GUIA PARA LA ADMINISTRACIÓN DE RIESGOS

BOGOTÁ, OCTUBRE 2021

CONTENIDO

1. INTRODUCCIÓN

La Agencia Nacional Digital, con el propósito de aplicar la Política de Gestión Integral del Riesgo, diseñó la presente guía, con la que busca dar los lineamentos generales para gestionar de manera adecuada sus riesgos, aplicando lo establecido en la Guía para la Administración del riesgo del DAFP[1], el Manual Operativo del Modelo Integrado de Planeación y Gestión y el Modelo Estándar de Control Interno, en su componente de Evaluación del Riesgo, como mecanismo para identificar, medir, valorar, monitorear, administrar y tratar los riesgos que pudieran afectar el logro de los objetivos institucionales.

2. OBJETIVO

Definir los lineamientos para la gestión integral de los riesgos que se pueden presentar en la ejecución de los procesos y proyectos de la Agencia Nacional Digital, encaminados a la identificación y respectivo tratamiento de los riesgos de corrupción, gestión y seguridad digital, con el fin de evitar situaciones que puedan afectar el cumplimiento de los objetivos institucionales.

3. ALCANCE

La presente guía se aplica a todos los procesos de la Agencia Nacional Digital, incluyendo los proyectos de desarrollo asociados al Proceso de Gestión de Proyectos de Ciencia, Tecnología e Innovación aplicada, los Procesos de Articulación y Prestación de Servicios Ciudadanos Digitales y a todas las acciones adelantadas por los colaboradores durante el ejercicio de sus actividades.

4. DEFINICIONES

a) **Activo de Información**: toda aquella información que reside en medio electrónico o físico, que tiene un significado y valor para la Agencia Nacional Digital.

b) **Administración del Riesgo:** un 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.

c) **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización, aprovechando las vulnerabilidades existentes en la Agencia.

[1] Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 – DAFP – diciembre 2020

d) Apetito de Riesgo: es el nivel de riesgo que la Agencia puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

e) Autocontrol: la capacidad que tiene cada colaborador público para detectar las desviaciones en su trabajo y realizar los correctivos necesarios; en tal virtud, la autoevaluación, como herramienta complementaria al autocontrol se convierte en un instrumento básico para la mejora continua de las entidades.

f) Autoevaluación: comprende el monitoreo que se le debe realizar a la operación de la entidad a través de la medición de los resultados generados en cada proceso, procedimiento, proyecto, plan y/o programa, teniendo en cuenta los indicadores de gestión, el manejo de los riesgos, los planes de mejoramiento, entre otros.

g) Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

h) Causa: medios, circunstancias, situaciones o agentes que pueden hacer que un riesgo se materialice.

i) Causa Inmediata: Condiciones bajo las cuales se presenta el riesgo, no constituye la causa principal.

j) Causa Raíz: Condiciones o medios por los cuales se puede presentar el riesgo, es la causa principal o básica que lo originan.

k) Ciclo de vida del proyecto: la serie de fases que atraviesa un proyecto desde su inicio hasta su cierre.

l) Confidencialidad: principio de la Seguridad de la Información que busca asegurar que la información sea accedida únicamente por personal autorizado.

m) Consecuencia: efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad.

n) Contenedor de la Información: cualquier plataforma tecnológica o lugar físico que almacena, procesa, transmite un Activo de Información por cualquier lapso de tiempo o propósito.

o) Control Correctivo: está diseñado para accionarse en el momento en que el riesgo se materializa, en este sentido permite corregir las causas del riesgo evitando que vuelva a ocurrir.

p) Control Detectivo: está diseñado para identificar un evento o resultado no previsto después de que se haya producido. Busca detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

q) Control Preventivo: está diseñado para evitar un evento no deseado en el momento en que se produce.

r) Disponibilidad: principio de la Seguridad de la Información que busca asegurar que la información esté disponible cuando sea requerido por los procesos, servicios, colaboradores y ciudadanos.

s) Establecimiento del contexto: definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.

t) Fuentes de riesgo externas: son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.

u) Gestión del Riesgo: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

v) Identificación del Riesgo: etapa en la cual se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias.

w) Impacto: consecuencias o efectos que pueden ocasionar a la organización la materialización del riesgo.

x) Integridad: principio de Seguridad de la Información que busca asegurar que la información esté protegida contra modificaciones no autorizadas para garantizar su consistencia, exactitud y completitud. Se debe garantizar la trazabilidad de la información.

y) Propietario del Activo: Colaborador encargado de identificar y establecer el alcance y valor o criticidad de un Activo de Información, los requerimientos de seguridad del mismo y la comunicación y divulgación de éstos.

z) Líder del Proceso: colaborador de la AND, responsable del adecuado cumplimento de las actividades que conforman un proceso, y que están encaminadas a satisfacer una demanda tanto interna como externa.

aa) Matriz de Riesgo: Documento en el cual se plasma la representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa.

bb) Probabilidad: se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.

cc) Riesgo: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

dd) Riesgos de Corrupción: Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

ee) Riegos de gestión: posibilidad de que un evento potencial afecte el cumplimiento de los objetivos de los procesos de la organización, sus definiciones estratégicas, o su operación. Estos riesgos pueden ser de carácter judicial, contractual, financiero, administrativo, imagen, asociados a la prestación de servicios, fiscales, contables y presupuestales.

ff) Riesgos de Seguridad Digital: 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.

gg) Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

hh) Riesgo Residual: Riesgo restante después de aplicar el tratamiento al Riesgo, a través de actividades de control.

ii) Riesgo Inherente: Riesgo identificado antes de aplicar actividades de control.

jj) Valoración del Riesgo: Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (riesgo inherente).

kk) Vulnerabilidad: debilidad asociada al Contenedor de un Activo de Información y que puede ser explotada para materializar un riesgo de seguridad digital, causando incidentes no deseados que pueden dar lugar a la pérdida de Confidencialidad, Integridad o Disponibilidad de los Activos de Información.

5. RESPONSABILIDADES FRENTE A LA GESTIÓN DEL RIESGO

Teniendo en cuenta lo indicado en MIPG, se clasifican las responsabilidades y roles frente a cada riesgo identificado, con el fin de realizar un tratamiento, seguimiento y evaluación que permita realizar una gestión del riesgo adecuada en la Agencia Nacional Digital.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Estratégica	Alta Dirección. Comité de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno	• Aprobar la Política de Gestión Integral del riesgo. • Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo). • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la Agencia y que puedan generar cambios en la estructura de los riesgos identificados y en sus actividades de control. • Realizar seguimiento y análisis periódico a los riesgos institucionales. • Revisar la exposición de la entidad a los riesgos de corrupción y fraude de acuerdo con los informes del canal de denuncias PQRSD. • Monitorear el tratamiento de las Denuncias de riesgos de corrupción y fraude desde el Comité Institucional de Coordinación de Control Interno. • Realimentar en el Comité Institucional de Gestión y Desempeño los ajustes que se deban hacer frente a la gestión del riesgo. • Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este. • Monitorear el cumplimiento de los estándares de conducta y la práctica de los principios y valores de los funcionarios públicos por medio del Comité Institucional de Coordinación de Control Interno.
Primera Línea de defensa	Director(a) General Líderes de procesos Gerentes de proyecto	• Realizar el análisis de contexto y análisis de causas, relacionados con cada mapa de riesgos que lidera. • Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlos cuando se requiera. • Realizar la evaluación del riesgo inherente y riesgo residual, aplicando las actividades de mejoramiento y fortalecimiento que correspondan. • Definir, aplicar y hacer seguimiento a las actividades de control para tratar los riesgos identificados, alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso o proyecto. • Supervisar la ejecución de las actividades de control aplicadas por el equipo de trabajo en la gestión del día a día. Detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar, con base en la evaluación del diseño de actividades de control. • Realizar evaluación periódica de las conductas asociadas a los valores y principios de los funcionarios públicos a través del instrumento para la evaluación de desempeño y notificar al área de planeación o quien haga sus veces las desviaciones que tengan injerencia en la gestión de riesgos. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de las actividades de control. • Informar a Planeación o quien haga sus veces (segunda línea) sobre los riesgos materializados en los programas, planes y/o procesos a su cargo.

		En el caso de los proyectos de desarrollo, el Gerente debe informar al cliente en las reuniones de seguimiento programadas, y coordinar con Control Interno (tercera línea) el establecimiento del plan de mejoramiento respectivo. • Diligenciar el mapa de riesgos del proceso o proyecto liderado, el cual debe ser aprobado por la AND (en el caso de los proyectos, requiere aprobación del cliente) y mantenerlo actualizada, en caso de requerir asesoría por parte de Control Interno, realizar la solicitud correspondiente. • Los líderes de Procesos, Proyectos, propietarios y responsables de Activos de Información son los encargados de realizar la gestión del Riesgo sobre dichos Activos de Información. El Oficial de Seguridad de la Información debe promover y apoyar la ejecución de esta actividad, basado en la metodología aprobada para tal fin.
Segunda Línea de defensa	Persona o equipo asignado para realizar las funciones de Planeación en la AND.	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo. • Consolidar el Mapa de riesgos institucional y presentar en el comité de gestión y desempeño los riesgos de mayor criticidad frente al logro de los objetivos para análisis y seguimiento. • Acompañar, orientar y entrenar a los líderes de procesos y proyectos en la identificación, análisis y valoración del riesgo. (labor que puede adelantar control interno de ser necesario, en su rol de asesorías y acompañamiento, sin establecer actividades, sino solo orientando). • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos y proyectos. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
Tercer Línea de defensa	Persona o equipo asignado para realizar las funciones de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de las actividades de control establecidas en los procesos y proyectos. • Proporcionar aseguramiento objetivo en los procesos y proyectos identificados no cubiertos por la primera y segunda línea de defensa. • Asesorar de forma coordinada con el equipo de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y en el diseño de las actividades de control. • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Programa Anual de Auditoría. • Recomendar mejoras a la política y guía de administración del riesgo. • Comunicar a la Alta Dirección sobre posibles materializaciones de riesgos críticos en la Agencia. • Realizar acompañamiento a los Gerentes de Proyecto de desarrollo, sobre la aplicación correcta de la presente guía.

		• Evaluar la eficacia de las actividades de control establecidas por la primera línea de defensa en los diferentes mapas de riesgo.

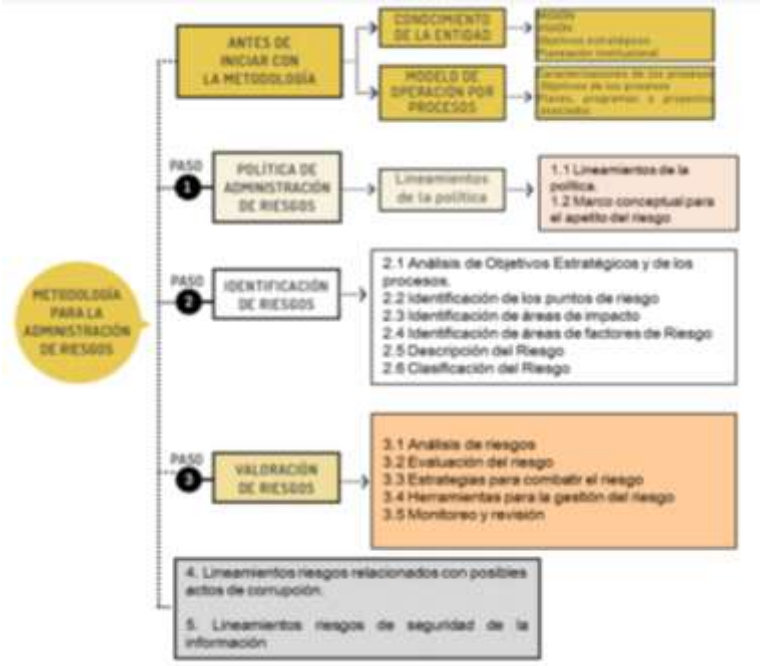
6. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO EN LA AND

La AND implementa las etapas de identificación y valoración de los riesgos, teniendo como referencia la Guía para la Administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP) y la Guía para la Gestión del Riesgo de Corrupción de la Secretaría de Transparencia de la Presidencia de la República.

Así mismo, la AND aplica su metodología de administración de riesgos en sus diferentes proyectos de desarrollo, reconociendo la importancia de controlar de forma organizada la ejecución de las actividades de control en sus proyectos, como también contar con un establecimiento adecuado de los riesgos que identifica, con el fin de prevenir sus materializaciones; enfocándose en el tratamiento efectivo de las causas que generan estos riesgos. Cabe mencionar, que la presente guía sirve como base para elaborar los diferentes planes de riesgos en los proyectos de Desarrollo.

A continuación, se aprecia la ilustración 1, que muestra de manera general la metodología aplicada en la Agencia.

Ilustración 1. Metodología para la gestión del Riesgo en la AND



Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

Antes de iniciar con la metodología, es necesario contar con la información que permita llevar a cabo una contextualización de la organización, partiendo del conocimiento de la Entidad en cuanto a su misión, visión, objetivos estratégicos y su planeación institucional. En la Agencia Nacional Digital este contexto se encuentra plasmado en el Plan Estratégico Institucional el cual rige el quehacer de la Entidad.

De igual manera es fundamental que la Entidad cuente con un Modelo de Operación por Procesos en el marco del cual se evidencie la estructura para la gestión en la entidad a partir de los procesos identificados y en los cuales se pueda llevar a cabo la gestión de riesgos. En la Agencia Nacional Digital, dicho modelo se encuentra descrito en el DE.MN.01 Manual del SIG AND y en la Resolución 019 de 2021 "Por la cual se adopta el SIG AND".

En este contexto, la Agencia Nacional Digital cuenta con la intranet como la herramienta por medio de la cual se encuentra la información de los diferentes procesos de la Entidad, los cuales cuentan con cartas descriptivas o caracterizaciones en las cuales se establecen los objetivos de los procesos y se enmarcan los planes o proyectos que genera la Agencia.

En el caso de los proyectos de CTI aplicada así como de Prestación y Articulación de Servicios Ciudadanos Digitales, es importante adicionar el análisis del contexto de acuerdo con la particularidad de cada proyecto (Ej. Entidad para la que se desarrolla el proyecto, población objetivo del proyecto, etc.)

Teniendo en cuenta el marco anterior, a continuación se describen los pasos de la metodología para la administración del Riesgo en la AND:

6.1. Política de Administración de riesgos

La Agencia elaboró la Política para la Gestión Integral del Riesgo en la Entidad, la cual tiene como objetivo establecer los lineamientos que le permitan proteger todos sus procesos de los potenciales riesgos asociados, así como establecer los mecanismos necesarios para evitar, reducir/mitigar, compartir/transferir y/o asumir los riesgos inherentes a su quehacer institucional y que pudieran afectar negativamente a las personas, las instalaciones, los bienes y los equipos de la entidad.

En este contexto, a continuación se menciona la Política de Gestión Integral del Riesgo de la AND:

La Corporación Agencia Nacional de Gobierno Digital – AND, se compromete a fortalecer la cultura de prevención, por medio de una adecuada gestión de Riesgos, dirigiendo sus esfuerzos hacia el establecimiento de los mecanismos necesarios para evitar, reducir/mitigar, compartir/transferir y/o asumir los riesgos relacionados con el desarrollo de todos sus procesos y que pudieran afectar

negativamente a las personas, las instalaciones y/o los bienes de la entidad; para tal efecto realizará la identificación, análisis, valoración e intervención de los riesgos inherentes al que hacer institucional, contribuyendo de esta forma al logro de los objetivos y la misión de la entidad.

La Agencia, por medio de la alta dirección asigna los recursos necesarios para lograr esta gestión del riesgo, propiciando los espacios que sean necesarios para que sus colaboradores participen de forma activa en todas las actividades relacionadas con el tema, lo anterior aplicando lo establecido en su guía interna de tratamiento de riesgos, que incluye en una sola metodología lo relacionado con riesgos de gestión u operativos, corrupción y seguridad digital.

Así mismo, los riesgos positivos que se identifican se entienden como oportunidades de mejora y se potencializan para ser aprovechados y mejorar los resultados de nuestra gestión institucional.

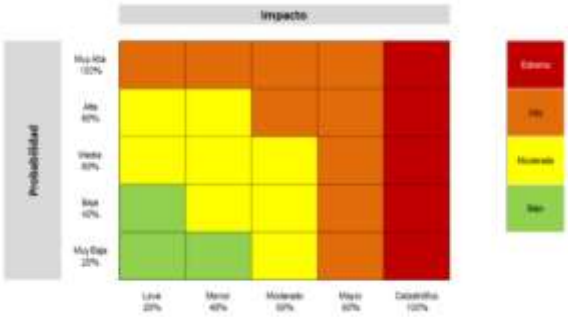
Ahora bien, por otra parte, la Política de Gestión Integral del Riesgo en la Agencia, establece el Apetito del Riesgo para la Entidad con el propósito de controlar el nivel del riesgo que la Agencia puede aceptar de acuerdo con sus objetivos, el marco legal y disposiciones de la alta dirección.

En este sentido a continuación se describen la capacidad del riesgo, el apetito del riesgo y la tolerancia del riesgo determinados en la Política de Gestión Integral del Riesgo de la Agencia:

Determinación de la Capacidad del Riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad.

En este contexto, la escala que resulta de combinar la probabilidad y el impacto en la valoración de los riesgos genera los niveles de riesgo, estos son: extremo, alto, moderado y bajo, tal como se muestra en el siguiente gráfico:

Ilustración 2. Matriz de calor – Niveles de severidad del riesgo



Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

En este marco, la Agencia Nacional Digital define que el valor máximo de la escala del nivel del riesgo que puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos, es el nivel del riesgo extremo, siendo este su capacidad de riesgo.

Determinación del Apetito del Riesgo: el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad. Equivale al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

En este contexto, la Agencia Nacional Digital define que el nivel de riesgo que la entidad puede aceptar para los riesgos operativos o de gestión es el nivel alto y para los riesgos de seguridad digital es el nivel moderado. En cuanto a los riesgos de corrupción el nivel aceptado por la entidad es el nivel bajo, siendo estos el apetito del riesgo de la Agencia.

Tolerancia del Riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

En este marco, la Agencia Nacional Digital define que la tolerancia del riesgo para riesgos operativos o de gestión es el nivel extremo, así como para los riesgos de seguridad digital es el nivel alto. En cuanto a los riesgos de corrupción el nivel de tolerancia continúa siendo el nivel bajo.

Teniendo en cuenta todo lo anterior, en la siguiente tabla se definen las medidas de respuesta que se pueden ejecutar dependiendo del nivel de Riesgo:

Tabla 1. Medidas de Respuesta a Niveles de severidad del riesgo

Nivel del Riesgo	Medidas de Respuesta
Riesgo nivel Bajo	Aceptar el Riesgo
Riesgo nivel Moderado	Aceptar el Riesgo o Reducir el Riesgo
Riesgo nivel Alto	Reducir el Riesgo, Transferir el Riesgo o Evitar del Riesgo
Riesgo nivel Extremo	Reducir el Riesgo, Transferir el Riesgo o Evitar el Riesgo

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

6.2. Identificación de Riesgos

Para la identificación de los riesgos, es necesario tener en cuenta los siguientes aspectos:

- Análisis de objetivos estratégicos y de los procesos: este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo del proceso u objetivos estratégicos de la entidad. Para la Agencia Nacional Digital, los objetivos estratégicos se encuentran en el Plan Estratégico Institucional y los objetivos de los procesos se encuentran en las cartas descriptivas de los procesos, publicadas en la intranet de la entidad.
  En el caso de los proyectos, es necesario que se tenga en cuenta el objetivo particular de cada uno de estos.

- Identificación de los puntos de riesgo: son actividades dentro del flujo del proceso o del proyecto, donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso o el proyecto, cumpla con su objetivo.

- Identificación de áreas de impacto: el área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional. En el punto 6.3 de este documento se encuentra la metodología para llevar a cabo la valoración del impacto.

- Identificación de áreas de factores de riesgo: son las fuentes generadoras de riesgos que puede tener una entidad o un proyecto. Estas fuentes pueden ser procesos, talento humano, tecnología, infraestructura o eventos externos.

- Descripción del Riesgo: la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. El Departamento Administrativo de la Función Pública propone la siguiente estructura que inicia con la frase POSIBILIDAD DE y analiza aspectos como:

  - Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.

  - Causa inmediata: circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

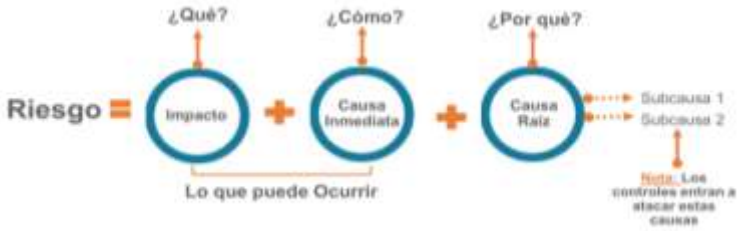
  - Causa raíz: es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo.

Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas.

El análisis de causas se puede realizar por medio de diferentes metodologías, como la utilización de los 5 Porqués, diagrama de cola de pescado o lluvia de ideas; para este caso cada líder del proceso o proyecto es libre de escoger la metodología que más se le facilite. De este análisis, depende la gestión del riesgo que se haga en un futuro, pues cada causa debe tener como mínimo una actividad de control asociada.

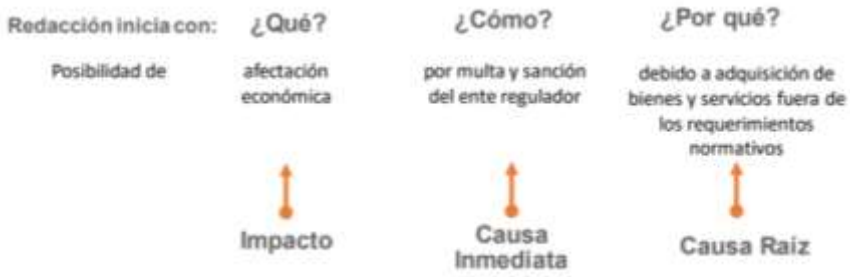
Teniendo en cuenta lo anterior, a continuación se presenta la estructura propuesta por el DAFP:

Ilustración 3. Estructura propuesta para la redacción del riesgo



Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

Ejemplo:



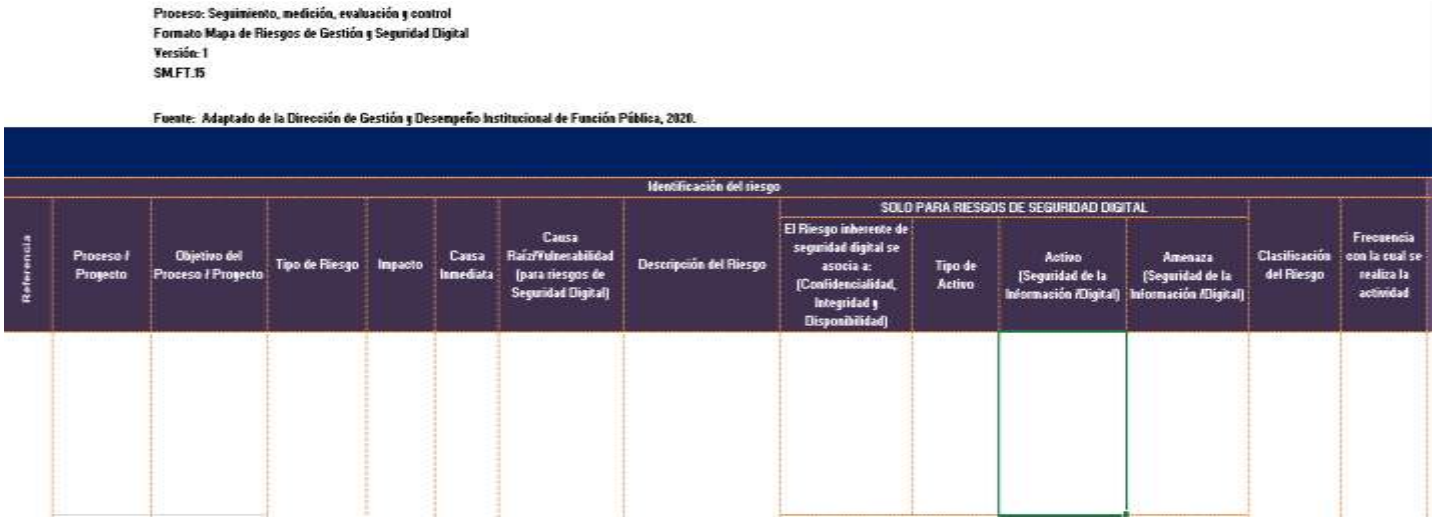
La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

- Clasificación del riesgo: permite agrupar los riesgos identificados, se clasifica cada uno de los riesgos en categorías como ejecución y administración de procesos; fraude externo; fraude interno;

fallas tecnológicas; relaciones laborales; usuarios, productos y prácticas; y daños a activos fijos/ eventos externos.

En este contexto, la Agencia Nacional Digital hace la identificación de los riesgos, incluyendo todos los aspectos antes mencionados a través del SM.FT.15 Mapa de Riesgos de Gestión y Seguridad Digital, el cual está adaptado sobre el mapa de riesgos propuesto por el DAFP, tal como se muestra a continuación:

Ilustración 4. Mapa de Riesgos – Identificación de los Riesgos



Proceso: Seguimiento, medición, evaluación y control
Formato Mapa de Riesgos de Gestión y Seguridad Digital
Versión: 1
SM.FT.15

Fuente: Adaptado de la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Identificación del riesgo													
								SOLO PARA RIESGOS DE SEGURIDAD DIGITAL					
Referencia	Proceso / Proyecto	Objetivo del Proceso / Proyecto	Tipo de Riesgo	Impacto	Causa Inmediata	Causa Raíz/Vulnerabilidad (para riesgos de Seguridad Digital)	Descripción del Riesgo	El Riesgo inherente de seguridad digital se asocia a: (Confidencialidad, Integridad y Disponibilidad)	Tipo de Activo	Activo (Seguridad de la Información /Digital)	Amenaza (Seguridad de la Información /Digital)	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad

Fuente: Equipo Planeación AND

Para los riesgos de seguridad digital se debe tener en cuenta que su identificación se basa en la afectación de tres principios en un activo o un grupo de activos dentro del proceso: “Integridad, confidencialidad o disponibilidad”. Para el riesgo identificado se deben asociar el grupo de activos o activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Le corresponde a la primera línea de defensa identificar los activos en cada proceso.

“Un activo, es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO que utiliza la organización para funcionar en el entorno digital. Así la entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano,

aumentando así su confianza en el uso del entorno digital."[2]

En esta etapa se deben identificar los contendores y activos de Información que se podrían ver afectados por las amenazas a las que estén expuestos, para este caso, la Agencia cuenta con una metodología de identificación y clasificación de Activos de Información liderada por el equipo de seguridad de la Información, la cual se encuentra articulada con la presente guía y con la matriz de riesgos.

Ilustración 5. Columnas para riesgos de seguridad digital en la matriz de riesgos

SOLO PARA RIESGOS DE SEGURIDAD DIGITAL			
El Riesgo inherente de seguridad digital se asocia a: (Confidencialidad, Integridad y Disponibilidad)	Tipo de Activo	Activo (Seguridad de la Información /Digital)	Amenaza (Seguridad de la Información /Digital)

Fuente: Equipo Planeación AND

Con el objetivo de que la gestión de riesgos de seguridad digital sea eficaz y eficiente, en la identificación de los riesgos de seguridad digital se debe realizar el análisis por proceso donde se tengan en cuenta los activos que tiene dicho proceso y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización

Nota: *tener en cuenta que la agrupación de activos debe ser del mismo tipo, ejemplo, analizar conjuntamente activos por tipo de hardware, software, información, entre otros, con el objetivo de determinar amenazas y vulnerabilidades comunes que puedan afectar a dicho grupo.*

Con el objetivo de facilitar la identificación de los riesgos, se lista a continuación las amenazas comunes, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos:

[2] *Fuente:https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b*

- Acceso a la red o al sistema de información por personas no autorizadas.
- Amenaza o ataque con bomba.
- Incumplimiento de relaciones contractuales.
- Infracción legal.
- Comprometer información confidencial.
- Ocultar la identidad de un usuario.
- Daño causado por un tercero.
- Daños resultantes de las pruebas de penetración.
- Destrucción de registros.
- Desastre generado por causas humanas.
- Desastre natural, incendio, inundación, rayo.
- Revelación de información.
- Divulgación de contraseñas.
- Malversación y fraude.
- Errores en mantenimiento.
- Fallo de los enlaces de comunicación.
- Falsificación de registros.
- Espionaje industrial.
- Fuga de información.
- Interrupción de procesos de negocio.
- Pérdida de electricidad.
- Pérdida de servicios de apoyo.
- Mal funcionamiento del equipo.
- Código malicioso.
- Uso indebido de los sistemas de información.
- Uso indebido de las herramientas de auditoría.
- Contaminación.
- Errores de software.
- Huelgas o paros.
- Ataques terroristas.
- Hurtos o vandalismo.
- Cambio involuntario de datos en un sistema de información.
- Cambios no autorizados de registros.
- Instalación no autorizada de software.
- Acceso físico no autorizado.
- Uso no autorizado de material con copyright.
- Uso no autorizado de software.
- Error de usuario.

Por su parte, las vulnerabilidades, son fallas o debilidades que afectan la confidencialidad, integridad y disponibilidad de los sistemas. La identificación podrá obtenerse de pruebas de vulnerabilidad, visitas, entrevistas y/o basados en los criterios que la Entidad vea necesarios. Las posibles amenazas y vulnerabilidades que ocasionan la aparición de un riesgo sobre un activo de información se relacionan a continuación, teniendo en cuenta el tipo de activo:

- Interfaz de usuario complicada.
- Contraseñas predeterminadas no modificadas.
- Eliminación de medios de almacenamiento sin eliminar datos.
- Sensibilidad del equipo a los cambios de voltaje.
- Sensibilidad del equipo a la humedad, temperatura o contaminantes.
- Inadecuada seguridad del cableado.
- Inadecuada gestión de capacidad del sistema.
- Gestión inadecuada del cambio.
- Clasificación inadecuada de la información.
- Control inadecuado del acceso físico.
- Mantenimiento inadecuado.
- Inadecuada gestión de red.
- Respaldo inapropiado o irregular.
- Inadecuada gestión y protección de contraseñas.
- Protección física no apropiada.
- Reemplazo inadecuado de equipos viejos.
- Falta de formación y conciencia sobre seguridad.
- Inadecuada segregación de funciones.
- Mala segregación de las instalaciones operativas y de prueba.
- Insuficiente supervisión de los empleados y vendedores.
- Especificación incompleta para el desarrollo de software.
- Pruebas de software insuficientes.
- Falta de política de acceso o política de acceso remoto.
- Ausencia de política de escritorio limpio y pantalla clara.
- Falta de control sobre los datos de entrada y salida.
- Falta de documentación interna.
- Carencia o mala implementación de la auditoría interna.
- Falta de políticas para el uso de la criptografía.
- Falta de procedimientos para eliminar los derechos de acceso a la terminación del empleo.
- Desprotección en equipos móviles.
- Falta de redundancia, copia única.
- Ausencia de sistemas de identificación y autenticación.

- No validación de los datos procesados.
- Ubicación vulnerable a inundaciones.
- Mala selección de datos de prueba.
- Copia no controlada de datos.
- Descarga no controlada de Internet.
- Uso incontrolado de sistemas de información.
- Software no documentado.
- Empleados desmotivados.
- Conexiones a red pública desprotegidas.
- Los derechos del usuario no se revisan regularmente.

6.3. Valoración de Riesgos

Para llevar a cabo la valoración de los riesgos es necesario tener en cuenta los siguientes aspectos:

- Análisis de riesgos: busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto. La probabilidad se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. A continuación se establecen los criterios para definir el nivel de probabilidad:

Ilustración 6. Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

Ahora bien, para determinar el impacto del riesgo se definen como variables principales, los impactos económicos y reputacionales, es decir todos los temas de afectación se agrupan en impacto económico y reputacional. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado. A continuación se establecen los criterios para definir el nivel de impacto:

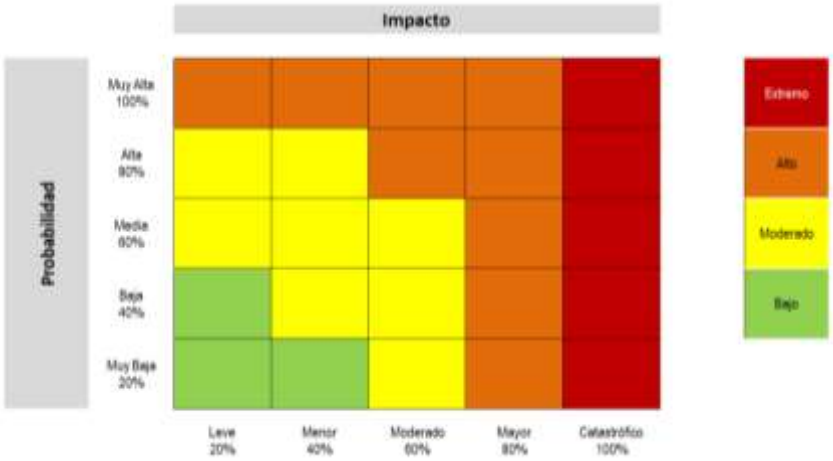
Ilustración 7. Criterios para definir el nivel de impacto

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

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

- Evaluación de riesgos: a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (Riesgo Inherente), con lo cual se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. A continuación se muestran las 4 zonas de severidad en la matriz de calor:

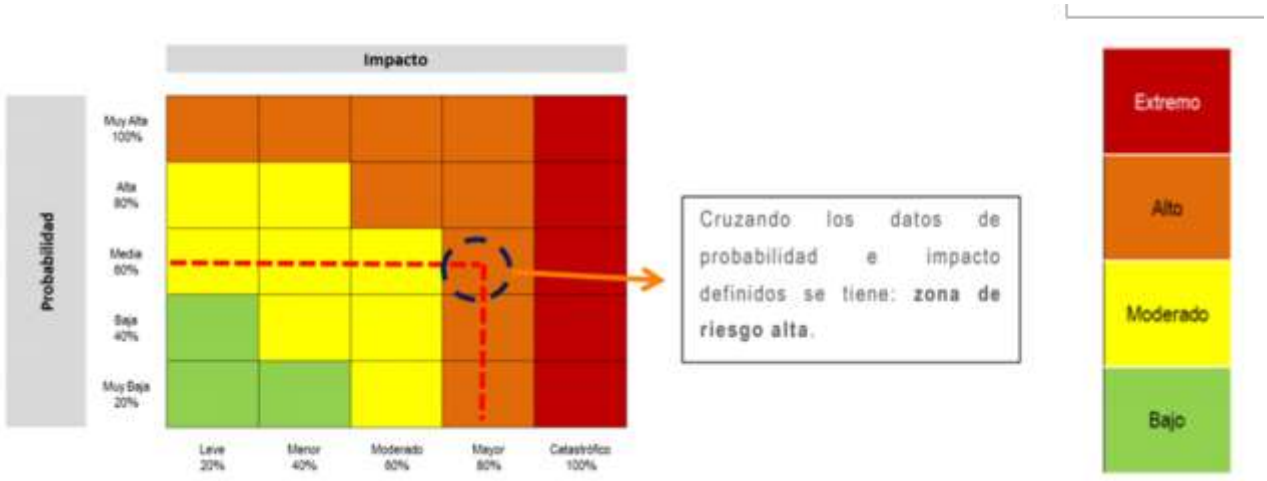
Ilustración 8. Matriz de calor – Niveles de severidad del riesgo



Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

Dependiendo del cruce de los datos entre el resultado de probabilidad e impacto se define la zona de riesgo, así:

Ilustración 9. Cruce de probabilidad e impacto para definir zona del riesgo



Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

Una vez se cuenta con la zona del riesgo identificada se debe llevar a cabo la valoración de controles. En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta que la identificación de dichos

controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. De igual manera, los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

En esta etapa es importante identificar los controles existentes para evitar trabajo o reprocesos innecesarios. Adicionalmente, se debe revisar la efectividad de los controles. Para la revisión de los controles existentes, se debe tener en cuenta:

- Revisar los documentos que contengan información sobre las actividades de control.
- Verificar con las personas responsables de cada proceso y proyecto.
- Efectuar revisiones en sitio, comparando los controles implementados contra la lista de controles que deberían estar.
- Cuáles controles están implementados correctamente y si son o no eficaces.
- Revisar los resultados de las auditorías internas.

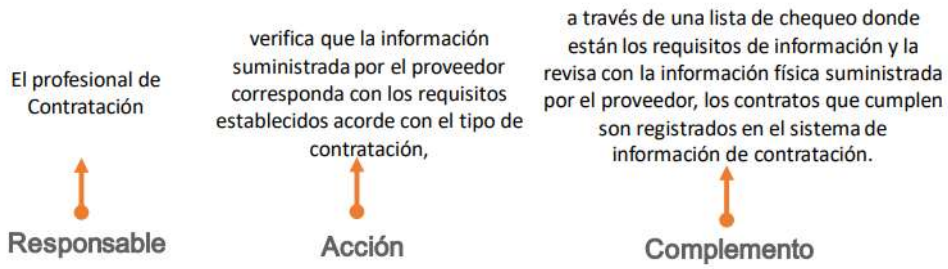
Ahora bien, para una adecuada redacción del control el Departamento Administrativo de la Función Pública propone la siguiente estructura:

- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.

- Acción: se determina mediante verbos que indican la acción que deben realizar como parte del control.

- Complemento: corresponde a los detalles que permiten identificar claramente el objeto del control.

Ilustración 10. Ejemplo de la estructura propuesta para la redacción de Controles



Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

Una vez definido el control es necesario determinar la Tipología de dicho control y en el momento en que debe ser activado, en el marco del ciclo de los procesos y , por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la siguiente ilustración se consideran 3 fases globales del ciclo de un proceso así:

Ilustración 11. Ciclo del proceso y tipologías de controles

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

Acorde a lo anterior, se encuentran las siguientes tipologías de controles:

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

Así mismo, de acuerdo con la forma como se ejecutan se encuentra:

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

Ya identificados los tipos de controles y la forma como se ejecutan, se debe llevar a cabo el Análisis y evaluación de los controles teniendo en cuenta sus atributos. A continuación se presentan los

atributos para el análisis del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En esta ilustración se puede observar la descripción y peso asociados a cada uno así:

Ilustración 12. Atributos para al análisis de controles

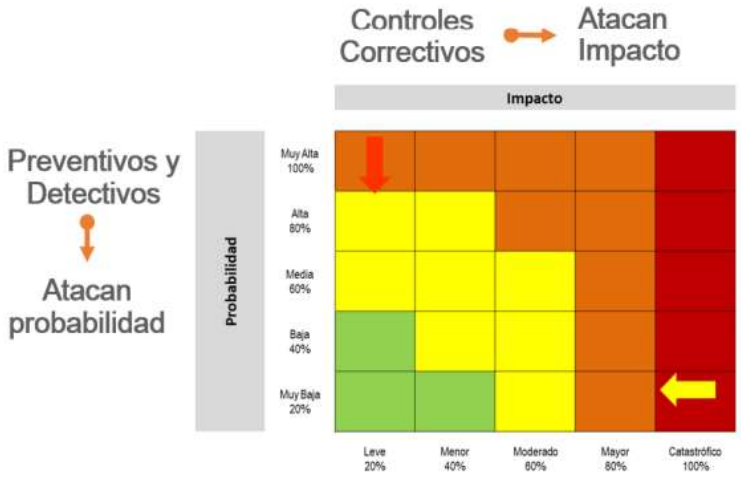
Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten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

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

Nota: Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento en la matriz de calor que corresponde a la siguiente ilustración, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles

Ilustración 13. Movimiento en la matriz de calor acorde con el tipo de control



Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

A partir del análisis de los atributos de los controles y su peso, se establece el valor de cada control, lo cual va a permitir generar el Riesgo Residual, de acuerdo con una fórmula planteada por el DAFP, es decir, el riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente.

Para la aplicación de los controles se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control. Para mayor claridad, en la siguiente ilustración se da al ejemplo donde se observan los cálculos requeridos para la aplicación de los controles:

Ilustración 14. Ejemplo de aplicación de controles para establecer el Riesgo Residual

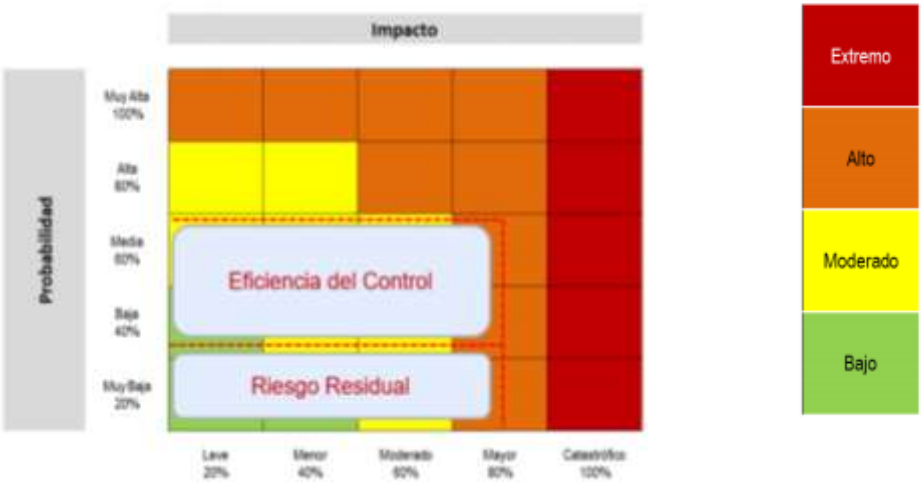
Controles y sus características				Peso
Control 1 El profesional del área de contratos verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Documentación	Documentado	X	-
		Sin documentar		-
	Frecuencia	Continua	X	-
		Aleatoria		-
	Evidencia	Con registro	X	-
		Sin registro		-
Total valoración control 1				40%

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = 36%
	Valor probabilidad para aplicar 2° control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = 25,2%
	Probabilidad Residual	25,2 %			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	80%			

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

De acuerdo con el resultado de la probabilidad y el impacto residual se ubica el riesgo residual en la zona de riesgo que corresponda, así:

Ilustración 15. Movimiento en la matriz de calor del Riesgo Residual

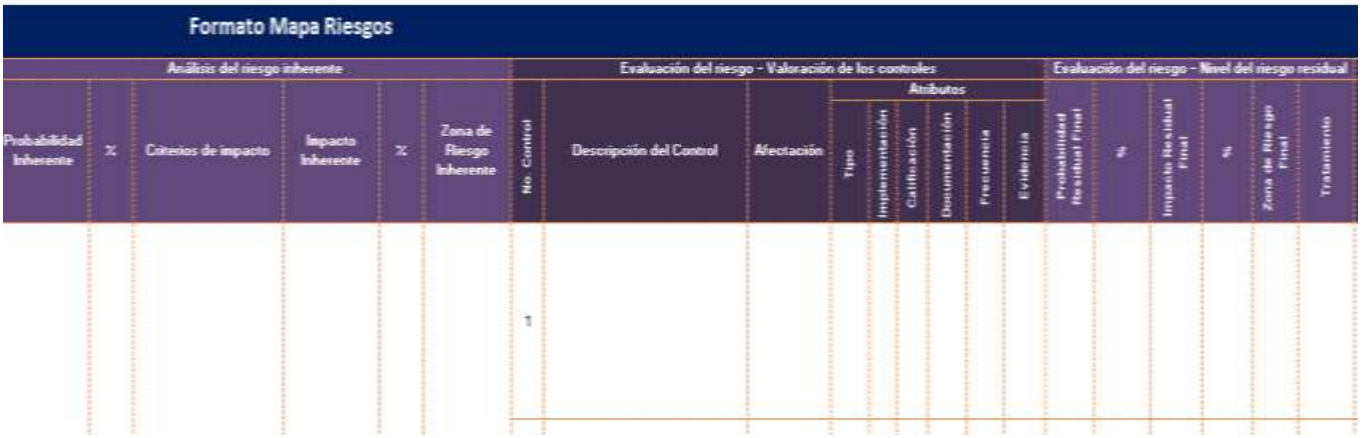


Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

En este contexto, la Agencia Nacional Digital hace la valoración de los riesgos, incluyendo todos los aspectos antes mencionados a través del SM.FT.15 Mapa de Riesgos de Gestión y Seguridad Digital, el cual está adaptado sobre el mapa de riesgos propuesto por el DAFP, tal como se muestra a continuación:

Ilustración 16. Mapa de Riesgos – Valoración de los Riesgos



Fuente: Equipo Planeación AND

- Estrategias para combatir el riesgo: es la decisión que se toma frente a un determinado nivel de riesgo, la cual puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente. En la siguiente ilustración se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Ilustración 17. Estrategias para combatir el Riesgo

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V5, DAFP

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio y se consideraría un control correctivo.

En este contexto, la estrategia para combatir el riesgo en la Agencia Nacional Digital, incluyendo todos los aspectos antes mencionados se identifica a través del SM.FT.15 Mapa de Riesgos de Gestión y Seguridad Digital, el cual está adaptado sobre el mapa de riesgos propuesto por el DAFP, tal como se muestra a continuación:

Ilustración 18. Mapa de Riesgos – Estrategia para combatir el riesgo y plan de acción

Evaluación del riesgo – Nivel del riesgo residual						Plan de Acción						
Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento	Plan de Acción	Responsable	Fecha Implementación	Fecha Seguimiento	Seguimiento	Estado	Indicador

Fuente: Equipo Planeación AND

- Herramientas para la gestión del riesgo: como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se tienen las siguientes:

  Gestión de eventos: un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología. Algunas fuentes para establecer una base histórica de eventos pueden ser:

  - Mesa de ayuda
  - Las PQRD (peticiones, quejas, reclamos, denuncias)
  - Oficina jurídica
  - Líneas internas de denuncias

  Este mecanismo genera información para que el evento no se vuelva a presentar, así mismo, es posible establecer el desempeño de los controles así: Desempeño del control= # eventos / frecuencia del riesgo (# veces que se hace la actividad)

  Indicadores clave de riesgo: hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar. Un indicador clave de riesgo, o KRI,

por su sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos.

Para la Agencia Nacional Digital, la herramienta para la gestión del riesgo principal es el Mapa de Riesgos.

- Monitoreo y revisión: el modelo integrado de plantación y gestión (MIPG) desarrolla en la dimensión 7 control interno las líneas de defensa para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores de la entidad.

  Para la Agencia el mencionado monitoreo y revisión se hace en el marco de las líneas de defensa descritas en el aparto 5 de este documento "Responsabilidades frente a la Gestión del Riesgo".

6.4. Lineamientos Riesgos relacionados con posibles actos de corrupción

Dado que para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018 del DAFP, en la Agencia Nacional Digital se continuará llevando a cabo la gestión de este tipo de riesgos de acuerdo con la Guía para la Administración de Riesgos de la AND, versión 1. Por lo anterior se continúa manejando el SM.FT.05 Mapa de riesgos para procesos.

6.5. Lineamientos Riesgos de Seguridad Digital

Los riesgos de seguridad digital serán identificados, valorados y tratados de acuerdo con la metodología descrita en la presenta guía.

Nota: Al finalizar la evaluación de los riesgos identificados, el gestor de riesgos de seguridad digital debe hacer firmar el documento de aceptación de los riesgos a los diferentes dueños de proceso, con el fin de establecer responsabilidad en la gestión de los riesgos de seguridad digital.

6.6. Seguimiento y Registro de riesgos materializados

El seguimiento de los riesgos identificados se realizará con base en el nivel de riesgo residual de acuerdo con las escalas descritas en la matriz de calor residual, así:

Nivel de Riesgo Residual	Periodicidad de Seguimiento
Extremo	Mensual
Alto	Trimestral
Moderado	Semestral
Bajo	Anual

El seguimiento principal estará en cabeza de los líderes de procesos, gerentes de proyectos y el equipo de trabajo que se designe para este fin, posteriormente desde el rol de Planeación, se realizará el seguimiento de acuerdo con la periodicidad descrita en la tabla anterior, en el caso que sea necesario, se realizarán las recomendaciones necesarias en relación con el diseño y ejecución de los controles incluidos los controles que mitigan los riesgos estratégicos o institucionales.

Anualmente se revisará el mapa de riesgos completo, tomando como base las auditorías realizadas por Control Interno, los organismos de control y las notificaciones de materialización realizadas por los líderes de procesos y gerentes de proyecto, con el objetivo de actualizar el mapa de riesgos institucional conforme a los cambios presentados en cada vigencia. Adicional, en este seguimiento se realizará la verificación de la efectividad de los controles identificados en los riesgos de los procesos y proyectos.

El reporte de los eventos de riesgos materializados será enviado mediante correo electrónico por el Líder del proceso o gerente de proyecto, al equipo asignado con funciones de Planeación, el cuál debe informar la situación presentada (incluyendo el análisis de causas respectivo), fecha inicio y fin del suceso, fecha de reporte, riesgo al cual está asociado, proceso o proyecto en donde se identificó el suceso, impacto, acciones adelantadas, actividades de control relacionadas y consecuencias. Este reporte debe realizarse cuando el evento del riesgo materializado se presente.

Partiendo del análisis de causas del evento materializado, se debe formular un plan de mejora que indique la corrección o actividades de mitigación de este.

Los colaboradores con rol y funciones de Planeación deben validar, consolidar y analizar los eventos de riesgos materializados reportados por los procesos o proyectos, y presentar en los casos requeridos, ante el Comité de Gestión y Desempeño aquellos que deban ser de su conocimiento y revisión. A través del Comité de Coordinación de Control Interno se realizará la verificación de la gestión realizada a los riesgos materializados.

7. COMUNICACIÓN

Los colaboradores con rol y funciones de Planeación y Control Interno coordinarán las acciones necesarias para promover la comunicación de información que promueva la cultura de gestión integral de los riesgos en la AND.

De igual forma, Planeación coordinará la divulgación y publicación de la matriz integral de riesgos, considerando la posibilidad de presentar la matriz integral o vista específica de la misma, las cuales pueden ser por nivel de identificación, por tipo de riesgo o por la clasificación que se considere pertinente, de acuerdo con las necesidades de divulgación y las partes interesadas a quienes se dirija la publicación, principalmente considerando: la página web y la intranet.

Respecto a los riesgos de Seguridad de la Información, todas las novedades se comunicarán al Oficial de Seguridad de la Información y se dejará la documentación asociada, que puede ser por correo electrónico u oficio, de igual manera el/la Oficial deberá presentar en el Comité de Gestión y Desempeño dichas novedades.

8. CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
1	23/09/2020	Emisión del documento
2	11/10/2021	Ajuste de todo el documento de acuerdo con la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 5 del DAFP.

Elaboró	Revisó	Aprobó
Johanna Laverde Moncada Profesional de Planeación	Anyela Méndez Profesional Control Interno, contratista Jorge Camargo Profesional Oficial de Seguridad de la Información	Johan Sebastian Eslava Garzón Director