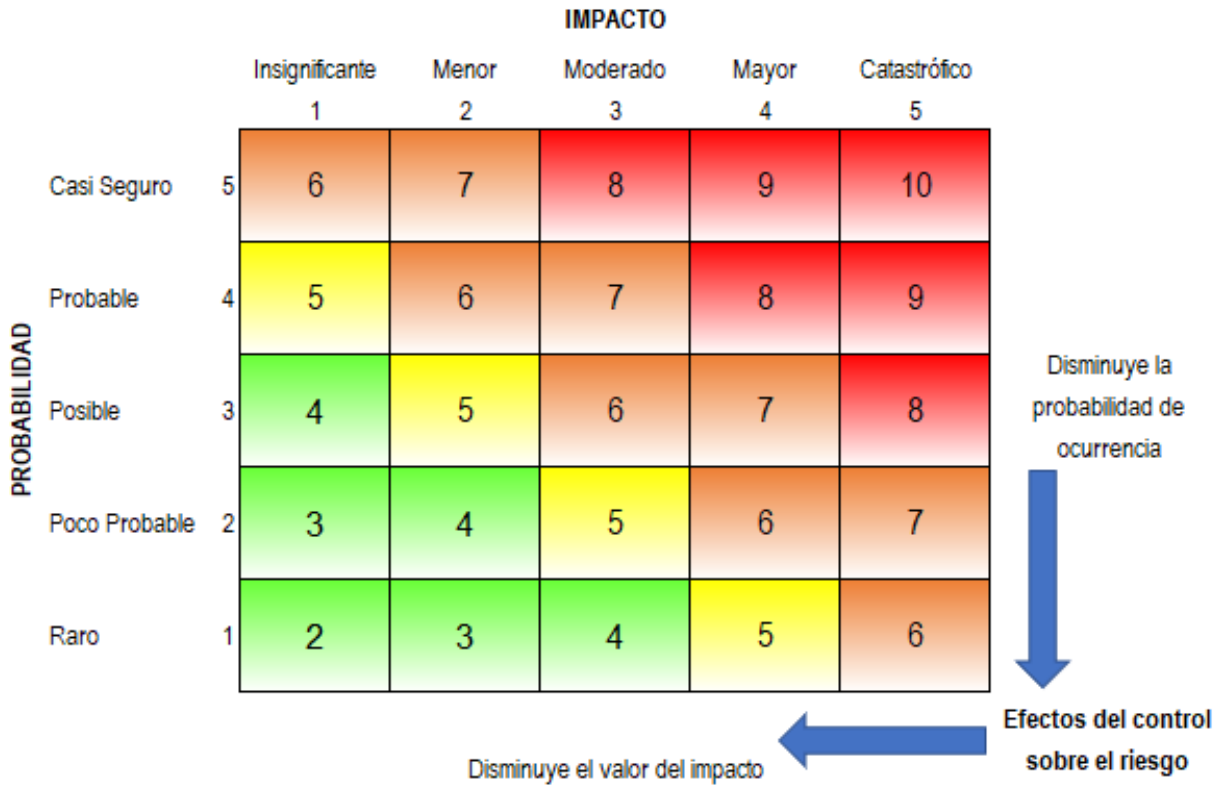
- **Automáticos:** aquellos que de forma automatizada anticipan la ejecución de las posibles causas que conlleven a la materialización del riesgo.

Cada control identificado deberá ser valorado en términos de su efectividad sobre el riesgo, de tal forma que para cada control será necesario identificar su naturaleza o categoría, la clase de control (respecto a la forma de uso o activación de este) y aplicación, en términos de identificar si modifica a la variable de probabilidad de ocurrencia, a la variable de impacto o ambas.

IMPORTANTE: La identificación y aplicación de los controles y salvaguardas deben modificar de alguna forma el valor del riesgo. En aquellos casos en donde el control existente no produzca un cambio significativo en el valor residual del riesgo, debe evaluarse la posibilidad de implementar controles adicionales, siempre que su implementación mantenga una adecuada relación costo / beneficio para el proceso y/o la entidad.

De igual forma, una vez sean identificados y valorados los riesgos de los procesos, aplicados los respectivos controles y salvaguardas y formulados y desplegados los planes de tratamiento de los riesgos que ameriten dicho complemento, se obtendrán un conjunto de valores residuales de exposición.

Como resultado de la evaluación de riesgos y análisis de los controles se asignará una calificación que permita saber con exactitud cuántas posiciones es posible desplazar el determinado riesgo, dentro del mapa de calor, en sentido favorable a la Comisión.



Fuente: Elaboración propia en la CNSC

Esta valoración, posterior a la implementación de controles, determinará las prioridades para el manejo o tratamiento de los riesgos y la fijación de políticas para la toma de decisiones en caso de que su valoración no mejore después de ser aplicado el tratamiento. El resultado de esta evaluación también hace parte del mapa de riesgos de la Entidad.

4.3.3 Estrategias para combatir el riesgo

Una vez conocido el valor residual de los riesgos, la CNSC adopta las siguientes respuestas de tratamiento:

- **Reducir:** implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles.

- **Evitar:** implica no proceder con la actividad que causa el riesgo o buscar alternativas para obtener beneficio del proceso.

- **Compartir:** reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido.

- **Aceptar:** no se adopta ninguna medida que afecte la probabilidad de ocurrencia o el impacto.

Zona	Valor residual cualitativo	Respuesta
Roja	Extremo	Plan de tratamiento para reducir, evitar, o compartir el riesgo.
Naranja	Alto	Plan de tratamiento para reducir, evitar, o compartir el riesgo.
Amarilla	Medio	Aceptar el riesgo o generar plan de tratamiento para reducir, evitar o compartir el riesgo.
Verde	Bajo	Aceptar el riesgo.

Fuente: Elaboración propia en la CNSC

Como acción por defecto para el tratamiento de cualquier riesgo, la CNSC establecerá controles para reducir su probabilidad de ocurrencia o su impacto.

Para los riesgos de corrupción, en todos los casos, la respuesta de tratamiento será evitar, compartir o reducir el riesgo.

4.3.4 Herramientas para la Gestión del Riesgo

La CNSC cuenta con diversas herramientas que permiten implementar la política de administración de riesgos, y realizar una adecuada gestión de riesgos en las etapas de identificación, valoración y comunicación.

Estas herramientas se implementan como formatos del SIG, y su manejo se describe a continuación:

Herramientas	Finalidad	Manejo
Mapa de riesgos	Identificar y valorar el riesgo, identificar los controles y la incidencia de éstos en el riesgo.	Por proceso, se registran los riesgos, especificando su tipo, causas y consecuencia. Estos se valoran en términos de probabilidad de ocurrencia e impacto para obtener el valor de exposición. Para cada riesgo se describe un control, en términos de su naturaleza, clase, y el criterio de valoración que afecta.

Herramientas	Finalidad	Manejo
		A partir de los valores ingresados se determina su efectividad, la indicación para ajustar el riesgo y se obtiene el valor residual del riesgo (tras aplicar el control).
Juicio de expertos para la valoración del riesgo	Facilitar el ejercicio de valoración de riesgos por parte de uno o más expertos	Se identifica el experto o conjunto de expertos que valorará el riesgo. Se entrega un formato a cada uno de los expertos para que identifique el riesgo que se analizará, a partir del código y su descripción, transcriba la secuencia de causas identificadas y la consecuencia del riesgo. Finalmente, el experto realiza la valoración de probabilidad de ocurrencia y la valoración de impacto, registrándolas en los campos correspondientes.
Plan de tratamiento de riesgos	Describir las acciones adicionales a los controles, para los riesgos con los valores de exposición más altos	Para los riesgos cuyo valor residual sea alto y extremo, se elige una política de tratamiento y se describe de forma clara la serie de actividades que conforman el plan. Luego, se delimita la actividad en términos de inicio y fin, se registran los recursos necesarios para llevarla a cabo y se define su responsable de ejecutar la acción.
Gestión ante la materialización del riesgo	Identificar acciones, procedimientos o mecanismos alternos para activar en caso de que el riesgo se materialice, y se pueda registrar de manera detallada los sucesos, consecuencias reales y acciones tomadas para contenerlo.	Para todos y cada uno de los riesgos identificados, se define el interesado que debe informarse acerca de la materialización del riesgo, en caso de presentarse. Adicionalmente, se describen tanto los pasos o acciones que se pueden adoptar en caso de que se materialice el riesgo, como relacionar los documentos que respaldan las posibles acciones de respuesta o contención que se hayan identificado.

Herramientas	Finalidad	Manejo
Mapa de riesgos de corrupción	Identificar y valorar los riesgos de corrupción, identificar los controles y la incidencia de estos en el riesgo.	Del mapa de riesgos se extraen los tipificados como de corrupción para cada proceso, junto con sus causas, consecuencia y valoración de probabilidad de ocurrencia. Con respecto al impacto, se aplica el cuestionario de criterios para calcular el impacto de riesgos de corrupción.
Cuestionario para calificar el impacto de riesgos de corrupción	Obtener una valoración cuantitativa del impacto del riesgo de corrupción a partir de preguntas formuladas desde el supuesto de materialización del riesgo.	Aplicar el cuestionario sobre cada riesgo de corrupción, a uno o más expertos del proceso. De acuerdo con el porcentaje de impacto obtenido, se extrapolará el valor de impacto del riesgo. Este valor se registra en el mapa de riesgos de corrupción para determinar la zona de riesgo en que se encuentra.

Fuente: Elaboración propia en la CNSC

4.3.5 Monitoreo y revisión de los riesgos

Como lo refiere la *Guía para la administración del riesgo y el diseño de controles en entidades públicas*, del DAFP, el monitoreo y la revisión de los riesgos, y en general toda la gestión del riesgo se desarrolla a través de un esquema de asignación de roles y responsabilidades, por líneas estratégicas y de defensa, que para la CNSC se adopta como se describe a continuación:

Aspecto	Línea estratégica	Primera línea de defensa	Segunda línea de defensa	Tercera línea de defensa
Composición CNSC	- La alta dirección, en cabeza del Comisionado Presidente, y el Comité de Coordinación de Control Interno.	- Servidores públicos de la CNSC. - Líderes de procesos, programas y proyectos.	- Oficina Asesora de Planeación. - Supervisores de contratos o proyectos. - Responsables de sistemas de gestión.	- Oficina de Control interno

Aspecto	Línea estratégica	Primera línea de defensa	Segunda línea de defensa	Tercera línea de defensa
Roles	- Define el marco para la gestión del riesgo y su control. Supervisa el cumplimiento de la gestión del riesgo y del control.	- Diseña, implementa y monitorea los controles. - Gestiona continua y directamente los riesgos.	- Soporta y guía a la línea estratégica y la primera línea de defensa en la gestión adecuada de los riesgos. - Monitorea la gestión del riesgo y control ejecutado por la primera línea de defensa.	- Proporciona información sobre el estado del sistema de control interno, con el enfoque basado en riesgos, incluida la operación de la primera y segunda línea.
Responsabili-dades	- Revisar cambios en el direccionamiento estratégico, que puedan generar nuevos riesgos o modificaciones a los ya identificados. - Hacer seguimiento a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. - Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.	- Revisar cambios en el direccionamiento estratégico o en el entorno, que puedan generar nuevos riesgos de sus procesos, programas y proyectos o modificaciones a los ya identificados, para la actualización de los mapas de riesgos. Identificar los activos de seguridad de la información en cada proceso. - Establecer las actividades de control. - Revisar en primer nivel el adecuado diseño de los controles. - Revisar que las actividades de control de sus procesos se encuentren	- Revisar cambios en el direccionamiento estratégico o en el entorno, que puedan generar nuevos riesgos de sus procesos, programas y proyectos o modificaciones a los ya identificados, para solicitar y apoyar la actualización de los mapas de riesgos, y realizar las recomendaciones a que haya lugar. - Análisis de los objetivos de la entidad, tanto del orden estratégico como de procesos. - Revisar el adecuado diseño de los controles, que se han establecido en la primera línea de defensa y hacer las recomendaciones a que haya lugar.	- Revisar cambios en el direccionamiento estratégico o en el entorno, que puedan generar nuevos riesgos de sus procesos, programas y proyectos o modificaciones a los ya identificados, con el fin de que se actualicen los mapas de riesgos por parte de los responsables. - Revisar el adecuado diseño de los controles, que se han establecido en la primera línea de defensa y hacer las recomendaciones a que haya lugar. - Revisar el riesgo inherente y residual de los procesos, programas y proyectos de la Entidad, y

Aspecto	Línea estratégica	Primera línea de defensa	Segunda línea de defensa	Tercera línea de defensa
	- Asegurarse de permear la gestión del riesgo en todos los niveles de la Comisión, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a esta gestión.	documentadas y actualizadas en los procedimientos. - Asegurar la ejecución de los controles. - Establecer una respuesta para el tratamiento de los riesgos. - Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de proceso, e identificar los posibles riesgos que se estén materializando. - Revisar y reportar los eventos de riesgos que se han materializado y las causas de estas situaciones.	- Hacer seguimiento y orientar sobre la inclusión y actualización de los controles en los documentos correspondientes. - Liderar, difundir y brindar asesoría acerca de la administración y gestión de los riesgos de todo tipo. - Consolidar el mapa de riesgos de corrupción a partir del mapa de riesgos de la CNSC	pronunciarse cuando la calificación de probabilidad de ocurrencia y/o impacto no sea coherente con los resultados de las auditorías realizadas, y realizar las recomendaciones a que haya lugar. - Verificar el reporte del seguimiento y las acciones de tratamiento referentes a los riesgos de corrupción. - Dar a conocer a toda la entidad el Plan Anual de Auditorías basado en riesgos y los resultados de la evaluación de la gestión del riesgo.

Fuente: Elaboración propia en la CNSC

El monitoreo:

- Es continuo, sin embargo, se revisarán los mapas de riesgos por lo menos una vez cada año, con el fin de identificar acciones pertinentes o actualizaciones.
- Evalúa que los controles sean eficaces y eficientes en el diseño y la operación.
- Detecta cambios en el contexto externo e interno que puedan exigir revisión de los controles y planes de tratamiento del riesgo, y establecer un orden de prioridades.
- También incluye las auditorías Internas llevadas a cabo por la Oficina de Control Interno.
- Permite la identificación de nuevos riesgos.

A su vez, las acciones de tratamiento resultantes del proceso de valoración de los riesgos pueden tener la participación de varios responsables, y están en capacidad de reportar, a los líderes de procesos, los resultados de la implementación de dichas acciones.

Gestión para la materialización de los riesgos

Tras haber realizado de una manera adecuada las tareas de identificación de los riesgos, la valoración de estos antes y después de identificar y aplicar controles, y de formular cuando sea pertinente planes de tratamiento, quedará latente la posibilidad de que una causa se manifieste, provocando que el riesgo se materialice.

Como un mecanismo de prevención, se requerirá que los procesos lleven a cabo la identificación de actividades que puedan atender, contener o mitigar dicho evento. Estas acciones de atención de uno o varios riesgos materializados deberán contar con responsables por acción y un mecanismo que permita ser aplicado durante dicho evento.

En el evento en que efectivamente se materialice un riesgo, el dueño del proceso deberá reportarlo en el menor tiempo posible.

Durante el periodo durante el cual es atendida la situación se ejecutarán las acciones de respuesta o de contención reportadas como gestión para la materialización de riesgo.

Una vez concluya el evento y se restablezca la normalidad operativa, se deberá analizar la(s) causa(s) raíz y valoración, tanto de las consecuencias reales de la materialización, como de la efectividad de las acciones que se formularon inicialmente para atender este tipo de eventos.

Cualquier evento que derive en la materialización de uno o varios riesgos en los procesos, conducirán a actualizar su mapa de riesgos, que incluya una revisión a la valoración de los riesgos.

El reporte oportuno de la materialización de riesgos puede ayudar a correlacionar eventos mayores y a desplegar contramedidas de contención o erradicación de causas que afecten la operación de la Entidad.

Seguimiento a la administración del riesgo

De forma cuatrimestral, e indistintamente de su tipificación, la CNSC hará seguimiento a todos sus riesgos, a partir de los roles y responsabilidades definidos para las líneas estratégica y de defensa. En esta responsabilidad son los gestores de los procesos establecidos dentro del Sistema Integrado de Gestión quienes efectúan la validación de comportamiento del control en los periodos que sean necesarios y reportan los resultados de los seguimientos cuatrimestrales, como mínimo.

Comunicación transversal

Con el fin de asegurar que la administración del riesgo se convierta en parte integral de la planeación de los procesos, programas y proyectos, la Oficina de Control Interno en coordinación con el Representante del Sistema Integrado de Gestión – SIG, desarrollará planes de capacitación y realizará las publicaciones que sean necesarias para lograr la interiorización y sensibilización de los servidores públicos hacia el tema de la administración del riesgo en la CNSC, con el apoyo de los procesos de comunicaciones y gestión del talento humano, de tal forma que se facilite su entendimiento y se informe a los interesados sobre cualquier cambio.

4.4 Administración del riesgo de corrupción

Durante el proceso de identificación del riesgo, se tendrá en cuenta que en su redacción concurran los siguientes componentes:

- la definición la acción u omisión,
- el elemento de uso del poder,
- el elemento de desviación de la adecuada gestión de lo público, y
- el elemento del beneficio privado.

A modo de ejemplo, acerca de cómo deben ser redactados los riesgos de corrupción, se plantea que al analizar el evento "posibilidad de recibir o solicitar cualquier dádiva o beneficio" y su configuración como riesgo de corrupción, se pueden determinar los componentes a través de la siguiente construcción:

Acción u omisión	Elemento de uso del poder	Elemento de desviación de la gestión de lo público	Elemento del beneficio privado
Posibilidad de recibir o solicitar cualquier dádiva o beneficio	Por parte del directivo	Celebrar un contrato	Generar un beneficio a nombre propio o de terceros

Fuente: Elaboración propia en la CNSC

Como resultado se obtiene como riesgo de corrupción, la posibilidad de recibir o solicitar cualquier dádiva o beneficio por parte del directivo, con el fin de celebrar un contrato generando un beneficio a nombre propio o de terceros.

La identificación de riesgos de corrupción será una consecuencia de la identificación y valoración de los riesgos de gestión y de seguridad de la información. Es decir, que, si durante la realización de las actividades de identificación o actualización de estos riesgos se encuentran elementos suficientes para tipificarlos como riesgo de corrupción, se procederá a adelantar la valoración y determinar las acciones de control en el mapa de riesgos de corrupción vigente en la Comisión.

En cuanto a la valoración de impacto del riesgo de corrupción, la CNSC siempre lo considera negativo, y determina su nivel como moderado, mayor o catastrófico.

Denominación	Afectación operativa	Afectación económica	Afectación de imagen
Moderado	El evento materializado impide el normal funcionamiento de la Presidencia o alguno de los Despachos de los Comisionados o en las Oficinas Asesoras o las Direcciones de la Comisión.	El evento materializado produce una pérdida de dinero o un sobrecosto calculado entre cinco (5) y hasta diez (10) salarios mínimos mensuales legales vigentes.	El evento materializado produce una reclamación de más de veintiséis (26) ciudadanos y/o una (1) entidad pública.

Denominación	Afectación operativa	Afectación económica	Afectación de imagen
Mayor	El evento materializado impide parcialmente el normal funcionamiento de la Comisión.	El evento materializado produce una pérdida de dinero o un sobrecosto calculado entre diez (10) y hasta veinticinco (25) salarios mínimos mensuales legales vigentes.	El evento materializado produce una reclamación de más de dos (2) entidades públicas y/o una institución de educación superior y/o un ente de control externo.
Catastrófico	El evento materializado impide totalmente el funcionamiento de la Comisión.	El evento materializado produce una pérdida de dinero o un sobrecosto calculado mayor a veinticinco (25) salarios mínimos mensuales legales vigentes.	El evento materializado produce una reclamación de más de dos (2) Instituciones de educación superior y/o un ente de control externo y/o el Congreso de la República.

Fuente: Elaboración propia en la CNSC

Con respecto al seguimiento y verificación de la gestión del riesgo de corrupción en la CNSC, serán adelantados por la Oficina de Control Interno, a través del mapa de riesgos de corrupción y de acuerdo con los lineamientos de la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* emitida por el DAFP. Su resultado se publicará en la página web de la Comisión o en un lugar de fácil acceso para el ciudadano, y la periodicidad de esta publicación se llevará a cabo dentro de los diez (15) primeros días hábiles de mayo, septiembre y enero.

4.5 Administración del riesgo de seguridad de la información

Con los propósitos de lograr tanto una aplicación unificada de criterios y acciones relacionadas con la administración de riesgos en la CNSC, y de desarrollar el Subsistema de Gestión de Seguridad de la Información articulado con el Sistema Integrado de Gestión de la CNSC, se aplicará la metodología de administración del riesgo, implementando tanto la política y sus lineamientos, como la identificación, valoración, y la comunicación de los riesgos de manera unificada, es decir que no existe otra guía o lineamiento para identificar, valorar o desplegar acciones de tratamiento de riesgos específicamente para los temas de seguridad de la información, puesto que todos los procesos entienden que este concepto es transversal a toda la Entidad.

Para efectos de precisión respecto a la seguridad de la información, cuando se evidencien las consecuencias potenciales o reales de materialización de riesgo, y cuando sea pertinente, dicha consecuencia se asociará al pilar de la seguridad de la información (*Confidencialidad, Integridad o Disponibilidad*) que pueda verse afectado, incluyendo esta afectación como una calificación más de las consecuencias de la materialización del riesgo. Para tener en cuenta esta calificación se pueden ver las posibles afectaciones al impacto asociadas a la seguridad de la información.

Ejemplo:

Riesgo	Causa	Consecuencia	Pilar de seguridad de la información
Adulteración de la información del Sistema de control RPCA.	Ausencia de controles en la información. Bajo compromiso y ética profesional.	Declaración de derechos no constituidos en los términos establecidos por la ley. Falsedad en la información	Integridad

Fuente: Elaboración propia en la CNSC

Los resultados de la identificación y valoración de los riesgos por proceso, deben ser un insumo para que la gestión de activos de información del proceso sea debidamente aplicada, según lo descrito en el procedimiento vigente para tal fin.

Es posible que durante la construcción o revisión del inventario de activos de información se identifiquen riesgos que no se habían contemplado en la revisión inicial, esto conlleva a realizar una actualización de la mencionada matriz de riesgos del proceso aplicando los pasos descritos en esta guía.

Para efectos de comprender mejor las afectaciones de los riesgos en la gestión de los activos de información, se debe tener en cuenta que por lo general las amenazas que puedan afectar al activo, pueden modificar el valor del impacto del riesgo asociado o identificado para esté. De otro lado, las vulnerabilidades que pueden afectar a un activo, por lo general afectan el valor de probabilidad de ocurrencia del riesgo asociado.

Cuando se asocian los riesgos a los activos de información, se facilita la identificación de los pilares de la seguridad que se deben resguardar para proteger a cada activo y, por tanto, se pueden validar y complementar la calificación en cada riesgo, manteniendo de esta forma consistencia en los valores y controles adoptados.

Los eventos de materialización de los riesgos que tengan alguna afectación a la seguridad de la información serán revisados a la luz del procedimiento de gestión de incidentes de seguridad de la información.

1.2 Niveles de aceptación del riesgo

La Comisión Nacional del Servicio Civil puede aceptar los riesgos cuyo valor de exposición sea medio o bajo, sin embargo, procurará establecer controles para todos los riesgos como buena práctica. Adicionalmente se debe consagrar la aceptación por parte de los lideres de proceso de los resultados de la valoración de los riesgos. Consecuentemente, los riesgos cuyo valor de exposición sea alto o extremo son prioritarios en el tratamiento y requieren la formulación de

planes concretos para complementar los controles, que se incluirán en la herramienta dispuesta por la Entidad para registrar los planes de tratamiento de riesgos.

Por otra parte, y en línea con lo establecido en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas*, emitida por el Departamento Administrativo de la Función Pública, la CNSC establece que los riesgos de corrupción son inaceptables y por tanto siempre requerirán la definición, implementación y seguimiento de medidas de control.

1.3 Conservación de los resultados de la gestión

Tanto los mapas de riesgos, como el mapa de riesgos de corrupción, herramientas de valoración, actas de trabajo, planes de tratamiento de riesgos, y acciones para gestionar la materialización de riesgos, serán remitidas por los líderes del proceso, programa o proyecto a la Oficina Asesora de Planeación para su custodia, como insumo para los seguimientos y demás acciones asignadas a la segunda línea de defensa, y podrá conservar una copia no controlada de los mismos, como insumo para las revisiones o actualizaciones posteriores. No obstante, en la intranet de la CNSC se publicará tanto el mapa de riesgos y en la página web el mapa de riesgos de corrupción.

El detalle de esta información podrá ser consultada por los dueños de cada proceso, por los auditores internos para los ejercicios de verificación y cumplimiento de procedimientos internos y por los entes de control que los requieran mediante una solicitud formal realizada a través del correo electrónico institucional o de la radicación de esta a través de los procedimientos de gestión documental relacionados y vigentes.

5 Control de Modificaciones

Versión	Fecha de Vigencia	Modificación Realizada	Solicitada por
2.0	20/08/2014	Actualización del manual en todos sus numerales	Jefe Oficina Asesora de Planeación
3.0	26/02/2016	Actualización del manual	Jefe Oficina Asesora de Planeación
4.0	30/05/2018	Actualización del manual para aclaración de parámetros de valoración, planes de tratamiento, asignación de responsables, acciones para atender la materialización de riesgos y planificación general.	Jefe Oficina Asesora de Planeación
5.0	11/06/2019	• Precisión del nombre. • Adaptación y ampliación del contenido de acuerdo con la Política de Administración del Riesgo en la CNSC aprobada por el Comité de Coordinación de Control Interno, y la *Guía para la administración del riesgo y el diseño de controles en entidades públicas,* cuya cuarta versión fue emitida por el DAFP en octubre de 2018.	Comité de Coordinación de Control Interno

		• Adecuación del contenido a plantilla usable y accesible.	
6.0	18/03/2022	• Se revisó y actualizó la guía teniendo en cuenta la guía de administración de riesgos – DAFP y la actualización de contexto de la entidad.	Jefe Oficina Asesora de Planeación

Elaboró	Revisó	Aprobó
Nombre: Nelsy Aracely Garzón Guzmán **Cargo**: Contratista **Dependencia:** Oficina Asesora de Planeación **Nombre:** Hugo Fernando Ramírez Ospina **Cargo:** Contratista **Dependencia:** Dirección de Tecnologías de la Información y las Comunicaciones	**Nombre:** José Jorge Roca Martínez **Cargo**: Jefe **Dependencia:** Oficina Asesora de Planeación	**Nombre:** José Jorge Roca Martínez **Cargo**: Jefe **Dependencia:** Oficina Asesora de Planeación