

# **Departamento Administrativo Nacional de Estadística**



## **Sinergia Organizacional SIO**

**GUÍA DE ADMINISTRACIÓN DE RIESGOS.**

**Jul/2021**

	<b>GUÍA DE ADMINISTRACIÓN DE RIESGOS.</b>		<b>CÓDIGO: SIO-040-GUI-002</b> <b>VERSIÓN: 1</b> <b>FECHA: 7/Jul/2021</b>
<b>PROCESO: Sinergia Organizacional</b>		<b>SUBPROCESO: Implementación y Mantenimiento</b>	

## **TABLA DE CONTENIDO**

- 1. INTRODUCCIÓN**
- 2. OBJETIVO**
- 3. ALCANCE**
- 4. DESCRIPCIÓN DE TAREAS**
  - 4.1. Establecer la política de administración de riesgos**
  - 4.2. Identificar riesgos**
    - 4. 2. 1. Establecer el contexto**
    - 4. 2. 2. Identificar riesgos**
  - 4.3. Valorar riesgos**
    - 4. 3. 1. Analizar riesgos**
      - 4. 3. 1. 1. Criterios para determinar la probabilidad de los riesgos**
      - 4. 3. 1. 2. Criterios para determinar el impacto de los riesgos**
    - 4. 3. 2. Evaluar riesgos**
      - 4. 3. 2. 1. Valorar el nivel de riesgo inherente**
      - 4. 3. 2. 2. Determinar y evaluar controles**
      - 4. 3. 2. 3. Valorar el nivel de riesgo residual**
    - 4. 3. 3. Monitorear y hacer seguimiento a los riesgos y a la efectividad de los controles**
  - 4.4. Comunicación y consulta**
  - 4.5. Aspectos complementarios para la administración de riesgos de seguridad de la información**
- 5. DEFINICIONES**
- 6. REGISTROS**
- 7. BIBLIOGRAFIA**
- 8. ANEXOS**

## **1. INTRODUCCIÓN**

La presente guía es un documento complementario de la política y del procedimiento de administración de riesgos, la cual pretende ampliar la descripción de las actividades necesarias para la administración de los riesgos de gestión, de corrupción y de seguridad de la información que se pueden presentar en los programas, proyectos o procesos del DANE – FONDANE. Estas actividades conforman un marco metodológico, cuyo desarrollo requiere la aplicación de una serie de aspectos técnicos para realizar adecuadamente la identificación y valoración de los riesgos.

Es importante tener en cuenta que la política de administración de riesgos establece la gobernanza de la administración de los riesgos de gestión, de corrupción y de seguridad de la información de la entidad, la cual opera bajo un modelo de líneas de defensa que establece los roles y las responsabilidades de todos los actores entorno a la administración de riesgos. En el DANE-FONDANE operan cuatro líneas de defensa, las cuales son:

- La línea estratégica, conformada por la alta dirección de la Entidad y el Comité Institucional de Coordinación de Control Interno.
- La primera línea de defensa, compuesta por los líderes de procesos, directores territoriales, responsables de programas, de proyectos y sus equipos de trabajo (servidores públicos y contratistas a nivel nacional).
- La segunda línea de defensa, de la cual hacen parte la Oficina Asesora de Planeación, el Comité de Seguridad de la Información, el responsable de seguridad de la información y la Oficina Asesora Jurídica.
- Y la tercera línea de defensa, conformada por la Oficina de Control Interno.

Por su parte, el procedimiento de administración de riesgos tiene como objetivo establecer las actividades necesarias para administrar los riesgos que se pueden presentar en los programas, proyectos o procesos del DANE – FONDANE. Este procedimiento se hace operativo a través de tres herramientas para identificar, valorar y monitorear los riesgos de gestión, de corrupción y de seguridad de la información, y fueron diseñadas atendiendo el marco metodológico descrito en la presente guía. Estas herramientas son: formato mapa de riesgos de gestión, formato mapa de riesgos de corrupción y formato mapa de riesgos de seguridad de la información.

## **2. OBJETIVO**

Establecer un marco metodológico para la administración de riesgos que oriente a las líneas de defensa en la identificación y valoración de los riesgos de gestión, de corrupción y de seguridad de la información a los que están expuestos los programas, proyectos o procesos del DANE y del FONDANE.

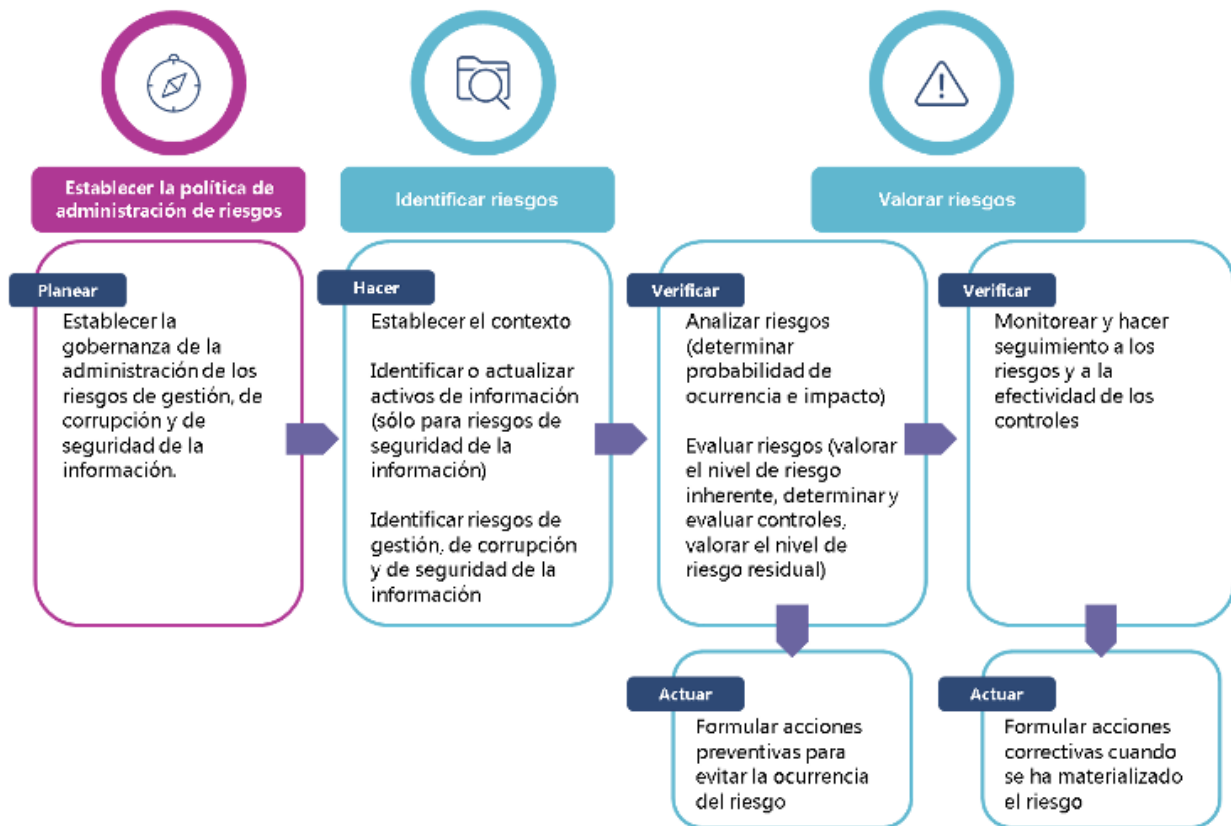
## **3. ALCANCE**

Los lineamientos contenidos en la presente guía, aplican para la administración de los riesgos de gestión, de corrupción y de seguridad de la información del DANE-FONDANE.

## **4. DESCRIPCIÓN DE TAREAS**

El marco metodológico de la administración de riesgos en el DANE y FONDANE se desarrolla siguiendo un conjunto de actividades en forma secuencial, las cuales se basan en la Guía para la administración del riesgo y el diseño de controles del Departamento Administrativo de la Función Pública - DAFP. Este marco metodológico está comprendido por tres grandes etapas que son: el establecimiento de la política de administración de riesgos, la identificación de riesgos y la valoración de riesgos, como se muestra en la siguiente imagen.

Imagen 1. Marco metodológico para la administración de riesgos



Fuente: Adaptado del Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 (p. 13).

#### 4.1. Establecer la política de administración de riesgos

La primera etapa del marco metodológico de riesgos consiste en establecer una política que contiene la gobernanza de la administración de riesgos traducida en roles y responsabilidades que se deben seguir para una adecuada identificación, valoración, tratamiento y seguimiento de los riesgos de gestión, de corrupción y de seguridad de la información (los cuales incluyen riesgos de seguridad digital), que pueden presentarse en los programas, proyectos o procesos del DANE – FONDANE.

#### 4.2. Identificar riesgos

La segunda etapa del marco metodológico de riesgos consiste en el establecimiento del contexto y la identificación de riesgos.

##### 4. 2. 1. Establecer el contexto

El contexto estratégico constituye la base para identificar los eventos que se podrían presentar o suceder y las consecuencias que tendrían sobre el cumplimiento de la misión, de los objetivos institucionales, de los planes de acción o el normal desarrollo de los procesos; el análisis del contexto estratégico se realiza a partir del conocimiento del entorno externo e interno en el que opera la entidad.

En el contexto externo, se realiza un análisis de amenazas considerando factores políticos, económicos y financieros, sociales y culturales, tecnológicos, ambientales, legales y reglamentarios. Una amenaza es toda

aquella circunstancia, fenómeno o situación que puede ocasionar un daño o poner en peligro el logro de los propósitos institucionales aprovechando una vulnerabilidad. Las amenazas son situaciones externas e inciertas, que no sabemos si van a ocurrir y sobre las cuales la entidad no tiene incidencia sobre su ocurrencia o magnitud.

En el contexto interno se analizan las debilidades, considerando los siguientes factores: financieros, personal, procesos, tecnología, estratégicos, comunicación, estructura organizacional, relacionamiento con grupos de interés, cultura organizacional, infraestructura, entre otros. También es importante considerar aspectos relacionados con el contexto del proceso, como por ejemplo: su objetivo, alcance e interrelación con otros procesos, sus procedimientos asociados y sus responsables. Particularmente, las fallas o debilidades asociadas a estos factores se consideran como vulnerabilidades que hacen a la entidad susceptible a la acción de las amenazas.

#### **4. 2. 2. Identificar riesgos**

La identificación de riesgos se realiza a partir del análisis del contexto, concretamente de las amenazas y las vulnerabilidades. Este análisis del contexto debe surgir naturalmente de un ejercicio de autocontrol del proceso; no obstante, otras fuentes que se pueden considerar para la identificación de riesgos son: cambios en el Sistema Integrado de Gestión, resultados de indicadores de gestión, informes de auditoría de organismos de control externos, informes de seguimiento, de evaluación y de auditorías internas, medición de la satisfacción de los grupos de interés, PQRSD, revisión por la dirección y resultados del análisis de salidas no conformes.

Un riesgo de gestión es la posibilidad de ocurrencia de algún evento que impida o afecte el normal desarrollo de las actividades y que tendrá un impacto sobre el cumplimiento de la misión, de los objetivos institucionales, de los planes de acción o el normal desarrollo de los procesos, entre otros aspectos.

Para identificar un riesgo hay que preguntarse ¿qué podría suceder?, o ¿qué podría salir mal?, es decir, de qué forma se podrían ver afectados los procesos o los objetivos institucionales como resultado de la acción de las amenazas sobre las vulnerabilidades.

A su vez, los riesgos de gestión se subclasifican de la siguiente manera:

Tabla 1. Tipología de riesgos de gestión

<b>Tipo de riesgo</b>	<b>Definición</b>
<b>Riesgos estratégicos</b>	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad. Estos riesgos están asociados a la administración de la Entidad, al cumplimiento de la misión y de los objetivos estratégicos y a la definición de políticas y de lineamientos.
<b>Riesgos gerenciales</b>	Posibilidad de ocurrencia de eventos que afecten a los procesos estratégicos y/o a la alta dirección.
<b>Riesgos operativos</b>	Es la posibilidad de ocurrencia de eventos, que tienen un impacto sobre el cumplimiento de los objetivos o el normal desarrollo de los procesos. Estos riesgos se encuentran íntimamente ligados a las actividades que se desarrollan en la entidad y a los productos y servicios que ofrece.
<b>Riesgos financieros</b>	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, costos, etc. Están relacionados con el manejo de recursos, la ejecución presupuestal, la elaboración de los estados financieros, los pagos y manejos de excedentes de tesorería.
<b>Riesgos tecnológicos</b>	Posibilidad de ocurrencia de eventos que afecten la infraestructura y capacidad tecnológica de la entidad.
<b>Riesgos de cumplimiento</b>	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la entidad debido al incumplimiento o desacato de la normatividad legal y de las obligaciones contractuales; se asocian con el cumplimiento de requisitos legales, contractuales, de ética pública y en general con el compromiso de la entidad frente a sus grupos de interés.
<b>Riesgo de imagen o reputacional</b>	Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de la entidad ante sus clientes y partes interesadas; están relacionados con la percepción y la confianza por parte de los grupos de interés con respecto a la gestión de la entidad.

Fuente: Adaptado de Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 (p. 28).

Un riesgo de corrupción es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. Las prácticas corruptas pueden ser realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y en la administración de los bienes públicos o en general, por cualquier persona que tenga la intención de cometer un acto de corrupción. Para identificar un riesgo de corrupción, es necesario que en la descripción del riesgo concurren los componentes de su definición: ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO O PARA UN TERCERO.

Para establecer riesgos de seguridad de la información es necesario identificar y clasificar los activos de información, implementando la guía para la identificación, clasificación y valoración de activos de información establecida por la Alta Dirección de la Entidad. En los mapas de riesgos de seguridad de la información se

incluyen los activos catalogados como críticos o que requieren mayores niveles de protección. Estos mapas se elaboran por cada proceso de acuerdo con su competencia y gobernanza sobre los activos, es decir para todos los procesos se incluyen riesgos asociados a los activos: información y hardware de escritorio; para el proceso de gestión de bienes y servicios se incluye adicional a estos los activos de: instalaciones y servicios de TI en lo concerniente al acceso físico; por último para el proceso de gestión tecnológica se incluyen los activos de: servicios de TI, la información de usuario, software, hardware de infraestructura crítica, redes de comunicación, dispositivos de almacenamiento de datos, equipamiento auxiliar, claves criptográficas y log (registro de actividad).

Los activos de información catalogados como reservados o clasificados se incluyen en el mapa de riesgos de seguridad de la información; así mismo se incluyen los activos considerados críticos para el funcionamiento de la Entidad, además se incluyen los activos que se relacionan directamente con el centro de datos del DANE definido como infraestructura crítica cibernética- ICC.

Otro aspecto importante a identificar, son las consecuencias que puede tener el riesgo, es decir, los efectos que tendría en caso de que llegara a materializarse; estos se traducen en pérdidas económicas, afectaciones a los servidores, sanciones, multas, demandas, cese de actividades, reprocesos, retrasos, entre otras.

### **4.3. Valorar riesgos**

La tercera etapa del marco metodológico de riesgos se refiere a la valoración de riesgos, la cual comprende el análisis, evaluación, el monitoreo y seguimiento de los riesgos.

#### **4. 3. 1. Analizar riesgos**

El análisis de los riesgos, consiste en determinar su probabilidad de ocurrencia e impacto aplicando los criterios establecidos por el DAFP (para riesgos de gestión y de corrupción) y por el Ministerio de Tecnologías de la Información y las comunicaciones – MinTIC (para riesgos de seguridad de la información).

##### **4. 3. 1. 1. Criterios para determinar la probabilidad de los riesgos**

Para establecer la probabilidad, es necesario analizar qué tan posible es que ocurra el riesgo en términos de frecuencia o de factibilidad. La entidad adapta los criterios de probabilidad sugeridos por el DAFP en la Guía para la administración de riesgo y el diseño de controles en las entidades públicas y por el MinTIC en la Guía de orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, Territoriales y Sector Público.

La siguiente tabla indica los criterios para establecer la probabilidad de ocurrencia de los riesgos de gestión y de corrupción:

Tabla 2. Criterios para establecer la probabilidad de ocurrencia de los riesgos de gestión y de corrupción

Probabilidad	Frecuencia	Factibilidad
Es la estimación en términos probabilísticos de que un riesgo se materialice.	El riesgo puede haberse materializado antes; por lo tanto, podrá determinar la probabilidad de ocurrencia del riesgo con base en un criterio de frecuencia. Para tal fin, debe considerar la cantidad de riesgos ocurridos en un periodo determinado o contar con un historial que permita demostrar el nivel de probabilidad.	En este caso, debe tener en cuenta que el riesgo no se ha presentado pero es posible que suceda.
Casi seguro	El riesgo ha ocurrido más de 1 vez al año.	El evento ocurrirá en la mayoría de las circunstancias.
Probable	El riesgo ha ocurrido por lo menos 1 vez en el último año.	Se espera que el riesgo ocurra en la mayoría de las circunstancias o podría ocurrir varias veces.
Posible	El riesgo ha ocurrido por lo menos 1 vez en los últimos 2 años.	El evento puede ocurrir en algún momento.
Improbable	El evento ha ocurrido por lo menos 1 vez en los últimos 5 años.	El evento puede ocurrir bajo circunstancias excepcionales. Es poco común o frecuente.
Rara vez	El evento no se ha presentado en los últimos 5 años.	La posibilidad de ocurrencia es casi nula o es posible que no se haya presentado.

Fuente: Adaptado de Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 (p. 39).

Tabla 3. Criterios para establecer la probabilidad de ocurrencia de los riesgos de seguridad de la información

Probabilidad	Frecuencia	Factibilidad
Casi seguro	La situación se ha presentado una vez a la semana	El evento ocurrirá en la mayoría de las circunstancias.
Probable	La situación se ha presentado una vez al mes	Se espera que el riesgo ocurra en la mayoría de las circunstancias o podría ocurrir varias veces.
Posible	La situación se ha presentado una vez cada semestre	El evento puede ocurrir en algún momento.
Improbable	La situación se ha presentado una vez cada año	El evento puede ocurrir bajo circunstancias excepcionales. Es poco común o frecuente.
Rara vez	La situación ha presentado 1 vez cada 5 años	La posibilidad de ocurrencia es casi nula o es posible que no se haya presentado.

Fuente: Adaptado de Guía de orientación para la Gestión de Riesgos de Seguridad Digital en el Gobierno Nacional, Territoriales y Sector Público.

#### 4. 3. 1. 2. Criterios para determinar el impacto de los riesgos

Para establecer el impacto de un riesgo, es necesario realizar un análisis cualitativo de las consecuencias que puede tener su materialización, clasificándolas según su nivel de gravedad. La entidad determinó los criterios para establecer el nivel de impacto según el tipo de riesgo, es decir de gestión, de corrupción y de seguridad de la información, adaptando los criterios definidos por el DAFP en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 y en la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Magerit 3.0, como se muestra a continuación:

Tabla 4. Niveles para calificar el impacto de riesgos de gestión

Nivel	Descripción cualitativa del impacto
<b>Catastrófico</b>	<p>Se ubican en este nivel aquellos riesgos cuyas consecuencias afectan en forma muy grave las actividades del DANE y/o el logro de sus objetivos.</p> <p>Las dificultades presentadas son muy graves; su solución requiere realizar un análisis de causas y demanda tiempo, esfuerzos y recursos que pueden estar no previstos.</p> <p>Se ocasionan daños antijurídicos como efecto de la acción o de la omisión de la entidad, comprobados legalmente (responsabilidad patrimonial de la Entidad) o se comprueban responsabilidades fiscales, penales, disciplinarias o administrativas por la comisión de faltas gravísimas.</p> <p>Se presenta lesión del patrimonio público a causa del pago multas, indemnizaciones y/o sanciones.</p> <p>Se ocasionan cuantiosas pérdidas económicas por la pérdida, hurto o daño de bienes.</p> <p>La reputación de la entidad se ve afectada en forma muy grave, pues los hechos son de conocimiento público e impactan negativamente las relaciones con los grupos de interés.</p>
<b>Mayor</b>	<p>Se ubican en este nivel aquellos riesgos cuyas consecuencias afectan en forma grave las actividades del DANE y/o el logro de sus objetivos.</p> <p>Las dificultades presentadas son graves y no se resuelven fácilmente; su solución puede implicar la erogación de recursos no presupuestados.</p> <p>Hay lugar a la apertura de investigaciones disciplinarias y/o administrativas de las que se concluye que hay mérito sancionatorio por la comisión de faltas leves o graves.</p> <p>Se ocasionan pérdidas económicas por la pérdida, hurto o daño de bienes.</p> <p>La reputación de la entidad se ve afectada en forma grave, pues los hechos se conocen en la dirección de la entidad y a nivel territorial.</p>
<b>Moderado</b>	<p>Se ubican en este nivel aquellos riesgos cuyas consecuencias afectan en forma considerable las actividades del DANE y/o el logro de sus objetivos.</p> <p>Las dificultades presentadas se resuelven atacando sus causas raíz y su solución puede implicar la erogación de recursos no presupuestados.</p> <p>Se presentan demandas originadas por daños antijurídicos imputados a la Entidad por la acción u omisión de sus funciones o la apertura de investigaciones disciplinarias, administrativas, fiscales o penales.</p> <p>La reputación de la entidad se ve afectada en forma moderada, pues los hechos son conocidos por la dirección de la entidad y/o por organismos de control.</p>
<b>Menor</b>	<p>Se ubican en este nivel aquellos riesgos cuyas consecuencias afectan en forma leve las actividades del DANE y/o el logro de sus objetivos.</p> <p>Las fallas operativas presentadas en los procesos, en aspectos tecnológicos o en la infraestructura, se resuelven con la gestión normal de la entidad, atacando sus causas raíz, lo que conlleva al mejoramiento de los procesos.</p> <p>Se pueden presentar reclamaciones o quejas de los usuarios que podrían dar inicio a demandas en contra de la entidad o a la apertura de investigaciones disciplinarias, administrativas, fiscales o penales.</p> <p>La reputación de la entidad se ve afectada en forma mínima, pues los hechos se conocen en el área involucrada únicamente.</p>
<b>Insignificante</b>	<p>Se ubican en este nivel aquellos riesgos cuyas consecuencias no afectan en forma significativa las actividades del DANE ni el logro de sus objetivos.</p> <p>Las fallas operativas presentadas en los procesos, en aspectos tecnológicos o en la infraestructura, son mínimas y de fácil y pronta resolución.</p> <p>No hay pérdidas económicas, ni amonestaciones, sanciones o indemnizaciones, ni la intervención de organismos de control.</p> <p>Tampoco se ve afectada la reputación de la entidad.</p>

Fuente: Adaptado de Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 (p. 40).

Para la medición del impacto de los riesgos de corrupción, el DAFP definió diecinueve preguntas; la cantidad de respuestas afirmativas determinan el nivel de impacto; la entidad adopta esta medición, así:

Tabla 5. Preguntas para determinar el impacto de riesgos de corrupción

<b>Pregunta:</b> Si el riesgo de corrupción se materializa podría...
1. ¿Afectar al grupo de funcionarios del proceso?
2. ¿Afectar el cumplimiento de metas y objetivos de la dependencia?
3. ¿Afectar el cumplimiento de misión de la entidad?
4. ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?
5. ¿Generar pérdida de confianza de la entidad, afectando su reputación?
6. ¿Generar pérdida de recursos económicos?
7. ¿Afectar la generación de los productos o la prestación de servicios?
8. ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?
9. ¿Generar pérdida de información de la entidad?
10. ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?
11. ¿Dar lugar a procesos sancionatorios?
12. ¿Dar lugar a procesos disciplinarios?
13. ¿Dar lugar a procesos fiscales?
14. ¿Dar lugar a procesos penales?
15. ¿Generar pérdida de credibilidad del sector?
16. ¿Ocasionar lesiones físicas o pérdida de vidas humanas?
17. ¿Afectar la imagen regional?
18. ¿Afectar la imagen nacional?
19. ¿Generar daño ambiental?

Fuente: Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 (p. 46).

Si la respuesta de 1 a 5 preguntas es afirmativa, el impacto se cataloga como moderado; si se responde afirmativamente de 6 a 11 preguntas, el impacto se cataloga como mayor; y si se responde afirmativamente de 12 a 19 preguntas, el impacto se cataloga como catastrófico.

Los riesgos de corrupción siempre serán significativos; por lo tanto, su impacto puede ser moderado, mayor o catastrófico y no aplican los niveles insignificante o menor, que sí aplican para los demás riesgos.

Para los riesgos de seguridad de la información, los criterios a considerar para determinar el nivel de impacto sobre los activos de información (los cuales pueden ser infraestructuras críticas cibernéticas) son: obligaciones legales, seguridad, intereses comerciales o económicos, interrupción del servicio, orden público, operaciones, administración y gestión, pérdida de confianza (reputación) e información clasificada (nacional). Estos criterios se adaptan de acuerdo a las necesidades del DANE y FONDANE y se describen a continuación:

Tabla 6. Niveles para calificar el impacto de riesgos de seguridad de la información

Rango impacto	Obligaciones legales	Seguridad	Intereses comerciales o económicos	Interrupción del servicio	Orden público	Operaciones	Administración y gestión	Pérdida de confianza (reputación)	Información clasificada (nacional)
<b>Catastrófico</b>	Probablemente cause un incumplimiento excepcionalmente grave de una Ley o regulación	Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios	1. De muy elevado valor comercial 2. Causa de pérdidas económicas excepcionalmente elevadas 3. Causa de muy significativas ganancias o ventajas para individuos u organizaciones 4. Constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Entidad con un serio impacto en otras organizaciones	Alteración seria del orden público	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística	Probablemente impediría seriamente la operación efectiva de la Entidad, pudiendo llegar a su cierre	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones o el público en general.	Reservada
<b>Mayor</b>	Probablemente cause un incumplimiento grave de una Ley o regulación	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves	1. De elevado valor comercial 2. Causa de graves pérdidas económicas 3. Proporciona ganancias o ventajas desmedidas a individuos u organizaciones 4. Constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros	Probablemente cause una interrupción seria de las actividades propias de la Entidad con un impacto significativo en otras organizaciones	Probablemente cause manifestaciones, o presiones significativas	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística	Probablemente impediría la operación efectiva de la Entidad	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones o el público en general	Clasificada
<b>Moderado</b>	Probablemente sea causa de incumplimiento de una Ley o regulación	Probablemente sea causa de una mermas en la seguridad o dificulte la investigación de un incidente	1. De cierto valor comercial 2. Causa de pérdidas financieras o mermas de ingresos 3. Facilita ventajas desproporcionadas a individuos u organizaciones 4. Constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros	1. Probablemente cause la interrupción de actividades propias de la Entidad con impacto moderado. 2. Probablemente cause un cierto impacto en otras organizaciones.	Causa de protestas puntuales	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local	Probablemente impediría la operación efectiva de una parte de la Entidad	1. Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones o con el público en general 2. Probablemente afecte negativamente a las relaciones internas de la Entidad	
<b>Menor</b>								Probablemente cause una pérdida menor de la confianza dentro de la Entidad	
<b>Insignificante</b>	Pudiera causar el incumplimiento leve de una Ley o regulación	Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente	1. De pequeño valor comercial 2. Supondría pérdidas económicas mínimas	Pudiera causar la interrupción de actividades propias de la entidad con bajo impacto.	Pudiera causar protestas puntuales	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)	Pudiera impedir la operación efectiva de una parte de la Entidad	1. Pudiera causar una pérdida menor de la confianza dentro de la Entidad 2. No supondría daño a la reputación o buena imagen de las personas u organizaciones	

Fuente: Basado en la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Magerit 3.0.

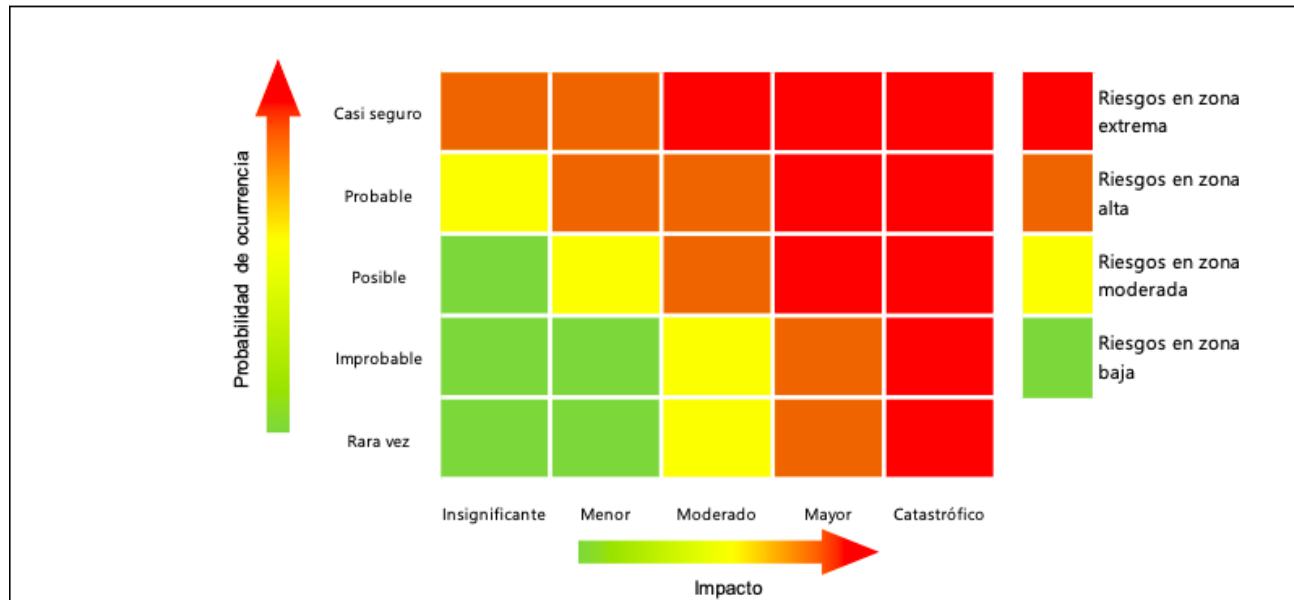
### 4. 3. 2. Evaluar riesgos

La evaluación de los riesgos consiste en determinar su nivel de severidad a partir de la combinación de probabilidad e impacto, lo cual se realiza tanto antes como después de establecer y evaluar los controles.

#### 4. 3. 2. 1. Valorar el nivel de riesgo inherente

Una primera evaluación de los riesgos se realiza determinando su probabilidad e impacto suponiendo que no existieran controles; es esto se le denomina riesgo inherente. La combinación de probabilidad e impacto determinarán el nivel de severidad del riesgo inherente, el cual puede ser extremo, alto, moderado o bajo y permite hacerse una idea de qué tan considerable o significativo puede llegar a ser el riesgo; la siguiente es la representación gráfica de la combinación de probabilidad e impacto:

Imagen 2. Mapa de calor para determinar el nivel de severidad de los riesgos



Fuente: Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 (p. 47).

#### 4. 3. 2. 2. Determinar y evaluar controles

Conocido el nivel de severidad de los riesgos inherentes, el paso a seguir es establecer y evaluar los controles que permitan atacar las vulnerabilidades causantes de los riesgos y por ende, prevenir o reducir la probabilidad de ocurrencia y/o el impacto de los mismos. Los controles pueden tener una naturaleza preventiva o detectiva; son preventivos cuando ayudan a anticipar eventos no deseados antes de que sucedan, y detectivos cuando permiten advertir la ocurrencia de las vulnerabilidades para tomar correctivos inmediatos. En general, los controles deben ser acciones que se están aplicando, y deben ser suficientes, comprensibles, eficaces, económicos y oportunos.

Algunas reglas para establecer controles:

- Para cada vulnerabilidad (debilidad o falla) se debe indicar un control o controles que ya estén funcionando y que sean efectivos para modificar la probabilidad de ocurrencia y/o el impacto del riesgo.
- Cada vulnerabilidad (debilidad o falla) debe analizarse por separado; es decir que no se deben combinar en la misma celda.
- Un control puede ser tan eficiente, que ayuda a mitigar más de una vulnerabilidad (debilidad o falla).
- Si una vulnerabilidad no tiene control, se deben formular acciones preventivas orientadas justamente a la implementación de controles.
- Cada control debe evaluarse tanto en su diseño como en su ejecución.
- Las acciones de control determinadas por la Entidad se deben documentar en las condiciones generales o en los puntos de control de los procedimientos.

Cada control debe ser evaluado, tanto en su diseño como en su ejecución, según los criterios establecidos por el DAFP.

Para evaluar los controles en su diseño, se asigna un puntaje a cada uno de los siguientes elementos:

- El control tiene un responsable de ejecutarlo
- La autoridad, competencias y responsabilidades de ejecutar el control se encuentran distribuidas entre diferentes funcionarios en forma adecuada
- El control tiene una periodicidad oportuna para su ejecución
- El control tiene un propósito (preventivo o detectivo)
- Se describe cómo se realiza la actividad de control, indicando si se utilizan fuentes de información e instrumentos confiables
- Las desviaciones o situaciones anormales detectadas durante la ejecución del control son investigadas y resueltas de forma oportuna
- Se obtienen evidencias completas de la ejecución del control

Si la sumatoria de los puntajes se encuentra entre 96 y 100 puntos, el control en su diseño es fuerte. Si se encuentra entre 86 y 95, es moderado. Y si se encuentra entre 0 y 85 es débil.

Los elementos para evaluar la ejecución de los controles son los siguientes:

- Fuerte, cuando siempre se ejecuta el control
- Moderado, cuando se ejecuta algunas veces o en algunas sedes o subsedes
- Débil, cuando no se ejecuta el control

La combinación de la evaluación del diseño y de la ejecución de cada control, permite determinar su solidez individual, la cual puede ser fuerte (su calificación es de 100 puntos), moderada (su calificación es de 50 puntos) o débil (su calificación es de 0 puntos). La calificación de la solidez de cada control será la menor calificación del diseño o ejecución, tal como lo establece el DAFP en la siguiente tabla:

Tabla 7. Valoración de la solidez individual de cada control

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCIÓN DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE:100 MODERADO:50 DÉBIL:0	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SÍ / NO
fuerte: calificación entre 96 y 100"	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
moderado: calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

Fuente: Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 (p. 63).

En caso de existir más de un control en cada riesgo, se debe valorar la solidez del conjunto de controles, la cual se obtiene al promediar la calificación de la solidez individual de cada uno de ellos y se determina de acuerdo con la siguiente tabla:

Tabla 8. Valoración de la solidez del conjunto de controles

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
<b>Fuerte</b>	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
<b>Moderado</b>	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
<b>Débil</b>	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Fuente: Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 (p. 64).

Es de anotar que si la solidez del conjunto de controles es débil, el responsable del proceso deberá suscribir un plan de tratamiento con acciones preventivas y que en caso de que no existan controles, estas acciones deben estar justamente orientadas a su creación e implementación.

4. 3. 2. 3. Valorar el nivel de riesgo residual

Una vez que se ha determinado la solidez del conjunto de controles, se podrá determinar en qué grado contribuyen a minimizar la probabilidad de ocurrencia e impacto de los riesgos inherentes. En el mapa de calor, se podrá apreciar un desplazamiento de la probabilidad en uno o dos niveles hacia abajo, así como del impacto en uno o dos niveles hacia la izquierda, de acuerdo con la siguiente tabla:

Tabla 9. Disminución de la probabilidad e impacto de los riesgos de acuerdo con la solidez del conjunto de controles

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES.	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
fuerte	directamente	directamente	2	2
fuerte	directamente	indirectamente	2	1
fuerte	directamente	no disminuye	2	0
fuerte	no disminuye	directamente	0	2
moderado	directamente	directamente	1	1
moderado	directamente	Indirectamente	1	0
moderado	directamente	no disminuye	1	0
moderado	no disminuye	directamente	0	1

**IMPORTANTE**

Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

**IMPORTANTE**

Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

Fuente: Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 (p. 66).

Conocido el nivel de severidad de los riesgos residuales, se podrán tomar decisiones con respecto a otras medidas de tratamiento adicionales para prevenir la materialización de los riesgos, de conformidad con los niveles de aceptación establecidos en la Política de administración de riesgos. El tratamiento específico de los riesgos de seguridad de la información, se realiza mediante la implementación de la política general de seguridad y privacidad de la información, sus políticas complementarias y los procedimientos relacionados.

### **4. 3. 3. Monitorear y hacer seguimiento a los riesgos y a la efectividad de los controles**

El monitoreo consiste en una revisión cuatrimestral que la primera línea de defensa realiza a los riesgos identificados; en esta revisión se analiza si las amenazas y vulnerabilidades que originan los riesgos aún se presentan o si se pueden estar presentando riesgos emergentes; igualmente se determina si los riesgos identificados se han materializado y si los controles están bien diseñados, se ejecutan con rigurosidad y son efectivos para contrarrestar las vulnerabilidades, lo cual debe ser debidamente verificable mediante el aporte de evidencias. Se establece un plan de mejoramiento con acciones correctivas en caso de que se hayan materializado riesgos.

Los resultados de los monitoreos de riesgos de gestión y de corrupción se reportan a la Oficina Asesora de Planeación; el monitoreo de los riesgos de seguridad de la información o los incidentes de seguridad presentados deben ser informados al responsable de seguridad de la información o a quien haga sus veces. Los funcionarios de la Oficina Asesora de Planeación y el responsable de seguridad de la información consignan en las herramientas anexas, las observaciones y recomendaciones derivadas del análisis relacionadas con la implementación de nuevos controles, el fortalecimiento de los controles existentes y su documentación en los procedimientos. Así mismo asesoran en los ajustes a que haya lugar en los mapas de riesgos y en la formulación de los planes de mejoramiento, en caso de que se hayan materializado los riesgos. Con la información recopilada, la Oficina Asesora de Planeación y el responsable de seguridad de la información elaboran en lo correspondiente, un reporte ejecutivo para la línea estratégica.

Por último la tercera línea de defensa realiza la evaluación independiente sobre la efectividad del sistema de administración de riesgos y la validación del cumplimiento de las responsabilidades de las demás líneas de defensa. Los informes resultantes deben ser publicados en la página web.

### **4.4. Comunicación y consulta**

La comunicación y consulta es un aspecto transversal que se realiza con los grupos de interés internos y externos, con el fin de asegurar que los riesgos identificados permitan encontrar puntos críticos para mejorar la prestación de los servicios y la operación de los procesos.

En la elaboración y actualización de los mapas de riesgos se debe involucrar a los funcionarios y contratistas con mayor experiencia en los procesos institucionales para que aporten su conocimiento en las diferentes etapas del marco metodológico de la administración de los riesgos.

### **4.5. Aspectos complementarios para la administración de riesgos de seguridad de la información**

La Guía de gestión de riesgos (guía No. 7) del Modelo de Seguridad y Privacidad de la Información - MSPI del MinTIC resume las actividades de administración de riesgos de seguridad de la información. En la siguiente imagen se observa la relación de las etapas del MSPI con el marco metodológico de la administración de riesgos de la entidad.

Tabla 10. Relación de las etapas del MSPI con el proceso de gestión de riesgos de seguridad de la información

ETAPAS DEL MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDADDE LA INFORMACION
<b>Planear</b>	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
<b>Implementar</b>	Implementación del Plan de Tratamiento de Riesgo
<b>Gestionar</b>	Monitoreo y Revisión Continuo de los Riesgos
<b>Mejora Continua</b>	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Fuente: Ministerio de Tecnologías de la Información y las comunicaciones – MinTIC Guía de gestión de riesgos (guía No. 7) del Modelo de seguridad y privacidad de la información (p. 12).

El anexo 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4 del DAFP, contiene los lineamientos para la gestión de riesgos de seguridad digital en entidades públicas basados en el Modelo Nacional de Gestión de Riesgos de Seguridad Digital – MGRSD establecido por el MinTIC. La gestión de riesgos de seguridad de la información se desarrolla en cuatro fases: planificación, ejecución, monitoreo y revisión y mejoramiento continuo.

En la fase de planificación se determina el contexto interno y externo de la Entidad, se crea la política de administración de riesgos con roles y responsabilidades, se identifican los activos y los riesgos inherentes de los activos críticos y críticos cibernéticos con sus amenazas y vulnerabilidades, se identifican y evalúan los controles existentes, se definen las acciones de tratamiento y los indicadores para medir su eficacia y efectividad.

Para facilitar el desarrollo de esta fase, el responsable de seguridad de la información de la Entidad, utilizando la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Magerit – versión 3.0. (Libro II - Catálogo de Elementos), define los riesgos de seguridad de la información asociados a cada tipo de activo: información, software, servicios, hardware, redes de comunicación, equipamiento auxiliar, instalaciones, dispositivos de almacenamiento de datos, log y claves criptográficas. El catálogo de elementos de la metodología Magerit 3.0, permite tener certeza sobre las amenazas asociadas al tipo de activo y los atributos de confidencialidad, integridad y disponibilidad que se pueden ver afectados. Igualmente, realiza un análisis de vulnerabilidades y controles existentes en la Entidad, y la información obtenida se utiliza como insumo para parametrizar el formato mapa de riesgos de seguridad de la información SIO-040-PDT-002-f-003. Durante la asesoría a la primera línea de defensa, el responsable de seguridad de la información, valida los riesgos identificados, la adecuación y pertinencia de los controles y completa la información faltante; también presta asesoría en la formulación de planes de tratamiento o de mejoramiento relacionados con la administración de riesgos de seguridad de la información.

En la fase de ejecución, se desarrollan las acciones de tratamiento. El responsable de seguridad de la información supervisa y acompaña la implementación de estas acciones y la Alta Dirección apoya con la asignación de los recursos.

En la fase de monitoreo y revisión, la primera, segunda y tercera línea de defensa, verifican el adecuado diseño y ejecución de las actividades de control, monitorean los riesgos determinando si se han materializado, suministran recomendaciones para mejorar la eficacia y eficiencia de los controles y hacen seguimiento a los planes de tratamiento para determinar su efectividad; realizado esto, es necesario valorar nuevamente los riesgos de seguridad de la información para verificar si los niveles de severidad de los riesgos residuales han

disminuido. Así mismo, según los lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, se tienen en cuenta los incidentes de seguridad digital que hayan afectado a la entidad y también los indicadores definidos para hacer seguimiento a las medidas de seguridad implementadas. Todo lo anterior contribuye a la toma de decisiones por parte de la línea estratégica.

En esta fase, según el Modelo Nacional de Gestión de Riesgos de Seguridad Digital, el responsable de seguridad de la información reporta a la línea estratégica: los riesgos de seguridad de la información, el listado de activos críticos, el reporte de criticidad, plan de tratamiento de riesgos e impactos frente a la materialización de riesgos. Los activos y servicios digitales críticos (aquellos que afectan gravemente al funcionamiento de la entidad) y los riesgos, amenazas y vulnerabilidades más importantes identificados durante el ejercicio de riesgos, deberán ser reportados al CSIRT de Gobierno.

Los activos críticos cibernéticos del centro de datos del DANE, los riesgos, amenazas y vulnerabilidades críticas relacionados con estos, se reportan al Comando Conjunto Cibernético - CCOC, dado que es la Entidad encargada de administrar esta información, con los respectivos acuerdos de confidencialidad. La Oficina de Control Interno realiza la evaluación independiente sobre la administración de riesgos de seguridad de la información en la Entidad. El responsable de seguridad de la información formula los indicadores de desempeño para la gestión de riesgos para reportar a la línea estratégica.

En la fase de mejoramiento continuo, los responsables de los procesos toman las acciones para controlar y prevenir hallazgos, falencias o incidentes de seguridad de la información. Se debe llevar un registro documentado del tratamiento realizado al hallazgo, así como las acciones realizadas para mitigar el impacto y ver el resultado. El marco metodológico para la administración de riesgos de seguridad de la información de la Entidad debe ser socializado para que los funcionarios y contratistas comprendan sus responsabilidades frente a la seguridad de la información en los roles que desempeñan.

## 5. DEFINICIONES

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000:2013). Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 2016, pág. 56).
- **Administración del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. (DAFP 2018).
- **Amenaza:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO/IEC 27000:2016).
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (ISO/IEC 27000:2013).
- **Control:** Medida que modifica el riesgo. (NTC ISO 31000:2011). Medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. (Modelo Nacional de Gestión de Riesgos de Seguridad Digital). Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones). (Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAFP, versión 4, 2018, página 49).
- **CSIRT:** Por su sigla en inglés: Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad cibernética). ([http:// www.first.org](http://www.first.org)). (Modelo Nacional de Gestión de Riesgos de Seguridad Digital).
- **CCOC:** Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT. (Modelo Nacional de Gestión de Riesgos de Seguridad Digital).

- Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. (ISO/IEC27000:2013).

- Información: Datos relacionados que tienen significado para la entidad. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. (ISO/IEC 27001:2013).

La Ley 1712 del 2014, se refiere a la información como un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

- Infraestructura crítica cibernética nacional: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).

- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos. (ISO/IEC27000:2013).

- 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 de seguridad digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. (DAFP 2018).

- Riesgo inherente: Es aquel al que se enfrenta la entidad en ausencia de controles que modifiquen su probabilidad de ocurrencia o impacto. (DAFP 2018).

- Riesgo residual: Es el riesgo que permanece luego de haber diseñado, implementado y valorado la efectividad de los controles. (Basado en DAFP 2018).

- Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27000:2016).

- Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854 2016, pág. 29).

- Usuario: Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información. Las personas que se relacionan con la entidad y usan información de la entidad en virtud de sus funciones o relación contractual, exclusivamente para el ejercicio de las mismas. (Guía para la Gestión y Clasificación de Activos de Información (guía No. 5) del MinTIC).

- Vulnerabilidad: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas. (Basado en DAFP 2018).

## 6. REGISTROS

Código	Nombre	Almacenamiento Físico	Almacenamiento Magnético
SIO-040-PDT-002-f-001	Mapa de riesgos de gestión		X
SIO-040-PDT-002-f-002	Mapa de riesgos de corrupción		X

SIO-040-PDT-002-f-003	Mapa de riesgos de seguridad de la Información		X
-----------------------	--	--	---

## 7. BIBLIOGRAFIA

Departamento Administrativo de la Función Pública (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas. Recuperado de [https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document\\_library/bGsp2ljUBdeu/view\\_file/34316499](https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2ljUBdeu/view_file/34316499)

Gobierno de España (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Magerit – versión 3.0. Libro II - Catálogo de Elementos. Recuperado de <https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html>

Ministerio de Tecnologías de la Información y las Comunicaciones (2016). Guía de gestión de riesgos de seguridad y privacidad de la información (guía No. 7). Recuperado de [https://www.mintic.gov.co/gestioni/615/articles-5482\\_G7\\_Gestion\\_Riesgos.pdf](https://www.mintic.gov.co/gestioni/615/articles-5482_G7_Gestion_Riesgos.pdf)

Ministerio de Tecnologías de la Información y las Comunicaciones. Modelo Nacional de Gestión de Riesgos de Seguridad Digital. Recuperado de [https://www.mintic.gov.co/portal/604/articles-61854\\_documento.docx](https://www.mintic.gov.co/portal/604/articles-61854_documento.docx)

## 8. ANEXOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN	
---------	-------	---------------------------	--

ELABORÓ	REVISÓ	APROBÓ
<b>Nombre:</b> Sandra Patricia Burgos Chaquer <b>Cargo:</b> Profesional Especializado <b>Fecha:</b> 17/Mar/2021	<b>Nombre:</b> Hernan David Gonzalez Carrillo <b>Cargo:</b> Profesional Especializado <b>Fecha:</b> 29/Abr/2021	<b>Nombre:</b> Lina Paola Cardozo Orjuela <b>Cargo:</b> Jefe Oficina Asesora de Planeación <b>Fecha:</b> 07/Jul/2021

Si este documento es impreso se considera copia no controlada