AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

MANUAL DE GESTIÓN DEL RIESGO

BOGOTÁ D.C. FEBRERO DE 2020

TABLA DE CONTENIDO

1. OBJETIVO

1.1. OBJETIVO GENERAL

Establecer los lineamientos y criterios que se deben aplicar en la Agencia para la Reincorporación y la Normalización - ARN para la identificación, análisis, valoración, seguimiento y monitoreo de los riesgos de gestión, corrupción, seguridad digital, protección de datos personales y demás requeridos por la normatividad que pueden afectar el logro de los objetivos institucionales, de procesos, proyectos y planes.

1.2. OBJETIVOS ESPECÍFICOS

- Definir la metodología que facilite a los procesos la adecuada gestión del riesgo.

- Hacer corresponsables a los colaboradores de la ARN en la búsqueda de las acciones encaminadas a prevenir la materialización del riesgo.

- Desarrollar capacidades en cada dependencia de la ARN de manera que les permita gestionar los riesgos de gestión, corrupción, seguridad digital inherentes a los procesos en los que participa y el establecimiento de las medidas de prevención a través de la formulación y ejecución de acciones preventivas.

- Establecer una base confiable para la toma de decisiones y la planificación.

- Asegurar el cumplimiento de normas, leyes y regulaciones.

2. ALCANCE

Este documento establece la política institucional de administración de riesgos, con estructuración de responsabilidades, metodología, herramientas y evaluación, acorde con el Modelo Integrado de Planeación y Gestión-MIPG. Los lineamientos y criterios establecidos en este documento aplican para los procesos y dependencias de la Agencia para la Reincorporación y la Normalización.

3. DEFINICIONES

ACTIVO: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización (ISO/IEC 13335-12004).

ACTIVO DE INFORMACIÓN: Es cualquier información o sistema relacionado con el tratamiento de esta, que tenga valor para la entidad.

ADMINISTRACIÓN DE RIESGOS: Conjunto de elementos de control que, al interrelacionarse, permiten a la entidad pública, evaluar la ocurrencia de eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función.

AGENTES GENERADORES DEL RIESGO: Se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.

AMENAZAS: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

ANÁLISIS DE RIESGO: Elemento de control, que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública, para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar cuan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

AUTOEVALUACIÓN DEL CONTROL: Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún efectivos y apropiados.

CAUSA: Son los medios, las circunstancias y agentes generadores de riesgo, solos o en combinación con otros. Los agentes generadores de riesgo se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.

CAUSA EXTERNA (AMENAZA): Causa potencial externa de un incidente no deseado, el cual puede causar el daño a un sistema o la entidad.

CAUSA INTERNA (VULNERABILIDAD): Debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

CIBERSEGURIDAD: Conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación,

confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.
COMPARTIR EL RIESGO: Se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.

CONFIDENCIALIDAD: Acceso a la información por parte únicamente de quien esté autorizado, característica/propiedad por la que la información no está disponible o revelada a individuos, entidades o procesos no autorizados (ISO/IEC 13335-1:2004).

CONSECUENCIA (IMPACTO): Los efectos o situaciones resultantes de la materialización del riesgo que impactan los objetivos de la entidad o el proceso, expresado cualitativa o cuantitativamente.

CONTROL CORRECTIVO: Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad detectada u otra situación no deseable.

CONTROL PREVENTIVO: Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad potencial u otra situación potencial no deseable.

CONTROL: Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

DATO: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la ARN, así como cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

DISPONIBILIDAD: Propiedad de ser accesible y utilizable a demanda por una entidad.

ESTIMACIÓN DEL NIVEL DEL RIESGO INICIAL o INHERENTE: Se realiza a través de la determinación de la probabilidad y el impacto que puede causar la materialización del riesgo.

EVALUACIÓN DEL RIESGO: Proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.

EVENTO: Incidente o situación, que ocurre en un lugar determinado durante un periodo de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

FRECUENCIA: Medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

GESTIÓN 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.

GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL: Conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

IDENTIFICACIÓN DEL RIESGO: Descripción de la situación no deseada. Se puede entender como el proceso que permite determinar que podría suceder, por qué sucedería y de qué manera se llevaría a cabo.

IMPACTO CREDIBILIDAD O IMAGEN: Se refiere a la pérdida de la misma frente a diferentes actores sociales o dentro de la entidad.

IMPACTO DE CONFIDENCIALIDAD DE LA INFORMACIÓN: Se refiere a la pérdida o revelación de la misma. Cuando se habla de información reservada institucional se hace alusión a aquella que por la razón de ser de la entidad sólo puede ser conocida y difundida al interior de la misma; así mismo, la sensibilidad de la información depende de la importancia que ésta tenga para el desarrollo de la misión de la entidad.

IMPACTO LEGAL: Se relaciona con las consecuencias legales para una entidad, determinadas por los riesgos relacionados con el incumplimiento en su función administrativa, ejecución presupuestal y normatividad aplicable.

IMPACTO OPERATIVO: Aplica en la mayoría de las entidades para los procesos clasificados como estratégicos o de apoyo, ya que sus riesgos pueden afectar el normal desarrollo de otros procesos dentro de la misma.

IMPACTO: Se entiende como las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso; propiedad/característica de salvaguardar la exactitud y completitud de los activos (ISO/IEC 13335-1:2004).

MAPA DE RIESGOS: Documento con la información resultante sobre el análisis y la valoración de los riesgos institucionales.

MONITOREAR: Comprobar, supervisar, observar, o registrar la forma en que se lleva a cabo una actividad con el fin de identificar posibles cambios.

NIVELES DE ACEPTACIÓN DEL RIESGO O TOLERANCIA AL RIESGO: Establece “los niveles aceptables de desviación relativa a la consecución de los objetivos” (NTC GTC 137 Numeral 3.7.16). Están asociados a la estrategia de la entidad y se consideran para cada uno de los procesos. Para los riesgos de corrupción son inaceptables.

PÉRDIDA: Consecuencia negativa que trae consigo un evento.

PROBABILIDAD: Se entiende como la posibilidad de ocurrencia del riesgo. Se debe medir a través de la relación entre los hechos ocurridos realmente y la cantidad de eventos que pudieron ocurrir; puede ser medida con criterios de frecuencia o factibilidad.

REDUCCIÓN DEL RIESGO: Aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia.

RIESGO: Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

RIESGO DE CORRUPCIÓN: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

RIESGO DE GESTIÓN: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

RIESGO DE SEGURIDAD DIGITAL: Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan. Se describe en términos de pérdida o degradación de alguna de las tres características básicas: confidencialidad, integridad y disponibilidad.

RIESGOS DE SEGURIDAD DIGITAL: Son los relacionados con el desarrollo de actividades del entorno digital. Estos riesgos pueden resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan. Se describe en términos de pérdida o degradación de alguna de las tres características básicas: confidencialidad, integridad y disponibilidad.

RIESGO INHERENTE o INICIAL: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

RIESGO RESIDUAL: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

RIESGOS ESTRATÉGICOS: Posibilidad de ocurrencia de eventos que puedan poner en peligro el cumplimiento de la misión y/o los objetivos estratégicos de la entidad.

RIESGOS OPERATIVOS: Posibilidad de ocurrencia de eventos que puedan poner en peligro el cumplimiento de los objetivos de los procesos de la entidad.

RIESGOS TECNOLÓGICOS: Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

SISTEMA DE ADMINISTRACIÓN DE RIESGO: Conjunto de elementos del direccionamiento estratégico de una entidad concerniente a la administración del riesgo.

TRATAMIENTO DE DATOS PERSONALES: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. En el caso de las imágenes de personas

determinadas o determinables, operaciones como la captación, grabación, transmisión, almacenamiento, conservación, o reproducción en tiempo real o posterior, entre otras, son consideradas como tratamiento de datos personales y, en consecuencia, se encuentran sujetas al régimen general de protección de datos personales.

TRATAMIENTO DE RIESGOS: Proceso para modificar el riesgo (NTC GTC137, Numeral 3.8.1).

VULNERABILIDAD: Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

4. CONSIDERACIONES GENERALES

La ARN determina lineamientos para la identificación, administración, tratamiento, control y seguimiento de riesgos que puedan afectar la consecución de sus objetivos.

El enfoque de la ARN para la gestión de riesgos es proactivo, preventivo e integral; armónico con los lineamientos trazados por el Departamento Administrativo de la Función Pública-DAFP; de acuerdo con el Marco Estratégico institucional establecido.

Para el desarrollo de la metodología de construcción del mapa de riesgos se debe seguir el esquema que se presenta a continuación:

5. POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DE RIESGOS

La ARN adopta una política institucional de administración de riesgos integral que establece funciones y responsabilidades para la gestión del riesgo, con estructuración de metodología y herramientas y dispone evaluación sistemática de los riesgos por parte de los líderes de proceso y sus equipos de trabajo, así como la evaluación del Grupo de Control Interno de Gestión.

Acorde con el Modelo Integrado de Planeación y Gestión-MIPG y los lineamientos del Departamento Administrativo de la Función Pública-DAFP, la política institucional de administración de riesgos de la ARN está basada en una línea estratégica y tres líneas de defensa, corresponsabilidad, plan anual de auditorías basado en riesgos, monitoreo de riesgos, intolerancia total frente a los riesgos de corrupción, alineamiento estratégico y establecimiento de zonas de riesgo, y armonización con otras políticas y planes institucionales, a saber:

5.1. LÍNEA ESTRATÉGICA

A cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno, define el marco general para el control y gestión del riesgo en la Entidad.

5.2. PRIMERA LÍNEA DE DEFENSA

Los jefes de dependencia y/o coordinadores de grupo constituyen la primera línea de defensa y tienen el deber de implementar los mecanismos de identificación, valoración, control, acciones y mecanismos de seguimiento para la mitigación de los riesgos, reportando a la segunda línea sus progresos e inconvenientes.

5.3. SEGUNDA LÍNEA DE DEFENSA

Los líderes de proceso, jefe de la Oficina Asesora de Planeación, supervisores e interventores de contratos, comité de contratación y presupuesto, comité de conciliación y defensa judicial, mesa de seguridad de información, constituyen la segunda línea de defensa. Los líderes de proceso tienen el deber de realizar el análisis de la efectividad de las acciones y mecanismos de seguimiento establecidos, así como la asesoría en la aplicación de los sistemas institucionales de tratamiento de riesgos y adoptar los dispositivos de difusión que defina el Comité Institucional de Coordinación de Control Interno, en el nivel directivo, misional y operativo, de tal forma que se asegure su implementación. Los supervisores e interventores tienen el deber de analizar la efectividad de las acciones de control de riesgos en los contratos que supervisan o en los que realizan la interventoría. La Jefatura de la Oficina Asesora de Planeación tiene el deber de coordinar el monitoreo y seguimiento del sistema institucional de control de riesgos y presentar los resultados en el Comité Directivo y/o en el Comité Institucional de Gestión Desempeño, así como de facilitar las evaluaciones independientes que realice el Grupo de Control Interno de Gestión.

5.4. TERCERA LÍNEA DE DEFENSA

El Grupo de Control Interno de Gestión constituye la tercera línea de defensa y tiene el deber de realizar evaluación independiente sobre la gestión del riesgo en la entidad, formular e implementar en cada vigencia un plan anual de auditorías basado en riesgos y comunicar los resultados de la evaluación de la gestión del riesgo.

Las **tres líneas de defensa** (líderes de proceso, jefes de dependencia, coordinadores de grupo, supervisores e interventores de contratos, comité de contratación y presupuesto, comité de conciliación y defensa judicial, mesa de seguridad de información y Grupo de Control Interno de Gestión) deben conservar

evidencia de la comunicación de la información y reporte de la administración del riesgo en todas sus etapas.

5.5. CORRESPONSABILIDAD

La ARN involucra como sujetos corresponsables de su política institucional de administración de riesgos a todos los colaboradores de la entidad (servidores públicos, contratistas, pasantes y voluntarios).

El Comité Institucional de Coordinación de Control Interno se asegura de su incorporación en todos los niveles de la entidad.

5.6. PLAN ANUAL DE AUDITORÍAS BASADO EN RIESGOS

En concordancia con las normas legales, el Grupo de Control Interno de Gestión incluye en su plan anual de auditorías específicamente dirigidas a evaluar la identificación, valoración y control de los riesgos en la entidad.

5.7. MONITOREO DE RIESGOS

La ARN dispone de un software para el monitoreo sistemático de los riesgos.

5.8. INTOLERANCIA TOTAL FRENTE A RIESGOS DE CORRUPCIÓN

La ARN no tolera ningún nivel de riesgos de corrupción. Por ello, todos los riesgos identificados en el mapa de riesgos de corrupción son considerados riesgos extremos y requieren monitoreo y seguimiento mensual a los controles establecidos e incluir evaluación de la gestión de riesgos de corrupción en el plan anual de auditorías basado en riesgos, en todas las vigencias.

5.9. ALINEAMIENTO ESTRATÉGICO Y ZONAS DE RIESGO

La administración de riesgos institucionales debe estar alineada con los objetivos estratégicos y con los procesos institucionales, de manera que se prevenga y/o minimice cualquier evento que pueda afectar negativamente el logro de dichos objetivos, sin menoscabo del adecuado tratamiento de los riesgos operacionales.

Para los riesgos que se valoren en **Zona de Riesgo Extrema,** se realiza registro monitoreo y seguimiento mensual y los valorados en **zonas de Riesgo Alta, Moderada o Baja,** trimestralmente.

5.10. ARMONIZACIÓN CON OTRAS POLÍTICAS, PLANES Y PROYECTOS INSTITUCIONALES

La política institucional de administración de riesgos se armoniza con los planes que hacen parte de las estrategias, productos o acciones del Plan Estratégico Institucional, de los proyectos de inversión de la Entidad o los que surjan con motivo del desarrollo del plan de continuidad del negocio, de políticas públicas del Gobierno Nacional o de normas legales.

6. OBJETIVOS DE LA POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DE RIESGOS

El objetivo general de la política institucional de administración de riesgos es defender la gestión de la entidad ante la posible ocurrencia de eventos que afecten el logro de sus objetivos estratégicos u operacionales, contribuir a la formulación e implementación de sus estrategias y facilitar el desarrollo de sus acciones mediante la mitigación de la probabilidad y el impacto de los riesgos.

Los objetivos específicos de la política institucional de administración de riesgos son:

- En el marco del Modelo Integrado de Planeación y Gestión-MIPG, trazar lineamientos para que todos los procesos de la entidad establezcan mecanismos de identificación, valoración, control y acciones de mitigación de los riesgos, verificados por sólidos mecanismos de seguimiento y gestión, con un enfoque preventivo y proactivo.

- Establecer sistemas, definiendo roles, responsabilidades, herramientas y procedimientos para el control de los riesgos institucionales.

- Involucrar a todas las dependencias, servidores, contratistas y colaboradores de la entidad en la corresponsabilidad de control de los riesgos institucionales, desarrollando diversos mecanismos de sensibilización y comunicación al respecto.

7. DIRECTRICES GENERALES FRENTE A LA ADMINISTRACIÓN DEL RIESGO EN LA ARN (ROLES Y RESPONSABILIDADES)

- La Alta Dirección, en cabeza del representante legal, lidera la política institucional de administración de riesgos.

- La Oficina Asesora de Planeación orienta, asesora la implementación de la metodología de gestión del riesgo en la entidad y administra la herramienta

dispuesta por la entidad para la operatividad de los mapas de riesgos. El Grupo de Control Interno de Gestión efectúa la evaluación de la eficacia y efectividad en la gestión del riesgo.

- La responsabilidad sobre la identificación, análisis, evaluación y tratamiento de los riesgos es de cada dependencia/proceso en cabeza del líder, quien cuenta para este propósito con la asesoría y acompañamiento de la Oficina Asesora de Planeación.

- La responsabilidad sobre la implementación de los controles y acciones contenidas en el mapa de riesgos, el seguimiento, la verificación de su eficacia y efectividad, el proponer cambios, la adecuada documentación y socialización es de los líderes de proceso y/o jefes de dependencia a cargo de los riesgos.

- Las acciones definidas para el tratamiento de los riesgos se consignan en la herramienta establecida por la Entidad, con sus respectivas fechas de inicio y terminación para cada acción.

- Para el seguimiento del tratamiento de los riesgos se debe tener en cuenta lo establecido en el título “Seguimiento basado en reporte de acciones”, del documento Manual de Seguimiento a la Planeación y Gestión Institucional, código DE-M-03.

- Para el tratamiento de los riesgos se tiene en cuenta la valoración determinada en el mapa de riesgos de la siguiente manera:

    - Las acciones por emprender sobre los riesgos ubicados en la zona de riesgo extrema y alta y los tiempos de ejecución de las mismas son definidas por los líderes de proceso y/o jefes de dependencia y los dueños del riesgo y son sometidas a revisión del Comité Institucional de Gestión y Desempeño y aprobación del Comité Institucional de Coordinación de Control Interno. Dichas acciones estarán orientadas a reducir, evitar, compartir o transferir el riesgo.

    - Cuando el cálculo del nivel de riesgo que permanece luego de tomar medidas de tratamiento **(riesgo residual),** se ubique en zona de riesgo baja o moderada, no se requiere implementar acciones preventivas. Sin embargo, se debe continuar con la aplicación de los controles establecidos y el monitoreo permanente del comportamiento del riesgo. Se someten a revisión y aprobación por parte de los líderes de proceso.

- Las acciones por ejecutar en el marco de la administración del riesgo deben orientarse a la optimización de los procedimientos, fortalecimiento de los controles, implementación y fortalecimiento de las políticas encaminadas a cumplir con los objetivos institucionales.

- Cuando las acciones del riesgo no son cumplidas dentro de las fechas establecidas, estas deben trasladarse a un plan de mejoramiento para su tratamiento, esta acción debe quedar registrada en el software SIGER, de acuerdo con lo establecido en el “Procedimiento gestión de acciones correctivas y de mejora”, código EM- P-01.

- Corresponde a la Oficina Asesora de Planeación impulsar a nivel institucional una cultura de prevención y gestión del riesgo congruente con el Sistema de Gestión Integral, facilitando así el cumplimiento de los propósitos de la Entidad y los requerimientos del Sistema, para ello se deben planificar y desarrollar acciones en el marco del Plan Institucional de Capacitación.

- La Política de Administración del Riesgo y los controles establecidos se revisan al menos una vez al año, en el último trimestre de cada vigencia, y se ajustan si es necesario para adaptarlos a los cambios que se puedan presentar en la Entidad.

- Para la difusión y apropiación de la política institucional de administración de riesgos, en el plan anual de capacitación y en el plan de comunicación interna se incluyen actividades sobre la apropiación.

8. CONTENIDO Y DESARROLLO

Para implementar la política institucional de riesgos y aplicar las directrices señaladas, en la ARN se sigue la siguiente metodología:

8.1. IDENTIFICACIÓN DE RIESGOS

8.1.1. Contexto Estratégico

Para establecer los riesgos en los procesos de la Entidad se parte de analizar el contexto externo, el contexto interno y el contexto del proceso. El contexto estratégico está definido como las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos institucionales.

Las situaciones externas o del entorno pueden ser de carácter social, cultural, económico, tecnológico, político, normativo y legal, bien sea internacional, nacional o regional según sea el caso de análisis.

Las situaciones internas están relacionadas con la estructura, cultura organizacional, el modelo de operación, el cumplimiento de los planes y programas, los sistemas de información, los procesos y procedimientos y los recursos humanos y económicos con los que cuenta una entidad.

Para los riesgos de seguridad de información, se debe seleccionar entre los siguientes factores internos y externos:

FACTORES INTERNOS (VULNERABILIDADES)	
TIPO	**DESCRIPCIÓN**
Procesos	• Falta de procedimiento formal para el registro y retiro del registro de usuario • Falta de proceso formal para la revisión (supervisión) de los derechos de acceso • Falta o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes • Falta de procedimiento de monitoreo de los recursos de procesamiento información • Falta de auditorías (supervisiones) regulares Abuso de los derechos • Falta de procedimientos de identificación y evaluación de riesgos • Falta de reportes sobre fallas incluidos en los registros de administradores y operador • Respuesta inadecuada de mantenimiento del servicio • Falta o insuficiencia en el acuerdo a nivel de servicio • Falta de procedimiento de control de cambios Incumplimiento en el mantenimiento del sistema de información • Falta de procedimiento formal para el control de la documentación del SGSI • Falta de procedimiento formal para la supervisión del registro del SGSI • Falta de procedimiento formal para la autorización de la información disponible al público

FACTORES INTERNOS (VULNERABILIDADES)	
TIPO	**DESCRIPCIÓN**
	• Falta de asignación adecuada de responsabilidades en la seguridad digital • Falta de plan de continuidad del negocio • Falta de políticas sobre el uso del correo electrónico • Falta de procedimientos para la introducción del software en los sistemas operativos • Falta de registros en las bitácoras*(logs) de administrador y operario. • Falta de procedimientos para el manejo de información clasificada • Falta de responsabilidades en la seguridad digital en la descripción de los cargos • Falta o insuficiencia en las disposiciones (con respecto a la seguridad digital) en los contratos con los empleados • Falta de política formal sobre la utilización de computadores portátiles • Falta de control de los activos que se encuentran fuera de las instalaciones • Falta o insuficiencia de política sobre limpieza de escritorio y de pantalla • Falta de autorización de los recursos de procesamiento de la información • Falta de mecanismos de monitoreo establecidos para las brechas en la seguridad • Falta de revisiones regulares por parte de la gerencia • Falta de procedimientos para la presentación de informes sobre las debilidades en la Seguridad • Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales
Recurso Humano	• Ausencia del personal • Procedimientos inadecuados de contratación • Entrenamiento insuficiente en seguridad • Uso incorrecto de software y hardware • Falta de conciencia acerca de la seguridad • Falta de mecanismos de monitoreo • Trabajo no supervisado del personal externo o de limpieza • Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería

FACTORES INTERNOS (VULNERABILIDADES)	
TIPO	**DESCRIPCIÓN**
Infraestructura	• Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos • Ubicación en un área susceptible de inundación • Red energética inestable • Falta de protección física de las puertas y ventanas de la edificación
Tecnología	**RED** • Falta de prueba del envío o la recepción de mensajes • Líneas de comunicación sin protección • Tráfico sensible sin protección • Conexión deficiente de los cables. • Punto único de falla • Falta de identificación y autentificación de emisor y receptor • Arquitectura insegura de la red • Transferencia de contraseñas autorizadas • Gestión inadecuada de la red (capacidad de recuperación del enrutamiento) • Conexiones de red pública sin protección **HARDWARE** • Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento. • Falta de esquemas de reemplazo periódico. • Susceptibilidad a la humedad, el polvo y la suciedad. • Sensibilidad a la radiación electromagnética • Falta de control de cambio con configuración eficiente • Susceptibilidad a las variaciones de tensión • Susceptibilidad a las variaciones de temperatura • Almacenamiento sin protección • Falta de cuidado en la disposición final • Copia no controlada **SOFTWARE Y EQUIPOS DE COMUNICACIONES** • Falta o insuficiencia de la prueba del software • Defectos bien conocidos en el software

FACTORES INTERNOS (VULNERABILIDADES)	
TIPO	**DESCRIPCIÓN**
	• Falta de "terminación de la sesión" cuando se abandona la estación de trabajo • Disposición o reutilización de los medios de almacenamiento sin borrado adecuado • Falta de pruebas de auditoría • Distribución errada de los derechos de acceso • Software de distribución amplia • Utilización de los programas de aplicación a los datos errados en términos de tiempo • Interfaz de usuario complicada • Falta de documentación • Configuración incorrecta de parámetros • Fechas incorrectas • Falta de mecanismos de identificación y autentificación, como la autentificación de usuario • Tablas de contraseñas sin protección • Gestión deficiente de las contraseñas • Habilitación de servicios innecesarios • Software nuevo o inmaduro • Especificaciones incompletas o no claras para los desarrolladores • Falta de control eficaz del cambio • Descarga y uso no controlados de software • Falta de copias de respaldo • Falta de protección física de las puertas y ventanas de la edificación • Falla en la producción de informes de gestión

FACTORES EXTERNOS (AMENAZAS)	
TIPO	**DESCRIPCIÓN**
Daño físico	• Fuego • Agua • Contaminación • Accidente Importante • Destrucción del equipo o medios • Polvo, corrosión, congelamiento • Fallas en el sistema de suministro de agua o aire acondicionado.

FACTORES EXTERNOS (AMENAZAS)	
TIPO	**DESCRIPCIÓN**
	• Perdida de suministro de energía. • Falla en equipo de telecomunicaciones
Medio Ambiente	• Fenómenos climáticos • Fenómenos sísmicos • Fenómenos volcánicos • Fenómenos meteorológicos • Inundación
Tecnológicos	**PERTURBACIÓN DEBIDA A LA RADIACIÓN** • Radiación electromagnética • Radiación térmica • Impulsos electromagnéticos **FALLAS TÉCNICAS** • Fallas del equipo • Mal funcionamiento del equipo • Saturación del sistema de información • Mal funcionamiento del software • Incumplimiento en el mantenimiento del sistema de información. **ACCIONES NO AUTORIZADAS** • Uso no autorizado del equipo • Copia fraudulenta del software • Uso de software falso o copiado • Corrupción de los datos • Procesamiento ilegal de dato
Compromiso de la información	• Interceptación de señales de interferencia comprometida • Espionaje remoto • Escucha encubierta • Hurto de medios o documentos • Hurto de equipo • Recuperación de medios reciclados o desechados • Divulgación • Datos provenientes de fuentes no confiables • Manipulación con hardware

FACTORES EXTERNOS (AMENAZAS)	
TIPO	**DESCRIPCIÓN**
	• Manipulación con software • Detección de la posición
Amenazas humanas	• Pirata informático, intruso ilegal • Criminal de la computación • Terrorismo • Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses) • Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos) • Error en el uso de funciones • Abuso de derechos • Falsificación de derechos • Negación de acciones • Incumplimiento en la disponibilidad del personal • No se alinean con las políticas y objetivos de la Entidad

Cada proceso es responsable del análisis del contexto estratégico partiendo para la identificación del análisis de los factores internos y externos que pueden afectar el cumplimiento del objetivo del proceso.

Se constituye en un insumo a partir del cual cada proceso identifica las causas generadoras de riesgos sobre las cuales de acuerdo con su naturaleza y alcance debe desarrollar acciones eficaces para su prevención y/o tratamiento.

Cada proceso debe, además, complementar el ejercicio identificando causas relevantes en el contexto interno y externo generadoras de riesgos para el cumplimiento del objetivo del proceso.

Para la **seguridad digital**, además de los ya lo mencionados, debe tenerse en cuenta el inventario de los activos de información.

La descripción del contexto estratégico se diligencia en la herramienta establecida por la Entidad.

8.1.2. Identificación de cada riesgo

En el marco resultante del análisis del contexto estratégico, se identifican los riesgos, entendiendo que es una actividad interactiva e integrada a la planeación

institucional, alineada con los objetivos estratégicos de la ARN y los objetivos de cada proceso. Si eventos de salud y seguridad en el trabajo o ambientales presentan probabilidad de impactar sobre los objetivos institucionales o del proceso, se debe(n) identificar el (los) riesgo(s) respectivo(s).

- Para los riesgos de gestión y corrupción

Para identificar un riesgo es clave preguntarse: ***¿Qué puede suceder?, ¿Cómo puede suceder?, ¿existe información sensible involucrada como datos personales?*** el ejercicio de identificación de riesgos en los procesos queda registrado en una herramienta en la que se registren las causas, los riesgos, su descripción, su clasificación y las consecuencias en caso de presentarse su materialización, como se define a continuación:

- **Causas:** Son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores de riesgo se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.

- **Riesgos:** A partir de las causas se identifican los riesgos, los cuales se nombran de manera negativa a un posible incumplimiento normativo, legal, funciones, o el evento que pudiese suceder.

  Para su identificación se deben traer las causas relacionadas en el contexto estratégico elaborado para cada proceso, teniendo en consideración que para un mismo riesgo se pueden asociar varias causas generadoras. Los riesgos identificados se registran en la herramienta establecida por la Entidad.

- **Descripción del Riesgo:** En este campo se debe describir las características generales o las formas en que se observa o manifiesta el riesgo identificado. (Aplica también para los riesgos de seguridad digital).

- **Clasificación del Riesgo:** Los riesgos identificados son clasificados, con el fin de establecer con mayor facilidad el análisis de impacto.

Clasificación del Riesgo

Estratégico	El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la Entidad por parte de la Alta Dirección.

Imagen	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
Operativos	Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la Entidad y de la articulación entre dependencias.
Financieros	Se relacionan con el manejo de los recursos de la Entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
Cumplimiento	Se asocian con la capacidad de la Entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
Tecnología	Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales, futuras y el cumplimiento de la misión.
Corrupción	Es la posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de la Entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- **Consecuencias:** En este campo se definen los posibles efectos ocasionados por el riesgo, generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

- Para los riesgos de seguridad digital

Para realizar la identificación de estos riesgos se debe tener en cuenta la “Matriz de activos de información de la Entidad”, que se encuentra en el link https://bit.ly/35fpK1j.

- **Clasificación del Riesgo:** Los riesgos identificados de seguridad digital clasificados en una categoría especial, a saber:

Seguridad Digital	Posibilidad que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se puede expresar como la función entre causas externas (amenazas) y causas internas (vulnerabilidades). Se puede describir en términos de pérdida o degradación de alguna de las tres

	características básicas: confidencialidad, integridad y disponibilidad.

8.2. VALORACIÓN DEL RIESGO

La valoración del riesgo busca confrontar el riesgo inicial (riesgo inherente), con el resultado de riesgo final (riesgo residual), después de aplicar los controles establecidos. Para ello, se realiza el análisis del riesgo, aplicando la pauta de valoración del mismo, como se indica a continuación.

8.2.1. Análisis del riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia del mismo y sus consecuencias (impacto), este último aspecto puede orientar la clasificación del riesgo, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. Para realizar un adecuado análisis de riesgos se debe tener en cuenta:

- Calificación de la probabilidad: Es la posibilidad de ocurrencia del riesgo. Puede ser medida con criterios de frecuencia, si se ha materializado, o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

- Calificación del impacto: Es el cálculo de la magnitud de las consecuencias de la materialización del riesgo.

8.2.2. Valoración de cada riesgo

Calificación de la probabilidad: La calificación de la probabilidad refleja la posibilidad de ocurrencia del riesgo, para ello se asigna una calificación de conformidad con la siguiente tabla:

Nivel	Descriptor	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado el evento en los últimos cinco años
2	Improbable	El evento puede ocurrir en algún momento	Al menos una vez, el evento ocurrió en los últimos cinco años

Nivel	Descriptor	Descripción	Frecuencia
3	Posible	El evento podría ocurrir en algún momento	Al menos una vez, el evento ocurrió en los últimos dos años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos una vez, el evento ocurrió en el último año
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez, el evento ocurrió al año

Calificación del impacto: La calificación del impacto del riesgo objeto de análisis, se realiza mediante la aplicación de los siguientes criterios:

a) Para los riesgos de gestión:

Se puede valorar el impacto en los cinco niveles descritos de la siguiente tabla:

Nivel	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la Entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la Entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la Entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la Entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la Entidad.

Para obtener una mayor precisión en la en la valoración del impacto para los riesgos de gestión del proceso, se puede tener en cuenta las tablas[1], que representan los impactos de mayor ocurrencia en las entidades del Estado.

[1] Tablas referidas por el Departamento Administrativo de la Función Pública-DAFP en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas*

Criterios para calificar el impacto – riesgos de gestión

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor≥50%. - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la Entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
MODERADO	- Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la Entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la Entidad.	- No hay interrupción de las operaciones de la Entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 4. 2018 / Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.*

b) Para los riesgos de seguridad digital

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	– Afectación ≥X% de la población – Afectación ≥X% del presupuesto anual de la Entidad. – Afectación muy grave del medio ambiente que requiere de ≥X años de recuperación.	– Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros. – Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. – Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	– Afectación ≥X% de la población. – Afectación ≥X% del presupuesto anual de la Entidad. – Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	– Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. – Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. – Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MODERADO	– Afectación ≥X% de la población. – Afectación ≥X% del presupuesto anual de la Entidad. – Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	– Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. – Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. – Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
MENOR	– Afectación ≥X% de la población. – Afectación ≥X% del presupuesto anual de la Entidad. – Afectación leve del medio ambiente requiere de ≥X días de recuperación.	– Afectación leve de la integridad. – Afectación leve de la disponibilidad. – Afectación leve de la confidencialidad.
INSIGNIFICANTE	– Afectación ≥X% de la población. – Afectación ≥X% del presupuesto anual de la Entidad. – No hay afectación medioambiental.	– Sin afectación de la integridad. – Sin afectación de la disponibilidad. – Sin afectación de la confidencialidad.

Fuente: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 4. 2018 / Elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones. 2017.*

Nota: Los porcentajes de impacto para los riegos digitales se establecen en relación con la afectación que tengan para el logro de los objetivos institucionales.

En concordancia con los lineamientos trazados por el Ministerio de Tecnologías de la Información y las Comunicaciones, las variables de confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la Estrategia de Gobierno Digital.

La variable población se define teniendo en cuenta el establecimiento del contexto externo de la Entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados.

La variable presupuestal es la consideración de presupuesto de la Entidad afectado por la materialización del riesgo y contempla sanciones económicas o impactos directos en la ejecución presupuestal.

La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.

c) Para los riesgos de corrupción

Contestar la siguiente serie de preguntas por cada riesgo de corrupción identificado, registrando con una X si la respuesta es SÍ o NO para su posterior conteo.

CUESTIONARIO DE PREGUNTAS

No.	Si el riesgo de corrupción se materializa podría…	Respuesta	
		SÍ	NO
1	¿Afectar al grupo de servidores 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 del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza en la entidad, afectando su reputación?		
6	¿Generación pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de los servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicio o de 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: *Guía para la administración del riesgo y el diseño de controles en entidades públicas, Bogotá, Departamento Administrativo de la Función Pública. Versión 4. 2018*

Una vez finalizado el registro del cuestionario se hace el conteo para saber la cantidad de respuestas para SÍ y para NO.

La siguiente tabla muestra en nivel en que quedaría el impacto para los riesgos de corrupción:

Valoración de impacto para los riesgos de corrupción
Respuesta afirmativa de UNO a CINCO preguntas genera impacto Moderado
Respuesta afirmativa de SEIS a ONCE preguntas genera impacto Mayor
Respuesta afirmativa de DOCE a DIECINUEVE preguntas genera impacto Catastrófico

Nota: La política de riesgos de la ARN establece intolerancia total frente a los riesgos de corrupción. Todo riesgo de corrupción será considerado como riesgo extremo.

8.2.3. Evaluación del riesgo

Una vez calificada la probabilidad y el impacto del riesgo objeto de análisis, se realiza el cruce de acuerdo con la *Matriz de Calificación, Evaluación y Respuesta a los Riesgos*, la cual permite determinar la calificación y zona de riesgo, esta matriz contiene un análisis cualitativo, que muestra la magnitud de las consecuencias (impacto) y la posibilidad de ocurrencia (probabilidad).

El resultado de la evaluación del riesgo se hace de manera automática una vez calificadas la probabilidad y el impacto y quedan consignadas en la herramienta del sistema administrador SIGER de la entidad, para este fin.

Matriz de Calificación, Evaluación y Respuesta a los Riesgos

IMPACTO/ PROBABILIDAD	1 Insignificante	2 Menor	3 Moderado	4 Mayor	5 Catastrófico
(1) Raro	1 (B)	2 (B)	3 (B)	4 (B)	5(B)
(2) Improbable	2 (B)	4 (B)	6(B)	8 (B)	10 (M)
(3) Posible	3 (B)	6 (B)	9 (M)	12 (M)	15 (A)
(4) Probable	4 (B)	8 (B)	12 (M)	16 (A)	20 (E)
(5) Casi Seguro	5 (B)	10 (M)	15 (A)	20 (E)	25 (E)

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo Moderada: Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo Alta: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo Extrema: Reducir el riesgo, Evitar, Compartir o Transferir

8.2.4. Valoración de los controles

Establecida la evaluación del riesgo, se diseñan los controles lo cual implica:

- Describirlos (estableciendo si son preventivos o correctivos).

- Revisarlos para determinar si los controles están documentados, si se están aplicando en la actualidad y si han sido efectivos para minimizar el riesgo.

- La valoración de los controles debe incluir un análisis de tipo cuantitativo, que permita saber con exactitud cuántos valores pueden ser descontados de su calificación inicial, a fin de disminuir el nivel de riesgo al que está expuesto el proceso analizado y así determinar las acciones a implementar.

- Las acciones de control sobre los riesgos actúan sobre la probabilidad de ocurrencia del mismo o sobre el impacto que generan al materializarse. Por lo tanto, para la evaluación de los controles existentes se debe tener en cuenta:

  - Evaluar el control por **probabilidad**, teniendo en cuenta que el control que se está analizando es preventivo y busca que el riesgo no se materialice.
  - Evaluar el control por **impacto**, teniendo en cuenta que el control que se está analizando busca restablecer a la situación normal.
  - *Preventivo*: Evita que un evento suceda. Ejemplo: *login* y *password* en un sistema de información previene (teóricamente) que personas no autorizadas puedan ingresar al mismo.
  - *Correctivo*: No prevé que un evento suceda, pero permiten enfrentar la situación una vez se ha presentado. Ej. Pólizas de seguro y otros mecanismos de recuperación de negocio o respaldo.

PARÁMETROS	CRITERIOS	PUNTAJES
Herramientas para ejercer el control	Posee una herramienta para ejercer el control.	15
	Existen manuales instructivos o procedimientos para el manejo de la herramienta	15

PARÁMETROS	CRITERIOS	PUNTAJES
	En el tiempo que lleva la herramienta ha demostrado ser efectiva.	30
Seguimiento al control	Están definidos los responsables de la ejecución del control y del seguimiento.	15
	La frecuencia de la ejecución del control y seguimiento es adecuada.	25
	TOTAL	100

Si el control afecta probabilidad o impacto se descontará un valor a la calificación inicial de la siguiente manera:		
Rangos de calificación de los controles	**Valor a disminuir en la probabilidad**	**Valor a disminuir en el impacto**
Entre 0-50	0	0
Entre 51-75	1	1
Entre 76-100	2	2

La valoración de los controles se efectúa siguiendo los criterios establecidos en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas*, del DAFP, y la aplicación de la herramienta SIGER.

El control debe tener definido el responsable de hacer la actividad, periodicidad específica, indicar cómo se realiza y fuente de información confiable, ser consistente para la mitigación del riesgo, indicar qué pasa con las observaciones o desviaciones como resultado de ejecutar el control y expresar cómo se evidencia su ejecución.

Ejemplos de la redacción de controles son los siguientes (Fuente: DAFP):

“El sistema SAP cada vez que se va a realizar un pago **[PERIOCIDAD]** valida que el proveedor al cual se le va a girar el pago no esté reportado en listas restrictivas, comparando el NIT o cédula con la información cargada **[CÓMO SE REALIZA]** en el aplicativo de las listas de clientes reportados en temas de lavado de activos **[FUENTE CONFIABLE]**. En caso de encontrar coincidencias el sistema no permite realizar el pago **[QUÉ PASA CON LAS OBSERVACIONES O DESVIACIONES]**. Como evidencia queda la programación interna del aplicativo y el reporte de coincidencia con listas restrictivas **[CÓMO SE EVIDENCIA SU EJECUCIÓN]**”.

"El profesional de contratación cada vez que se va a realizar un contrato **[PERIOCIDAD]** verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos de contratación **[CÓMO SE REALIZA]** a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física suministrada por el proveedor **[FUENTE DE LA INFORMACIÓN]**. En caso de encontrar información faltante, requiere al proveedor a través de correo para el suministro de la información y poder continuar con el proceso de contratación **[QUÉ PASA CON LAS OBSERVACIONES O DESVIACIONES]**. Como evidencia deja lista de chequeo diligenciada con la información de la carpeta del cliente y correos electrónicos solicitando la información faltante **[CÓMO SE EVIDENCIA SU EJECUCIÓN]**".

8.3. TRATAMIENTO DEL RIESGO

Los elementos de control son los que permiten estructurar los criterios orientadores en la toma de decisiones respecto al tratamiento de los riesgos y sus efectos.

De conformidad con los resultados obtenidos en la evaluación del riesgo después de haber evaluado los controles existentes, se define la opción de manejo del riesgo de acuerdo con la zona de riesgo donde éste se encuentre ubicado, así:

ZONA DE RIESGO	OPCIÓN DE MANEJO
B: Zona de riesgo Baja	Asumir el riesgo
M: Zona de riesgo Moderada	Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo Alta	Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo Extrema	Reducir el riesgo, Evitar, Compartir o Transferir

Las políticas identifican las acciones para tratar y manejar los riesgos, permitiendo tomar las decisiones adecuadas acerca de si se acepta, se evita, se comparte o se transfiere legalmente el impacto en cada uno de los riesgos identificados que al materializarse puede obstaculizar el cumplimiento de los objetivos institucionales y de los objetivos de los procesos.

8.3.1. Características de manejo de riesgos

- **Evitar el riesgo**: Tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior del proceso se generan cambios sustanciales por

mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico.

- **Reducir el riesgo**: Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección).

  La reducción del riesgo es probablemente el método sencillo y económico para superar las medidas más costosas y difíciles. Por ejemplo, a través de la optimización de los procesos y la implementación de controles.

- **Compartir o Transferir el riesgo:** Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.

- **Asumir el riesgo**: Cuando el riesgo queda en zona de riesgo “Baja” o “Moderada” el responsable del riesgo puede aceptar las posibles consecuencias, si éstas no afectan el logro de los objetivos del proceso y elabora planes de contingencia para su manejo.

Dicha selección implica equilibrar los costos y los esfuerzos para su implementación, así como los beneficios finales, por lo tanto, se deben considerar aspectos como: viabilidad jurídica, viabilidad técnica, viabilidad institucional, viabilidad financiera o económica y análisis de costo-beneficio.

En la herramienta establecida por la entidad se debe seleccionar la opción de manejo del riesgo.

8.3.2. Acciones

De acuerdo con la opción de manejo del riesgo definida a partir de la calificación del mismo, la entidad debe establecer de manera concreta que acciones o actividades debe desarrollar para el manejo de los riesgos, orientadas a evitar, reducir, compartir o asumir el riesgo.

Las acciones definidas deben ser realizables y efectivas en el tratamiento del riesgo, para ello, se debe considerar la viabilidad jurídica, técnica, institucional,

financiera y económica (balance costo-beneficio). Algunas de las acciones podrían ser: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos, cambios físicos, entre otros.

Las acciones definidas deben estar relacionadas con los controles descritos de manera que al evaluarlas se pueda determinar si estos están siendo adecuados para mitigar el riesgo, por su eficacia y efectividad.

Las acciones definidas se deben registrar en la herramienta establecida por la entidad y las evidencias de los resultados finales se deben guardar de acuerdo con lo definido en el Manual de Seguimiento de la Planeación y Gestión Institucional.

8.4. INDICADORES Y MONITOREO

Una vez diseñado y validado el mapa de riesgos es necesario monitorearlo, teniendo en cuenta que estos nunca dejan de representar amenazas para el cumplimiento de los objetivos estratégicos o de los procesos.

Se debe asegurar que las acciones establecidas en los mapas de riesgos se están llevando a cabo y evaluar la eficacia y efectividad en su implementación, adelantando revisiones para evidenciar todas aquellas situaciones o factores que pueden influir en la aplicación de las acciones para el manejo de los riesgos.

Cada proceso es responsable de evaluar y revisar periódicamente las acciones tomadas, verificando su eficacia con los controles establecidos y los resultados de las acciones tomadas, así como su eficacia y efectividad.

Para la medición de la eficacia y la efectividad de las actividades de control, en concordancia con la *Guía para la administración del riesgo y el diseño de controles en entidades públicas*, del Departamento Administrativo de la Función Pública-DAFP, la ARN establecerá uno o máximo dos indicadores claves de riesgo para cada proceso.

El registro del seguimiento se realiza a través del módulo de riesgos del software administrador del SIGER, el cual trimestralmente lanzará una tarea por cada riesgo identificado y se registra el avance de la acción propuesta, o el cierre de la acción el comportamiento del riesgo en: seguimiento a los controles, estado actual de los avances registrados por los responsables de las acciones, si el riesgo se materializó, describir que acciones se realizarán para el plan de contingencia con la definición del tiempo de cada una de ellas.

El Grupo de Control Interno de Gestión, en desarrollo de su función de seguimiento evaluará la eficacia, eficiencia y efectividad de las acciones establecidas, a través del software administrador del SIGER y comunicará a cada responsable de acción las recomendaciones y propuestas de mejoramiento y tratamiento a las situaciones detectadas.

El asesor del Grupo de Control Interno de Gestión presentará al Comité Institucional de Coordinación de Control Interno con una periodicidad de seis meses un informe de los resultados del seguimiento a la gestión del riesgo en la entidad y las recomendaciones de mejoramiento.

Así mismo, presentará informe cuatrimestral a la evaluación de los riesgos de corrupción.

8.5. DESVIACIONES

El no cumplimiento de la política institucional de gestión del riesgo, de las directrices de la Alta Dirección al respecto, de los controles o de las acciones establecidas constituyen desviaciones.

Las desviaciones menores son normalmente tratadas por correcciones que se toman para corregir y contener el problema (incluyendo acciones inmediatas), basadas en suficiente evidencia documentada.

Las desviaciones mayores o críticas se tratan primero por las correcciones, a continuación, se debe realizar una identificación sobre las causas raíz de la desviación y se establecerán las correspondientes acciones correctivas, que requieren la aprobación del Grupo de Control Interno de Gestión.

8.6. ACCIONES ANTE RIESGOS MATERIALIZADOS

En caso de la materialización de un riesgo, se deberá actuar de la siguiente manera:

Tipo de riesgo	Identificador del riesgo materializado	Actividad
Riesgo de corrupción	Dependencia o Proceso	• Informar a la Dirección General, a la Oficina Asesora Jurídica y al Grupo de Control Interno de Gestión sobre el hecho encontrado.

		• Identificar las acciones correctivas necesarias y formular plan de mejoramiento, el cual debe ser registrado en el módulo correspondiente del software SIGER. • Efectuar el análisis de causas, redefinir el control y determinar acciones de tratamiento, con aprobación del líder del proceso. • Solicitar a la Oficina Asesora de Planeación la actualización del mapa de riesgos.
	Grupo de Control Interno de Gestión	• Informar a la Oficina Asesora Jurídica para establecer las acciones a que haya lugar. • Informar al líder del proceso, para identificar las acciones correctivas necesarias y formular plan de mejoramiento, que debe ser registrado en el módulo correspondiente del SIGER. • Realizar la denuncia ante la instancia de control correspondiente, una vez establecido el alcance del evento materializado, a partir de la normatividad asociada al hecho. • Informar a la Oficina Asesora de Planeación, con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.
Riesgos de seguridad digital	Dependencia o Proceso	• Informar la materialización del riesgo al respectivo líder de proceso, por parte del servidor público o colaborador de la Entidad al que se le ha asignado la responsabilidad sobre un activo de información, en concordancia con el Manual del Sistema de Gestión de Seguridad de la Información (código TI-M-01).

		•Informar de sucedido a la Oficina de Tecnologías de la Información, a través de correo electrónico del líder del proceso, para que el responsable de seguridad informática del Grupo de Infraestructura y Soporte proceda a aplicar el tratamiento que requiere el incidente de seguridad digital. •Informar de inmediato el evento a la Dirección General, al Asesor de Estrategia y Seguridad y al Grupo de Control Interno de Gestión, mediante correo de la Jefatura de la Oficina de Tecnologías de la Información y/o del responsable de seguridad informática del Grupo de Infraestructura y Soporte. •Realizar una Mesa de Seguridad, con la participación del propietario del activo de información, el líder de su proceso o jefe de dependencia, el Asesor de Estrategia y Seguridad o la persona que delegue y la jefatura de la Oficina de Tecnologías de Información o la persona que delegue, para determinar las causas del evento y garantizar la continuidad del servicio o el restablecimiento del mismo. • Redefinir el control, determinar acciones de tratamiento y formular plan de mejoramiento por parte del líder del proceso en que se presentó el hecho, con apoyo de la Oficina de Tecnologías de la Información. •Registrar en el módulo correspondiente del SIGER el plan de mejoramiento, con aprobación del Asesor del Grupo de Control Interno de Gestión. •Solicitar a la Oficina Asesora de Planeación la actualización del mapa de riesgos.

	Grupo de Control Interno de Gestión	•Informar de inmediato, mediante correo electrónico, el evento hallado a la Dirección General, al Asesor de Estrategia y Seguridad, a la Jefatura de la Oficina de Tecnologías de la Información y al responsable de seguridad informática del Grupo de Infraestructura y Soporte. •Realizar una Mesa de Seguridad, con la participación del propietario del activo de información, del Asesor del Grupo de Control Interno de Gestión o la persona que delegue, el líder del proceso o jefe de dependencia en que se presentó el hecho, el propietario del activo de información, el Asesor de Estrategia y Seguridad o la persona que delegue y la jefe de la Oficina de Tecnologías de Información o la persona que delegue, para determinar las causas del evento y garantizar la continuidad del servicio o el restablecimiento del mismo. •Solicitar, mediante correo electrónico del Asesor del Grupo de Control Interno de Gestión al líder del proceso y/o jefe de dependencia en que se presentó la materialización del riesgo, replantear el control, redefinir acciones de tratamiento, formular plan de mejoramiento, someterlo a visto bueno de la Jefatura de la Oficina de Tecnologías de la Información y solicitar a la Oficina Asesora de Planeación la actualización del mapa de riesgos, dentro de los tres días hábiles siguientes a la fecha del evento. •Verificar que el líder del proceso o jefe de dependencia en que se presentó la materialización del riesgo formuló el plan de mejoramiento para registrar en el SIGER y solicitó a la Oficina Asesora de Planeación

		la actualización del mapa de riesgos correspondiente.
Riesgos de gestión	Dependencia o Proceso	•Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo, y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos. •Informar a la Oficina Asesora de Planeación, para actualizar el mapa de riesgos.
	Grupo de Control Interno de Gestión	•Informar al líder del proceso sobre el hecho encontrado. •Informar a la Oficina Asesora de Planeación, con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos •Acompañar al líder del proceso en la revisión, análisis y ajuste de controles y/o acciones correspondientes para resolver el hecho. •Verificar que se realizó la revisión, análisis y ajuste correspondiente y se actualizó el mapa de riesgos correspondiente.

9. DOCUMENTOS DE REFERENCIA

• *CONPES 3854 de 2016/Política Nacional de Seguridad Digital*, Ministerio de Tecnologías de la Información y las Comunicaciones-Ministerio de Defensa Nacional-Dirección Nacional de Inteligencia-Departamento Nacional de Planeación, versión aprobada en abril de 2016.

- *Guía para la administración del riesgo y el diseño de controles en entidades públicas*, Bogotá, Departamento Administrativo de la Función Pública, versión 4, 2018.
- *Guía para las normas de control interno del sector público/INTOSAI GOV 9100*, aprobada en 2004 por el XVIII Congreso de la Organización Internacional de las Entidades Fiscalizadoras Superiores-INTOSAI.

- *Manual del Sistema de Gestión de Seguridad de la Información,* de la Agencia para la Reincorporación y la Normalización, código TI-M-01.

- *Manual de Seguimiento a la Planeación y Gestión Institucional*, de la Agencia para la Reincorporación y la Normalización, código DE-M-03.

- *Norma Técnica Colombiana NTC/ISO 31000:2011 Gestión del Riesgo* – Principios y Directrices. Instituto Colombiano de Normas Técnicas y Certificación-ICONTEC.

- *Norma Técnica Colombiana NTC/ISO-IEC 27000:2017 Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de seguridad digital (SGSI). Visión general y vocabulario*, Instituto Colombiano de Normas Técnicas y Certificación-ICONTEC.