**TABLA DE CONTENIDO**

[1. INTRODUCCIÓN 1](#_Toc155883030)

[1.1. Antecedentes 2](#_Toc155883031)

[2. OBJETIVO 3](#_Toc155883032)

[2.1 Objetivos Específicos 3](#_Toc155883033)

[3 ALCANCE 4](#_Toc155883034)

[4 PRODUCTOS ESPERADOS 4](#_Toc155883035)

[5 TÉRMINOS Y DEFINICIONES 5](#_Toc155883036)

[5.1 Riesgo Operativo 5](#_Toc155883037)

[5.2 Riesgo Legal 5](#_Toc155883038)

[5.3 Riesgo Reputacional 5](#_Toc155883039)

[5.4 Definición de Factores de Riesgo 5](#_Toc155883040)

[6 Directrices Generales del SARO 6](#_Toc155883041)

[6.1 Responsabilidades 6](#_Toc155883042)

[6.2 Reunión Técnica de Administración de Riesgos 8](#_Toc155883043)

[7. Políticas de Administración de Riesgo Operativo 10](#_Toc155883044)

[7.1 Perfil de Riesgo 11](#_Toc155883045)

[7.2 Estructura Organizacional del SARO 11](#_Toc155883046)

[7.3 Política de Acceso y Administración de Usuarios 13](#_Toc155883047)

[7.4 Política de Seguridad de la Información 16](#_Toc155883048)

[7.5 Política de Prevención de Fraude y Corrupción 19](#_Toc155883049)

[7.6 Principios de Gestión del Riesgo Operativo 19](#_Toc155883050)

[7.7 Procedimiento de Gestión de Riesgo Operativo 19](#_Toc155883051)

[8 Metodologías para la Administración de Riesgo Operativo 21](#_Toc155883052)

[8.1 Procedimiento para la Identificación de Riesgos Operativos 22](#_Toc155883053)

[8.2 Medición de los riesgos operativos 24](#_Toc155883054)

[9 Autoevaluación de Riesgos y Controles Operativos 28](#_Toc155883055)

[10 Monitoreo de los Riesgos 28](#_Toc155883056)

[10.1 Registro de Eventos de Riesgo Operativo 28](#_Toc155883057)

[10.2 Inventario de Controles 29](#_Toc155883058)

[10.3 Evaluación de Controles 29](#_Toc155883059)

[11 Indicadores Claves de Gestión 30](#_Toc155883060)

[12 Seguros 31](#_Toc155883061)

[13 Seguridad de la Información 32](#_Toc155883062)

[14 Continuidad del Negocio 32](#_Toc155883063)

[15 HISTORIAL DE CAMBIOS 35](#_Toc155883064)

[16 APROBACIÓN 35](#_Toc155883065)

# INTRODUCCIÓN

El Manual de Gestión del Riesgo Operativo de la Dirección General de Crédito Público y Tesoro Nacional (DGCPTN) del Ministerio de Hacienda y Crédito Público (MHCP) describe las normas y/o principios generales que la Dirección usa en su administración del riesgo operativo. Este documento es parte integral de las políticas y los procedimientos del Ministerio que en su conjunto articulan un adecuado gobierno interno y la estructura de control.

Otras políticas y procedimientos de riesgo operativo más específicos podrán ser desarrollados dentro del marco establecido por esta manual, cuando sea necesario o apropiado. Se hace también referencia a otros documentos de política, presentados en la Sección 1.4, los cuales complementan las políticas descritas en este documento.

La Dirección General de Crédito Público y Tesoro Nacional en cumplimiento de sus responsabilidades, establece y aprueba procesos efectivos de gobierno interno, de gestión estratégica y de gestión de riesgos, para identificar, evaluar y supervisar debidamente las actividades operativas de la Dirección. Para ello, la Dirección General encarga a la Subdirección de Riesgos, del mantenimiento de políticas operativas sanas y prudentes para la consideración y aprobación, así como el desarrollo y ejecución de un programa de gestión de riesgo operativo efectivo.

### **Antecedentes**

En los últimos años con la globalización de los servicios financieros, la creciente sofisticación de las tecnologías, y la materialización de eventos de riesgo asociados directamente a las ejecución de operaciones, ha llamado la atención de los diferentes organismos de supervisión la adecuada administración del riesgo, en 1999 el Comité Conjunto de Estándares Australia / Estándares Nueva Zelanda OB-007 de Administración de Riesgos, documenta el estándar internacional para la administración del riesgo, de igual forma en 2006 el Comité de Supervisión Bancaria de Basilea publica el documento No. 2 “Convergencia internacional de medidas y normas de capital” el cual incluye en las estimaciones de capital para los bancos con actividad internacional, este documento recoge el Marco acordado para estimar la suficiencia de capital, así como los estándares mínimos a alcanzar, que las autoridades supervisoras de los países representados en el Comité presentarán para su adopción en sus respectivos países. Este Marco y los estándares en él recogidos, han contado con el respaldo de los Gobernadores de los Bancos Centrales y de los Jefes de Supervisión Bancaria del Grupo de los Diez[[1]](#footnote-1). En el ámbito nacional la Superintendencia Financiera de Colombia en 2006 publica la Circular Externa 048, la cual establece las Instrucciones Relativas a la Adopción de un Sistema de Administración de Riesgo Operativo (SARO). Para las entidades vigiladas, y crea el capítulo 23 de la circular 100 de 1995, posteriormente modificada por la Circular Externa 041 de 2007.

De acuerdo con lo anterior y con la evolución de las prácticas financieras, es necesario para los bancos o tesorerías adoptar mecanismos de administración del riesgo operativo con el fin de mitigar los riesgos, aparte de los riesgos de crédito, de tipos de interés, liquidez y de mercado.

# OBJETIVO

Establecer las políticas, metodologías, procedimientos y responsabilidades que se deben tener en cuenta en la operatividad de la Dirección General de Crédito Público y Tesoro Nacional por parte de todos los funcionarios de la Dirección.

## Objetivos Específicos

Proporcionar al Ministerio una herramienta que permita identificar, medir, controlar y monitorear el riesgo operativo, buscando minimizar las pérdidas, por la ocurrencia de acontecimientos internos o externos.

Con el desarrollo e implementación de la presente política lo que busca la Dirección es:

* Impulsar la cultura en materia de riesgo operativo.
* Prevenir la pérdida de recursos monetarios, mediante la debida y permanente identificación y control de los riesgos asociados.
* Identificar los cambios en los controles y los factores de riesgo operativo.
* Contar con una estructura organizativa que promueva la administración adecuada del riesgo operativo.
* Establecer una metodología que permita llevar a cabo la identificación, análisis, valoración, tratamiento, comunicación y monitoreo de dicho riesgo, contando con el apoyo de la Dirección General e involucrando a todos los colaboradores del Ministerio.
* Definir e identificar necesidades de capacitación, mayor conocimiento de los procesos, los sistemas de información y todo el ambiente necesario para la gestión del riesgo operativo.

# ALCANCE

Desde la definición de políticas a implementar a las operaciones de la Dirección General de Crédito Público y Tesoro Nacional, hasta la definición de lineamientos de riesgo operativo y los mecanismos de seguimiento a los controles establecidos en el presente manual para dichas operaciones.

# PRODUCTOS ESPERADOS

La adecuada aplicación de este manual le permitirá a la Dirección, entre otros aspectos los siguientes:

* Construir un adecuado ambiente de control para cada proceso.
* Identificar los Riesgos que puedan presentarse en el proceso y minimizarlos.
* Identificar las causas generadoras de los riesgos.
* Realizar una medición y una cuantificación de los riesgos inherentes y residuales a los procesos.
* Monitorear periódicamente los perfiles de riesgo y la exposición a posibles pérdidas que estos puedan originar.
* Reportar el resultado de los mapas de riesgo a las áreas o entidades interesadas.
* Mantener una base de datos de eventos de riesgos operativos materializados, con el fin de hacer seguimiento a la implementación de planes de acción de mitigación y documentar las lecciones aprendidas.
* Facilitar la cultura de autocontrol y ejecución de los procesos, que permita identificar fácilmente la ocurrencia de posibles fallas o deficiencias que originen pérdida directa o indirecta a la Dirección.
* Consolidar una cultura de riesgo en pro de optimizar los procesos y reducir la exposición a los riesgos.

# TÉRMINOS Y DEFINICIONES

* 1. Riesgo Operativo

De acuerdo con la CE 041 de 2007 expedida por la Superintendencia Financiera de Colombia, se entiende como el riesgo operativo, como 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. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores.[[2]](#footnote-2).

El riesgo operativo existe de alguna forma en cada una de las actividades y procesos de la Dirección, y puede resultar en pérdidas económicas, detrimento patrimonial, o daños a la reputación de la entidad.

### **Riesgo Legal**

Es la posibilidad de pérdida económica en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales.

El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones.

### **Riesgo Reputacional**

Es la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios[[3]](#footnote-3).

### **Definición de Factores de Riesgo**

Se entiende por factores de riesgo, las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operativo, estos factores se clasifican en Internos y Externos:

**Internos**

* **Recurso Humano**: Corresponde al conjunto de personas vinculadas directa (basada en un contrato de trabajo en los términos de la legislación vigente) o indirectamente (aquellas personas que tienen con la entidad una relación jurídica de prestación de servicios diferente a aquella que se origina en un contrato de trabajo) con la ejecución de los procesos de la entidad.
* **Procesos**: Corresponden a la interrelación ordenada de actividades para la transformación de elementos de entrada en productos o servicios, y así satisfacer una necesidad.
* **Tecnología**: Comprende las herramientas empleadas (hardware, software y telecomunicaciones) para soportar los procesos de la Dirección.
* **Infraestructura**: Es el conjunto de elementos de apoyo para el funcionamiento de una organización. Entre otros se incluyen: edificios, espacios de trabajo, almacenamiento y transporte.

**Externos**

* **Eventos externos**: Corresponde a la ocurrencia de eventos externos asociados a la fuerza de la naturaleza u ocasionado por terceros, que escapan en cuanto a su causa y origen al control de la entidad como fallas operativas en los proveedores o en las operaciones de *outsourcing*, incendios o desastres naturales, terrorismo, vandalismo, hurto, robo.

## Directrices Generales del SARO

Las políticas y directrices de gestión de riesgo operativo son transversales a todos los procesos de la Dirección General de Crédito Público y Tesoro Nacional, en búsqueda de las mejores prácticas que ha desarrollado el sector financiero en materia de gestión del riesgo operativo, las cuales le permiten a la Dirección identificar sus principales riesgos, evaluarlos, realizar planes de mitigación y retroalimentarlos periódicamente.

### **Responsabilidades**

La responsabilidad del riesgo operativo es de todos los funcionarios, contratistas y pasantes de la Dirección General de Crédito Público y Tesoro Nacional, en particular los dueños de los procesos deben velar porque se mitiguen los riesgos operativos que pueden originar pérdidas a la Nación.

#### Dirección General de Crédito Público y Tesoro Nacional

Es la encargada de dictar las directrices y políticas en cuanto a la administración de riesgos. En lo que respecta el sistema SARO, debe realizar las siguientes funciones:

1. Establecer las políticas relativas al SARO.
2. Aprobar el Manual de Riesgo Operativo y sus actualizaciones.
3. Hacer seguimiento y pronunciarse sobre el perfil de riesgo operativo de la Dirección.
4. Establecer las medidas relativas al perfil de riesgo operativo, teniendo en cuenta el nivel de tolerancia al riesgo de la Dirección.
5. Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente la Subdirección de Riesgo.
6. Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SARO.

#### Subdirección de Riesgo

Esta área designada por la Dirección de Crédito Público y Tesoro Nacional, tiene como objetivo administrar los riesgos operativos y apoyar a las áreas de la Dirección en la identificación, medición y control de los riesgos operativos. En este sentido, el área de Riesgos de la Dirección dentro del contexto de SARO tendrá a su cargo, como mínimo, las siguientes funciones:

1. Definir los instrumentos, metodologías y procedimientos tendientes a que la entidad administre efectivamente sus riesgos operativos.
2. Desarrollar e implementar el sistema de reportes, internos y externos, del riesgo operativo de la Dirección.
3. Administrar el registro de eventos de riesgo operativo.
4. Coordinar la recolección de la información para alimentar el registro de eventos de riesgo operativo.
5. Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los riesgos operativos medidos.
6. Establecer y monitorear el perfil de riesgo de la entidad e informarlo a la DGCPTN.
7. Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con el SARO y proponer sus correspondientes actualizaciones y modificaciones.
8. Desarrollar los modelos de medición del riesgo operativo.
9. Desarrollar los programas de capacitación de la Dirección relacionados con el SARO.
10. Capacitar a los gestores de riesgo de cada una de las áreas.
11. Realizar seguimiento a las medidas adoptadas para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.
12. Reportar semestralmente a la DGCPTN la evolución del riesgo, los controles implementados y el monitoreo que se realice sobre el mismo.

#### Gestores de riesgo

El gestor de riesgo es el funcionario designado por cada Subdirector para ser el enlace entre el área y la Subdirección de Riesgo, tiene como objetivo acompañar a los funcionarios en la identificación de los riesgos y diligenciar los formatos diseñados por la Subdirección de Riesgo, de igual forma comunicará a su respectivo Subdirector los riesgos identificados para su aprobación. En este sentido, el Gestor de Riesgos dentro del contexto de SARO tendrá a su cargo, como mínimo, las siguientes funciones:

1. Asistir a las capacitaciones que defina la Subdirección de Riesgos para divulgar la metodología y procedimientos para la gestión de riesgo operativo.
2. Retroalimentar a su jefe y compañeros de área, la información suministrada en las capacitaciones a las que asista.
3. Apoyar a los funcionarios de su Subdirección en el diligenciamiento del formato de identificación de riesgo y del formato de revelación de riesgo.
4. Coordinar la recolección de la información para alimentar el registro de eventos de riesgo operativo.
5. Informar al Subdirector de su área los planes de acción y controles propuestos para mitigar los riesgos.
6. Comunicar a la Subdirección de Riesgo los cambios en los riesgos operativos de su área, y apoyar en la profundización de la cultura de riesgo operativo en su área.

### **Reunión Técnica de Administración de Riesgos**

Con el fin de hacer seguimiento y control de los riesgos asociados a las actividades realizadas en la DGCPTN, se establece la Reunión Técnica de Administración de Riesgos la cual debe tener una periodicidad semestral, pero pueden ser citadas reuniones extraordinarias si las situaciones o eventos de riesgo lo requieren.

El área responsable de esta reunión será la Subdirección de Riesgo, quien se encargará de citar y coordinar lo relacionado con la agenda y la logística de cada reunión, para lo cual se dejará como memoria el documento objeto de análisis del día.

En esta reunión se presentará el perfil de riesgo inherente y residual de la DGCPTN, un resumen de los eventos de riesgo presentados durante el periodo y el seguimiento a los planes de acción de mitigación del riesgo operativo.

#### Integrantes

La Reunión estará conformada por los siguientes cargos:

• Director de Crédito Público y Tesoro Nacional, quien la presidirá

• Subdirector de Riesgo

• Subdirector de Tesorería

• Subdirector de operaciones

• Subdirector de financiamiento interno

• Subdirector de financiamiento externo

• Subdirector de operaciones

• Subdirector de Financiamiento con Organismos Multilaterales y Gobiernos

• Subdirector de Asociaciones Publico Privadas

• Subdirector de Financiamiento de Otras Entidades, Seguimiento, Saneamiento de Cartera

Podrán asistir como invitados, funcionarios o particulares que puedan hacer aportes en los asuntos tratados en la Reunión Técnica de Administración de Riesgos.

#### Funciones

Entre las funciones asignadas a esta Reunión, se destacan las siguientes:

* Servir como instancia de apoyo para la adecuada administración del riesgo de mercado, liquidez, emisor y contraparte, operativo, jurídico y demás que se consideren relevantes en relación con las actividades que realice la Dirección General de Crédito Público y Tesoro Nacional.
* Evaluar y dar concepto al Manual de riesgo Operativo, así como los cambios que requiera para la posterior aprobación (de la) Director(a) General de Crédito Público y Tesoro Nacional.
* Evaluar propuestas de nuevos límites o modificación de los aprobados y documentados en el Manual de Riesgo Operativo.
* Aprobar las metodologías de valoración y de medición de riesgo que debe elaborar la Subdirección de Riesgo. Así mismo, deberá aprobar los procedimientos y mecanismos de seguimiento al riesgo operativo que proponga dicha Subdirección.
* Analizar los resultados en materia de niveles de riesgo presentados por la Subdirección de Riesgo y proponer cursos de acción y estrategias relevantes para su mitigación y/o adecuada gestión.
* Analizar las propuestas sobre incursión en nuevos mercados, instrumentos, procedimientos o negocios en los cuales la Dirección de Crédito Público y Tesoro Nacional se encuentre interesada en participar con el objeto de formular las recomendaciones que se consideren pertinentes a el(la) Director(a) General de Crédito Público y Tesoro Nacional.
* Analizar cualquier sobrepaso a los límites establecidos y determinar el tratamiento que se les debe dar al mismo.
* Las demás que considere la Reunión Técnica de Administración de Riesgos.

## Políticas de Administración de Riesgo Operativo

Para la DGCPTN, los principales lineamientos para mitigar los riesgos operativos a los que se encuentra expuesta son:

* Realizar como mínimo una capacitación anual de asistencia obligatoria para todos los funcionarios de la DGCPTN liderada por la Subdirección de Riesgo.
* Realizar una capacitación semestral de asistencia obligatoria para los gestores de riesgo de cada área.
* Los dueños de los procesos deben establecer y documentar los procesos, procedimientos e instructivos en cada una de las áreas. Se deben segregar las funciones con el fin de prevenir los posibles conflictos de interés o duplicidad de actividades.
* Identificar, documentar, y actualizar junto con los gestores de riesgo de cada una de las áreas, los riesgos de cada uno de los procesos y la descripción de los controles aplicados a los mismos, en los mapas de riesgo.
* Estructurar un plan de continuidad de negocio, y efectuarle pruebas de funcionamiento anuales.
* Contar con personal calificado para el desarrollo de las actividades, siguiendo las directrices del MHCP.
* Garantizar las herramientas para la adecuada administración de riesgo operativo.
* Fomentar una cultura de riesgo operativo, partiendo de las capacitaciones y la intervención de los gestores al interior de cada una de las áreas.

Todos los funcionarios de la DGCPTN tienen el deber de:

* Reportar los eventos de riesgo operativo que tengan conocimiento.
* Conocer los riesgos operativos y controles definidos, en el desarrollo de sus funciones.
* Cumplir con las disposiciones aprobadas en los planes de acción para mitigar los riesgos operativos.
* Asistir a las capacitaciones de riesgo operativo que programe la Subdirección de Riesgo.

Adicional a lo anterior, la DGCPTN cuenta con el Sistema Único de Gestión (SUG) que permite identificar claramente los procedimientos y las funciones del personal, por área y su responsabilidad en la organización.

### **Perfil de Riesgo**

El nivel de riesgo operativo permitido para la DGCPTN es el perfil moderado que corresponde a riesgos de ocurrencia no muy frecuente, aunque probable; para los cuales existen adecuados controles y planes de contingencia.

### **Estructura Organizacional del SARO**

La gestión de riesgo operativo es transversal a todas las Subdirecciones de la DGCPTN, por ende, todos los subdirectores apoyados con la Subdirección de Riesgo administrarán los riesgos de cada uno de sus procesos y procedimientos definidos en el SUG.

Los principales agentes u organismos identificados en la gestión del riesgo operativo son: 1. Reunión de Administración de Riesgos, 2. El Director General de Crédito Público y Tesoro Nacional, 3. Subdirecciones de la DGCPTN, 4. La Subdirección de Riesgo, y 5. Los gestores de riesgo de cada una de las áreas. El siguiente esquema resume las relaciones de autoridad y control de estos organismos.

Reunión de Admón de Riesgos

**Director de Crédito Público y Tesoro Nacional**

Subdirección de Riesgo

***Middle Office***

8 Subdirecciones y Grupo de Asuntos Legales

***Front* y *Back Office***

Gestores de Riesgo

Línea de autoridad:

Línea de control:

La DGCPTN cuenta con una estructura organizacional de acuerdo a sus funciones y se encuentra dividida en 8 subdirecciones las cuales cuentan con el apoyo del Grupo de Asuntos Legales, como se muestra a continuación:

### **Política de Acceso y Administración de Usuarios**

* El jefe de cada dependencia (Director, Subdirector o Coordinador de Grupo) elaborará la programación de vacaciones de los funcionarios de su área la cual será enviada al enlace administrativo para que este consolide la programación de las vacaciones de todos los funcionarios de la Dirección para firma del director quien posteriormente enviará a la Subdirección de Recursos Humanos, con visto bueno de la DGCPTN, verificando que cada funcionario disfrute de su periodo de vacaciones. En casos debidamente justificados, por necesidades del servicio, se podrán suspender las vacaciones después de disfrutar como mínimo diez (10) días hábiles continuos por cada año de servicio, de conformidad con las garantías establecidas por la póliza de Infidelidad y Riesgos Financieros-IRF-
* Se podrá acumular hasta dos periodos de vacaciones, siempre que la acumulación obedezca a necesidades del servicio. Será responsabilidad del jefe de la dependencia, que los funcionarios no tengan más de dos periodos de vacaciones acumulados, para lo cual podrá programarlas de oficio, acordando con el funcionario entre varias alternativas, la fecha del disfrute. Si no hay acuerdo el jefe fijará la fecha y la comunicará a la Subdirección de Recursos Humanos
* Por cada periodo acumulado, el tiempo mínimo de disfrute de vacaciones es de diez (10) días hábiles
* La interrupción o el aplazamiento de vacaciones debe contar con el visto bueno de la DGCPTN, motivando las razones que justifican tal situación
* Queda prohibido el acceso a las instalaciones de la DGCPTN mientras los funcionarios se encuentren en alguna situación administrativa: vacaciones, incapacidades, licencias y/o permisos. En caso de requerir el ingreso, atendiendo a las necesidades del servicio, el mismo, debe ser autorizado por Director General de Crédito Público y Tesoro Nacional y, en estos eventos, se solicitará por parte del jefe Inmediato a la Subdirección de Recursos Humanos la expedición del respectivo acto administrativo que autorice el ingreso con copia al administrador de usuarios de la DGCPTN. (Se exceptúa la situación administrativa de incapacidad)
* Los funcionarios, contratistas y pasantes adscritos a la DGCPTN, son las únicas personas autorizadas para ingresar a las instalaciones de la DGCPTN, las demás personas que para el cumplimiento de sus funciones requieran ingresar de manera permanente por un tiempo determinado, deberán gestionar el permiso de acceso con el jefe del área donde van a desarrollar sus funciones y tramitar el acceso a través del administrador de usuarios de la DGCPTN, con la debida justificación
* Los proveedores, visitantes, contratistas, así como el personal externo al MHCP que requieran ingresar a la DGCPTN, deberán anunciarse en la recepción de la misma, y requerirán autorización del jefe del área del funcionario que visita
* Los visitantes deben entrar acompañados con la(s) persona(s) de la Dirección, la(s) cual(es) será(n) la(s) responsable(s) de las actividades que estos realicen en las instalaciones
* Se prohíbe el acceso a personal no autorizado a las instalaciones de la DGCPTN (funcionarios, vendedores o personal externo no autorizado)
* Todos los funcionarios deben tramitar ante el administrador de usuarios de la DGCPTN, la desactivación y activación de las tarjetas de ingresos por concepto de ingresos, retiros, traslados, vacaciones, incapacidades, licencias y/o permisos
* Queda prohibido el préstamo de las tarjetas de aproximación, para el desplazamiento en las dependencias de la DGCPTN
* Todos los funcionarios deben tramitar ante el administrador de usuarios de los sistemas de información de la DGCPTN la respectiva habilitación, modificación y deshabilitación para los ingresos, retiros, traslados, vacaciones, incapacidades, licencias y/o permisos, siguiendo el procedimiento establecido en los formatos diseñados para cada uno de los sistemas de información, registrando el tipo de la novedad
* Las contraseñas tendrán una vigencia máxima de un año, contado a partir de la fecha de la solicitud, para tal efecto, el usuario efectuará el respectivo cambio antes del vencimiento del término, de acuerdo con los formatos establecidos
* El manejo de las contraseñas es de naturaleza privada y exclusiva del funcionario autorizado. No podrá ser divulgada, compartida, ni cedida, sin importar la jerarquía de la persona que la solicite
* Todo acceso y perfil requerido para un funcionario de la DGCPTN, deberá corresponder con las funciones y labores que esté desarrollando el usuario
* Todo acceso y perfil definido por un área de la DGCPTN deberá contemplar un usuario principal (quien realiza diariamente la actividad) y dos *backup* en caso que el usuario principal NO pueda realizar la labor, a quien se realizará previamente la inducción correspondiente
* Las contraseñas deben ser memorizadas, sin dejar evidencia escrita de las mismas por cuanto la responsabilidad de su utilización indebida o no, recaerá en el funcionario titular, quien responderá legal y disciplinariamente por su utilización
* Toda novedad de habilitación, deshabilitación y/o modificación del perfil de un usuario a un aplicativo, deberá solicitarse por el área usuaria al administrador de usuarios de la DGCPTN indicando el tipo de novedad.
* Cada novedad debe ser aprobada por el Jefe Inmediato, con visto bueno del subdirector correspondiente. Para los subdirectores y/o coordinadores que dependan del despacho de la Dirección, dicha novedad debe ser aprobada por el Director General de Crédito Público y Tesoro Nacional
* Todos los funcionarios deben preparar un instructivo que contenga de forma clara las actividades que desarrolla en cumplimiento de sus funciones, y deberá capacitar a los funcionarios que servirán como *backup* de sus funciones, antes del inicio de cada situación administrativa, salida de vacaciones y por lo menos una vez cada semestre
* Todos los funcionarios deben tener definido dos *backup* y servir de *backup* de acuerdo a las funciones que realizan, las funciones de respaldo, no pueden generar un posible conflicto de interés, o ningún tipo de concentración de funciones.

### **Política de Seguridad de la Información**

* La Política de Seguridad de la Información al interior del Ministerio requiere que todos los sistemas de la entidad sean formalmente evaluados con relación a los requerimientos de *integridad, confidencialidad, disponibilidad y continuidad*. Deben establecerse arreglos de continuidad acorde con el nivel de riesgo inherente en cada sistema. Es responsabilidad de cada subdirector de área velar por la correcta implementación de medidas de seguridad de la información dentro de sus respectivas áreas
* La confidencialidad de la información del Ministerio de Hacienda y de los clientes o contrapartes (incluyendo información confidencial interna) es protegida a través de una combinación de códigos, políticas y medios físicos, organizacionales y tecnológicos, tales como candados, contraseñas, controles de acceso y encriptación de archivos
* Dar estricto cumplimiento al trámite de habilitación, modificación y des habilitación de los usuarios a los diferentes aplicativos, para lo cual deben tramitar ante los correspondientes Administradores la respectiva habilitación, modificación y des habilitación por concepto de ingresos, retiros, traslados, vacaciones, incapacidades, licencias y/o permisos, siguiendo el procedimiento establecido en los formatos diseñados para cada uno de los Sistemas registrando el tipo de la novedad
* Las contraseñas tendrán una vigencia máxima de un año contado a partir de la fecha de la solicitud. Para tal efecto, el usuario efectuará el respectivo cambio antes del vencimiento de este término
* El manejo de las contraseñas es de naturaleza privada y exclusiva del funcionario autorizado. No podrá ser divulgada, compartida, ni cedida, sin importar la jerarquía de la persona que la solicite
* Todos los usuarios deben ser identificados independientemente con permisos de accesos específicos e individualmente autorizados por razones básicas de la función misional con sus respectivas atribuciones; esta autorización debe estar basada en los principios del “*need-to-know*” (necesidad de saber) y “*least privilege*” (menor privilegio). Los métodos de acceso de usuarios deben exigir un proceso robusto de autenticación, autorización apropiada y auditoria confiable
* Todo acceso y perfil definido por un área de la DGCPTN deberá contemplar un usuario principal (quien realiza diariamente la actividad) y un backup en caso que el usuario principal no pueda realizar dicha labor previa inducción
* Toda novedad de habilitación, deshabilitación y/o modificación del perfil de un usuario a un aplicativo, deberá solicitarse por el área usuaria al administrador del sistema, indicando el tipo de novedad. Dicha novedad deberá ser aprobada por el jefe Inmediato, visto bueno del subdirector correspondiente. Para los subdirectores y/o coordinadores que dependan del Despacho, la novedad debe ser aprobada por la DGCPTN
* La información debe ser protegida con el nivel necesario en proporción a su valor y el riesgo para la función misional. La protección debe concentrarse en las propiedades de confidencialidad, integridad y disponibilidad de la información
* Los recursos tecnológicos deben ser protegidos con el nivel necesario en proporción a su valor y el riesgo para la función misional. Dichos recursos deben ser utilizados exclusivamente para desarrollar las actividades laborales de los funcionarios y terceras partes; esta utilización debe hacerse en forma adecuada, con el máximo de eficiencia y con ejemplar racionalidad
* Los usuarios, dueños y custodios de los activos de información del MHCP son responsables por el uso apropiado, protección y privacidad de estos activos. Los sistemas de información del MHCP deben generar y mantener pistas apropiadas de auditoría para identificar usuarios y documentar los eventos relacionados con incidentes de seguridad
* Para que la seguridad de la información sea efectiva, se requiere el esfuerzo de equipo, donde deben participar en forma activa todos los funcionarios que tengan interacción con los activos de la información de la entidad. Todos los funcionarios y terceras partes deben cumplir con las políticas de seguridad de la información y, además, desempeñar un papel activo para su comprensión, entendimiento y divulgación
* En forma periódica la DGCPTN debe efectuar las revisiones necesarias para evaluar el cumplimiento de las diferentes políticas de seguridad. Esta tarea debe ser realizada por la Subdirección de Riesgo
* El uso indebido de la información que los funcionarios conocen o administran es una falta grave sujeta a las sanciones disciplinarias y/o legales que surjan de su utilización. La información soportada por la infraestructura de tecnología informática del MHCP pertenece a la entidad, a menos que en una relación contractual se establezca lo contrario. Sin embargo, la facultad de otorgar acceso a la información es del responsable de la dependencia que genera o es propietaria de esta información
* La información propiedad del MHCP y sobre la cual tiene sus derechos, podrá ser suministrada a los entes de control pertinentes cuando estos lo requieran, con previa autorización expresa y aprobada para estos fines por las directivas de la entidad
* Para efectos de control del flujo de la información de los procesos de la entidad, se asignarán responsables de la información, quienes deben asegurar y otorgar acceso a la información que genere su dependencia, con el fin de lograr un adecuado ambiente de control y de segregación de funciones
* En caso de divulgación no autorizada de la información de propiedad del MHCP, se realizarán las investigaciones pertinentes para establecer las responsabilidades del caso y proceder conforme lo establece para estos casos la normatividad y los procedimientos del MHCP.

Por cada incumplimiento de las políticas aquí definidas, se dará traslado a la Oficina de Control Disciplinario Interno, con el propósito de que se inicien las acciones disciplinarias correspondientes.

### **Política de Prevención de Fraude y Corrupción**

* En la DGCPTN no se tolera ni el fraude ni la corrupción, por lo tanto, se han adoptado los mecanismos necesarios para evitarlos; mediante la implementación de controles y sistemas para su detección prevención y respuestas oportunas ante tales acciones
* Los mecanismos para evitar el fraude y la corrupción están integrados al SARO, comprendiendo que estos están en el marco del factor de riesgo del recurso humano de la DGCPTN
* Los riesgos de fraude y/o corrupción deben ser identificados en todos los procesos de la DGCPTN y deben ser incluidos en el mapa de riesgos del SMGI.

### **Principios de Gestión del Riesgo Operativo**

* El Riesgo Operativo es parte de las responsabilidades asumidas por los encargados de las direcciones y subdirecciones del Ministerio, de los procesos, de los sistemas y/o de los productos. Es un hecho que debe reflejarse en el seguimiento de los controles, en la concientización de riesgos y en el estilo de gerenciamiento a diario
* Las tareas y responsabilidades de manejo del Riesgo Operativo deben ser acordadas e incluidas en los objetivos de todos los encargados de las áreas, procesos, sistemas y/o productos
* Los funcionarios en todos los niveles de la entidad deben ser conscientes de sus responsabilidades en relación a los riesgos operativos
* Las políticas y metodologías están vigentes para asegurar la consistencia y promover las buenas prácticas en la administración del riesgo operativo
* La responsabilidad en la adecuada administración y gestión del riesgo operativo es de todos los funcionarios del Ministerio, quienes en su día a día conocen bien sus procesos y pueden identificar los posibles riesgos a que están expuestos.

### **Procedimiento de Gestión de Riesgo Operativo**

Para la DGCPTN la gestión del riesgo parte de un ambiente de auto control en cada uno de los procesos y procedimientos a su cargo, de acuerdo a este ambiente ha definido tres líneas de defensa para la gestión del riesgo operativo de la siguiente manera:

Para ejecutar las tres líneas de defensa de la Dirección, la Subdirección de Riesgo utilizará la metodología de gestión del riesgo documentada por la norma NTC 5254 de 2006 que es una traducción idéntica de la norma técnica australiana AS/NZ 4360:2004 de amplio reconocimiento mundial, esta norma establece los principales elementos del proceso de gestión de riesgo de la siguiente manera:

Diagrama

Descripción generada automáticamente

**Comunicación y Consulta**. Comunicar y consultar con interesados internos y externos según corresponda en cada etapa del proceso de administración de riesgos y concerniendo al proceso como un todo.

**Establecer el contexto.** Establecer el contexto interno y externo de la gestión del riesgo en el cual tendrá lugar el resto del proceso.

**Identificar riesgos.** Identificar qué, por qué y cómo pueden surgir las cosas como base para análisis posterior.

**Analizar riesgos.** Determinar los controles existentes y analizar riesgos en términos de consecuencias y probabilidades en el contexto de esos controles. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que ocurran esas consecuencias. Consecuencias y probabilidades pueden ser combinadas para producir un nivel estimado de riesgo.

**Evaluar riesgos.** Comparar niveles estimados de riesgos contra los criterios preestablecidos.

**Tratar los riesgos.** Aceptar y monitorear los riesgos de baja prioridad. Para otros riesgos, desarrollar e implementar un plan de administración específico que incluya consideraciones de fondeo, reduciendo pérdidas potenciales.

**Monitoreo y revisión.** Es necesario monitorear la eficacia de todas las etapas del proceso de gestión del riesgo. Esto es importante para la mejora continua.

## Metodologías para la Administración de Riesgo Operativo

Para administrar adecuadamente los riesgos operativos es necesario obtener información acerca de las áreas que potencialmente tengan un mayor impacto en la gestión de riesgos operativos, donde se permita un adecuado análisis, para poder determinar las causas que afecten los procesos, conocer acerca de la efectividad de los controles o las medidas que los minimizan y a través de las herramientas también permitir un buen monitoreo de la implementación o el desarrollo de los planes de acción que se llevan a cabo. Entre los principales objetivos de estas metodologías están:

* Identificar, Evaluar, Mitigar y Monitorear los diferentes riesgos operativos
* Crear una cultura proactiva en búsqueda de las mejores prácticas que presenta el mercado
* Generar conciencia de los riesgos relacionada con el nivel y naturaleza de las pérdidas operativas
* Realizar un registro e información gerencial de las pérdidas operativas reales y/o potenciales
* Identificar exposición del Ministerio en relación a los distintos tipos de riesgo operativo
* Ser un insumo de información fundamental para el análisis en la toma de decisiones
* Aplicar dentro de los procesos más significativos del Ministerio las mejores prácticas para prevenir los posibles riesgos operativos asociados.

### **Procedimiento para la Identificación de Riesgos Operativos**

Para la identificación de riesgos los funcionarios de la DGCPTN acompañados por el gestor de riesgo del área, basados en las actividades descritas en los procesos y procedimientos del SUG, mediante el método Delphi o juicio de expertos documentarán en el formato de identificación de riesgo o de registro de evento de riesgo los riesgos a los que se encuentran expuestos en sus procesos, los cuales deben ser comunicados y avalados por el dueño del proceso. Este formato debe ser enviado a la Subdirección de Riesgo para incluirlos en los mapas de riesgo de la Dirección.

La Subdirección de Riesgo, incluirá el riesgo en el mapa de riesgos de la Dirección y hará seguimiento a los controles implementados o por implementar para mitigar el riesgo.

Cuando se identifica un riesgo operativo cada funcionario que ejecuta el proceso debe documentar en el formato de identificación de riesgo.

El gestor de riesgo brindará al funcionario el apoyo en el diligenciamiento del formato en cuanto a la calificación del riesgo y la propuesta de controles para mitigar el riesgo.

El subdirector del área revisará los riesgos identificados y aprobará los controles propuestos para mitigar el riesgo.

La DGCPTN aprobará el perfil de riesgo operativo y hará seguimiento a su evolución.

De acuerdo a la guía para la administración de riesgos del Ministerio, la definición de las causas es de gran relevancia para lograr una adecuada administración del riesgo. Son las causas, los factores a eliminar o mitigar, para que el riesgo no se materialice, mediante la definición de controles efectivos. Dichas causas deben ser analizadas en la etapa de identificación o incluso cuando un riesgo se ha materializado.

Para tal fin, se utiliza la metodología del diagrama de Ishikawa (espina de pescado), es un método que permite visualizar de manera estructurada todas las causas posibles del riesgo mediante el análisis desde los agentes generadores de riesgo.





### **Medición de los riesgos operativos**

Los criterios para efectuar la medición de los riesgos son los siguientes:

**Probabilidad de ocurrencia**: La unidad de medida será: Raro, Improbable, Moderado, Probable, Casi Certeza. Para establecer la probabilidad de ocurrencia, se deberá tener en cuenta si se han presentado eventos de riesgo de manera permanente, esporádica o recurrente.

**Impacto**: La unidad de medida para el impacto será: Insignificante, Menor, Moderado, Mayor y Catastrófico y se califica teniendo en cuenta sus efectos económicos, reputacional, legal y operativo.

Los niveles de cada una de las escalas de medición serán definidos por la Subdirección de Riesgo de acuerdo a criterios estadísticos.

Una vez se realice la medición de la probabilidad y del impacto para los riesgos de cada proceso por las áreas responsables, la Subdirección de Riesgo revisará la calificación dada y debe realizar la medición consolidada para la Dirección, determinando el perfil de Riesgo Inherente.

#### Definición de los niveles de riesgo operativo.

Los riesgos evidenciados, deberán clasificarse conforme a los anteriores criterios empleando la matriz de riesgo definida. La DGCPTN manejará los siguientes niveles para determinar el impacto de los riesgos operativos según la escala que relaciona probabilidades de ocurrencia e impacto:



Para determinar la probabilidad de ocurrencia de los riesgos se utilizarán las siguientes escalas:



Los riesgos evidenciados, deberán clasificarse conforme las anteriores escalas empleando la matriz de riesgo definida:



|  |  |  |
| --- | --- | --- |
|  | Riesgo Extremo | Riesgos con frecuencia de ocurrencia alta; no existen los suficientes controles y planes de contingencia, o los actuales resultan insuficientes. (No Aceptado por la DGCPTN.) |
|  | Riesgo Alto | Riesgos que pueden tener o no una frecuencia de ocurrencia alta, pero que comparten el hecho de que los controles actuales y planes de contingencia pueden mejorarse. (No Aceptado por la DGCPTN.) |
|  | Riesgo Moderado | Riesgos de ocurrencia no muy frecuente, aunque probable; para los cuales existen adecuados controles y planes de contingencia. |
|  | Riesgo Bajo | Corresponden a aquellos riesgos de ocurrencia poco probable, para los cuales existen adecuados controles y planes de contingencia |

## Autoevaluación de Riesgos y Controles Operativos

La DGCPTN, establece las autoevaluaciones de riesgos y controles operativos como un medio para asegurar que las personas integrantes de las unidades significativas identifiquen y evalúen: *a*) sus riesgos operativos más significativos basándose en el impacto potencial del riesgo y *b*) la efectividad de los controles relacionados a dichos procesos.

Las evaluaciones de todas las unidades o áreas significativas de la Dirección se realizan periódicamente, con el fin de determinar los cambios que se puedan presentar de un periodo a otro. El programa provee una base para que la alta Dirección evalúe si existen controles y procesos apropiados, y establezca si estos son efectivos para mitigar el riesgo operativo de forma continua; de no ser así se deben tomar acciones correctivas apropiadas.

De igual forma la Subdirección de Riesgo, periódicamente realiza el monitoreo de las actividades de control establecidos en los procesos y procedimientos formalizados en el SUG, utilizando el formato de evaluación de controles.

## Monitoreo de los Riesgos

Periódicamente se realizará el seguimiento por parte de la Subdirección de Riesgo, con el fin de evaluar el cumplimiento a los controles establecidos y medir la eficiencia y eficacia de dichos controles mediante los siguientes mecanismos:

### **Registro de Eventos de Riesgo Operativo**

Todos los funcionarios de la DGCPTN son responsables cuando tengan conocimiento o evidencien la materialización de un evento de riesgo operativo de reportarlo a la Subdirección de Riesgo, la cual documentará el evento de riesgo con las evidencias que envíen las áreas, diligenciando el acta de registro del evento con la siguiente información:

• Proceso

• Subproceso

• Responsable del proceso

• Quien detecta el evento

• Fecha de descubrimiento

• Fecha de inicio del evento

• Fecha de finalización del evento

• Riesgo asociado

• Descripción del evento

• Tipo de Impacto

• Cuantificación del impacto

• Causa principal generadora del evento

• Causa secundaria

• Descripción de la causa

• Acción correctiva

• Descripción de la acción correctiva

• Acción preventiva

• Descripción de la acción preventiva

• Responsable de implementar la acción

• Lecciones aprendidas

• Que salió bien

• Que se puede mejorar

La Subdirección de Riesgo llevará una base de datos con esta información y hará seguimiento a la implementación de los planes de acción para mitigar los riesgos.

### 

### **Inventario de Controles**

La Subdirección de Riesgos hará un inventario de controles de acuerdo con la información documentada en los procedimientos de la Dirección, a los controles sin documentar que se evidencien en las visitas de campo que realizará en cada una de las subdirecciones y a los planes de acción que se documenten en las actas de revisión de eventos de riesgo.

Este inventario lo monitoreará la Subdirección de Riesgos, cada área copiará a la Subdirección de Riesgo el reporte de ejecución del control cada vez que lo realice cuando el control es manual, para los controles que se ejecutan en una plataforma tecnológica, la Subdirección de Riesgo realizará el monitoreo mediante la consulta de los reportes y *log* de auditoria de cada plataforma.

### **Evaluación de Controles**

La Subdirección de Riesgo realizará la evaluación de controles periódicamente, mediante la visita a cada una de las subdirecciones de acuerdo a la criticidad de cada proceso o la frecuencia de la materialización de los riesgos operativos, esta evaluación revisará los siguientes aspectos en cada control:

* Consecuencias y frecuencia por la omisión del control
* Nivel de relevancia del control
* Evaluación del diseño del control
* Tipo de control
* Nivel de cobertura del control
* Frecuencia de ejecución del control
* Línea del control.

De acuerdo a esta evaluación se medirá la efectividad y eficiencia del control la cual determinará el *score* del riesgo residual, tanto en su frecuencia como en el impacto.

## Indicadores Claves de Gestión

También conocidos por sus siglas en inglés como KRI´s (*Key Risk Indicators*). Los indicadores de riesgo claves son métricas, con frecuencias financieras, que pueden proporcionar información sobre la posición de riesgo operativo que puede afrontar la DGCPTN.

Estos indicadores son determinados con base en factores como los siguientes:

* Alcance y significancia del riesgo que se está midiendo
* Importancia para la Alta Dirección.

El indicador principal de riesgo operativo será el perfil de riesgo residual de la DGCPTN, la fórmula de cálculo será el valor promedio de la probabilidad y del impacto de todos los riesgos evaluados después de aplicar controles como se muestra a continuación:

|  |  |  |
| --- | --- | --- |
|  | Riesgo Extremo | Riesgos con frecuencia de ocurrencia alta; no existen los suficientes controles y planes de contingencia, o los actuales resultan insuficientes. (No Aceptado por la DGCPTN.) |
|  | Riesgo Alto | Riesgos que pueden tener o no una frecuencia de ocurrencia alta, pero que comparten el hecho de que los controles actuales y planes de contingencia pueden mejorarse. (No Aceptado por la DGCPTN.) |
|  | Riesgo Moderado | Riesgos de ocurrencia no muy frecuente, aunque probable; para los cuales existen adecuados controles y planes de contingencia. |
|  | Riesgo Bajo | Corresponden a aquellos riesgos de ocurrencia poco probable, para los cuales existen adecuados controles y planes de contingencia |

El nivel aceptado por la DGCPTN es el riesgo moderado, de igual forma se debe calcular el perfil de riesgo residual de cada proceso de la DGCPTN y cada Subdirección, para identificar alertas tempranas en cada proceso.

Las distintas áreas de la Dirección pueden utilizar estos indicadores para identificar y vigilar los riesgos operativos de mayor significancia y las tendencias resultantes pueden indicar algunas alertas tempranas. Estos indicadores pueden ayudar en la previsión de ocurrencia de riesgos específicos. Por ejemplo, los indicadores pueden señalar problemas en un determinado proceso que podrían implicar pérdidas operativas, lo que puede dar lugar a adoptar nuevas medidas en pos de reducir los efectos de riesgos no cubiertos.

Estos indicadores deberán ser preventivos y reflejar las causas potenciales de riesgo operativo, como pueden ser un crecimiento acelerado, la implementación de nuevos productos, la rotación de los efectivos, interrupciones en las operaciones, interrupciones en el sistema, etc. Cuando estos indicadores se asignan a unos límites máximos, un proceso de seguimiento eficaz puede ayudar a identificar los principales riesgos de forma transparente y permitir que la entidad reaccione ante los mismos de forma adecuada.

## Seguros

Al interior del Ministerio de Hacienda y Crédito Público existen otras normas o políticas que hacen parte de la gestión del Riesgo Operativo y que ayudan a la Dirección a fortalecer su gestión con el fin de evitar posibles pérdidas no esperadas.

La Dirección cuenta con pólizas de seguros para la mitigación de riesgos, como una manera de transferir el riesgo de pérdidas de alta severidad. Estas pólizas de seguros son desarrolladas para equilibrar el costo de cobertura con el grado de mitigación de riesgo, teniendo en cuenta la medida en que el riesgo es realmente reducido.

Cada una de las áreas debe conocer las condiciones de cumplimiento de la póliza y acatar las políticas creadas para la adecuada cobertura de los riesgos.

## Seguridad de la Información

Adicional a las políticas definidas anteriormente, la seguridad de la información en la DGCPTN será administrada siguiendo los siguientes principios básicos que fundamentan las políticas de seguridad de la información para la infraestructura tecnológica del MHCP:

**Autenticidad:** La información requerida para el cumplimento de las funciones del MHCP debe ser veraz y estar debidamente autorizada

**Confiabilidad:** La información procesada por del MHCP tiene carácter confiable

**Confidencialidad:** La información del MHCP debe estar debidamente protegida para que solo el personal autorizado tenga acceso

**Disponibilidad:** Los activos de información deben estar disponibles para soportar los objetivos de la función misional del MHCP

**Integridad:** Los activos de información deben estar adecuadamente protegidos para asegurar su completitud y precisión. Las medidas de validación definidas deben permitir detectar las modificaciones inapropiadas, la eliminación o la adulteración de los activos de información

**No Repudio:** Los activos de información deben estar provistos de mecanismos que permitan probar que una acción o un evento han tenido lugar y no puedan ser negados posteriormente

**Trazabilidad:** El MHCP requiere que se pueda realizar seguimiento de los cambios de la información y se identifiquen los agentes de cambio

Estos principios se encuentran documentados en la política de seguridad de la información del MHCP la cual hace parte integral de este documento.

## Continuidad del Negocio

El plan de continuidad del negocio (o sus siglas en inglés BCP, por *Business Continuity Plan*) es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcialmente o totalmente interrumpidas dentro de un tiempo predeterminado, después de una interrupción no deseada o desastre. El Plan de Continuidad del Negocios busca mantener un nivel aceptable de servicios en caso de fallas internas o externas, que puedan afectar a nuestros clientes o contrapartes. Por este motivo se busca:

* Minimizar las interrupciones a la operación normal
* Minimizar el impacto económico de la interrupción
* Establecer las Normas, Procedimientos e Instructivos para manejar la contingencia
* Identificar y entender las amenazas, riesgos y las medidas para cubrir los mayores riesgos minimizando rupturas materiales
* Mantener los planes individuales tratando con amenazas específicas que pueden levantarse durante una crisis
* Detallar los procedimientos que serán adoptados por el Ministerio en caso de una contingencia
* Proporcionar las medidas de mitigación de riesgo y la continuidad comercial planeando reducir posibles pérdidas

El plan de continuidad del negocio está compuesto por los siguientes planes, los cuales hacen parte integral de este documento:

* 1. **Plan de Atención de Emergencias**

Es el plan definido por el Ministerio de Hacienda y Crédito Público, contempla las contramedidas necesarias durante la materialización de una amenaza que atenten contra la integridad de los funcionarios, este plan esta administrado por la Dirección Administrativa del Ministerio.

### 

* 1. **Plan de Manejo de Crisis**

Es el plan definido por la DGCPTN para mitigar el riesgo reputacional al que se encuentra expuesta la Dirección. Define el procedimiento para atender la crisis y la cadena de comunicación.

### 

* 1. **Plan de Contingencia Tecnológica**

Define las acciones de recuperación en la continuidad de las operaciones en los sistemas de información que el MHCP tiene en producción en el menor tiempo y reduciendo el impacto en las operaciones del Ministerio. Es administrado por la Dirección de Tecnología.

* 1. **Plan de Contingencia Operativo**

Tiene como finalidad documentar las actividades, procesos y procedimientos requeridos para atender los procesos críticos, ante un escenario que impida el cumplimiento de los objetivos del proceso. Adicionalmente proporciona los mecanismos y herramientas alternas para cumplir con las obligaciones contractuales adquiridas por la nación.

# HISTORIAL DE CAMBIOS

| **FECHA** | **VERSIÓN** | **DESCRIPCIÓN DEL CAMBIO** | **ASESOR SUG** |
| --- | --- | --- | --- |
| 27-03-2019 | 1 | Creación del documento | Tatiana Santos Yate |
| 08-02-2024 | 2 | Se actualiza el documento en el formato institucional y se modifica la sección 6.2 Reunión Técnica de Administración de Riesgos, en cuanto a la periodicidad de trimestral a semestral, modificación solicitada por la Subdirección de Riesgo. | Claudia Umbarila Rodríguez |

# APROBACIÓN

|  |  |
| --- | --- |
| **ELABORADO POR:** | **Nombre:** John Neftali Mojica Morales  **Cargo:** Profesional Especializado  **Fecha:** 10-01-2024 |
| **REVISADO POR:** | **Nombre:** Johanna Eunice Murcia Gutierrez  **Cargo:** Subdirectora de Riesgo  **Fecha:** 10-01-2024 |
| **APROBADO POR:** | **Nombre:** Jose Roberto Acosta Ramos  **Cargo:**Director General de Crédito Público y Tesoro  Nacional  **Fecha:** 10-01-2024 |

1. El Comité de Supervisión Bancaria de Basilea, creado en 1975 por los Gobernadores de los bancos centrales del Grupo de los Diez, está compuesto por altos representantes de autoridades de supervisión bancaria y de bancos centrales de Alemania, Bélgica, Canadá, España, Estados Unidos, Francia, Italia, Japón, Luxemburgo, Suecia, Suiza, los Países Bajos y el Reino Unido. Sus reuniones suelen celebrarse en la sede del Banco de Pagos Internacionales en Basilea (Suiza), donde está ubicada su Secretaría. [↑](#footnote-ref-1)
2. Basilea en su definición de Riesgo Operativo incluye el Riesgo Legal pero excluye el Riesgo Reputacional. [↑](#footnote-ref-2)
3. Circular Externa 041 de 2007 de la Superintendencia Financiera. [↑](#footnote-ref-3)