TABLA DE CONTENIDO

INTRODUCCIÓN

La planeación con un enfoque basado en la gestión de riesgos se fundamenta en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que la entidad gestione acciones que reduzcan la probabilidad de ocurrencia y mitiguen el impacto negativo de la materialización de sus riesgos, a partir del análisis de su contexto interno, externo y de procesos, para el logro de sus objetivos y metas institucionales.

La adopción y aplicación de una política de riesgos, así como la definición de un marco de referencia y el desarrollo de un proceso consistente y sistemático, permite que la gestión del riesgo sea un ejercicio que establezca una base confiable para la toma de decisiones, aumente la probabilidad de alcanzar los objetivos planificados, prevenga actos de corrupción, y mejore la eficacia y la eficiencia operativa de los procesos a través de la minimización o prevención de pérdidas y gestión de incidentes.

A partir de este enfoque, la presente guía contiene la metodología establecida por la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología - ATENEA para la gestión integral de riesgos de: gestión, fiscales, seguridad digital e integridad pública, específicamente en su tipología de **corrupción**; de tal forma que sus colaboradores cuenten con los elementos que orienten el entendimiento de la gestión de riesgos en la entidad.

La aplicación de esta guía a todos los procesos de la entidad busca desarrollar la identificación, análisis, evaluación, tratamiento y monitoreo de riesgos con objetividad y precisión para el cumplimiento de los objetivos trazados por la entidad en su misión.

1. OBJETIVO

Establecer directrices metodológicas para gestionar de forma integral los riesgos de gestión, fiscales, seguridad digital e integridad pública corrupción, a los que se encuentra expuesta la Agencia en el desarrollo de su operación, reduciendo la probabilidad de ocurrencia y mitigando el impacto en la materialización de situaciones que pueden afectar negativamente la gestión institucional.

2. ALCANCE

La presente guía aplica para la gestión de todos los riesgos identificados en los procesos, a los que la entidad podría estar expuesta. Esta guía presenta la información requerida para la gestión integral de los riesgos de gestión, fiscal, seguridad digital e integridad pública - corrupción.

3. DEFINICIONES

Activo: en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Amenaza: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27001:2022).

Apetito de Riesgo: es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Bien Público: son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales.

Bien de Uso Público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques entre otros.

Bienes Fiscales: aquellos que están destinados al cumplimiento de las funciones o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

Causa: todos aquellos factores internos, externos y de procesos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa Inmediata: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

Causa Raíz (General): causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Causa Adecuada / Causa Eficiente (Riesgo Fiscal): evento (acción u omisión) que, de ocurrir, genera directamente el efecto dañoso sobre bienes, recursos o intereses patrimoniales de naturaleza pública; es condición necesaria para que el daño se produzca.

Confidencialidad: propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Conflicto de Interés: se presenta cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público. El interés del servidor público se presenta cuando debe decidir sobre asuntos en los que tiene un interés particular y directo en su

regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. (A partir de la Ley 1952 de 2019, art. 44, Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011).

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad y demás partes interesadas y grupos de valor.

Continuidad de Negocio: plan logístico para recuperar, restaurar los procesos misionales, críticos, parcial o totalmente interrumpidos por un riesgo materializado.

Contraparte: cualquier persona o entidad que tenga un interés propio o particular, diferente al interés de la organización.

Control: medida que permite reducir o mitigar un riesgo.

Controles Automáticos: son los que utilizan herramientas tecnológicas como sistemas de información o software que permiten incluir contraseñas de acceso, o controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros. Este tipo de controles suelen ser más efectivos en algunos ámbitos dada su complejidad.

Controles Correctivos: aquellos que permiten, después de ser detectado el evento no deseado, el restablecimiento de la actividad.

Controles Detectivos: aquellos que registran un evento después de presentado; sirven para descubrir resultados no previstos y alertar sobre la presencia de un riesgo.

Controles Manuales: políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros.

Controles Preventivos: aquellos que permiten eliminar la(s) causa(s) del riesgo, para prevenir su ocurrencia o materialización.

Corrupción: todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen: (i) El uso del poder para obtener beneficios personales, (ii) Pérdida o disminución del patrimonio público, (iii) El perjuicio social significativo, y (iv) La corrupción electoral. (A partir del artículo 2.1.4.3.1.3 del Decreto 1081 de 2015).

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.
Evento Potencial: hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos, los bienes y/o los intereses patrimoniales de naturaleza pública

Factores de Riesgo: son las fuentes generadoras de riesgos.

Fraude: errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Puede ser interno, en cuyo caso el fraude involucra a colaboradores, o externo, cuando se realiza por terceros, externos y la organización es la víctima (a partir de ISO37001:2025).

Gestión del Riesgo: enfoque estructurado que abarca desde la identificación de los riesgos, análisis de probabilidades e impactos, definición de controles, de planes de tratamiento, seguimiento y control por parte de cada uno de los niveles, nacional, regional y zonal, a través de los líderes de procesos, así como de cada colaborador de la Agencia para garantizar el logro de los objetivos misionales.

Gestión del Riesgo Fiscal: son las actividades que debe desarrollar cada entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

Gestor Público: es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales. Además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

Gestor Fiscal: son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique)". Entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: propiedad de exactitud y completitud.

Intereses Patrimoniales de Naturaleza Pública: son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas. Son algunos ejemplos de intereses patrimoniales de naturaleza pública, la rentabilidad proyectada de cualquier inversión pública, es decir antes de que se causen o generen efectivamente; la cobertura de garantías y pólizas; la participación accionaria pública en una empresa de economía mixta o en una empresa de servicios públicos con socio o socios públicos; los rendimientos financieros y frutos de recursos públicos cuando se proyectan, es decir antes de que se causen o generen efectivamente; así como, los intereses moratorios, indexaciones, actualización del dinero en el tiempo, estimación de pérdida de costo de oportunidad, cuando se trata de cobrar recursos públicos que un tercero debe; explotación de bienes públicos y/o recaudo de recursos públicos por un particular sin contrato o habilitación legal.

Mapa de Riesgos: es una representación gráfica o esquemática de la probabilidad e impacto de uno o más riesgos de un proceso, proyecto o programa. También se conoce con la denominación de mapa de calor ya que representa por cada zona la cantidad de riesgos en cada nivel (bajo, moderado, alto o extremo).

Matriz de Riesgos: documento donde se registra la identificación, análisis, evaluación y tratamiento de los riesgos por proceso.

Nivel de Riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo puede ser igual a probabilidad * impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de probabilidad – impacto.

Patrimonio Público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C-340-07).

Prevención: toda acción tendiente a evitar la generación de nuevos riesgos.

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en un periodo de tiempo.

Punto de Riesgo: actividades en las que potencialmente se genera riesgo. Tratándose de riesgos fiscales los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública.

Nota: para la identificación y priorización de los puntos de riesgo fiscal, la entidad deberá considerar las actividades frente a las cuales se hayan presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como aquellas que, por su naturaleza, puedan generar riesgos fiscales. Para apoyar este ejercicio, consulte en este documento la Tabla 2. Puntos de riesgo fiscal (Fuente: Anexo 3, capítulo "Identificación y valoración de riesgos fiscales y diseño de controles para su prevención y mitigación", Guía para la gestión integral del riesgo en entidades públicas, DAFP).

Recurso Público: para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

Riesgo: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgo Fiscal: es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

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.

Riesgos para la Integridad: toda actuación o decisión de las y los servidores públicos, así como de otros colaboradores de las entidades públicas que privilegien el interés particular sobre el general, asociadas a conductas no deseadas que van en contravía de los valores del servicio público. Incluido, también, el riesgo de que la integridad de la entidad sea utilizada para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas

Riesgo de Seguridad de la Información: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000).

Riesgo Inherente: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo Residual: el resultado de aplicar la efectividad de los controles al riesgo inherente.

Riesgos de Tecnología: posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.

Sistema de Gestión de Riesgos para la Integridad Pública -SIGRIP: esquema que define la interrelación e interacción de diferentes elementos para asegurar una gestión integral de los riesgos que afectan la integridad pública. El SIGRIP se articula con la Política para la Gestión Integral de Riesgos.

Soborno: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar (a partir de ISO37001:2025).
Soborno Entrante: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida a un servidor de la entidad.

Soborno Saliente: ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida por parte de servidores públicos a otros en nombre de la entidad.

Tolerancia al Riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes.

Valoración del Riesgo: consiste en emitir un juicio sobre la tolerancia o no del riesgo estimado. Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final.

Vulnerabilidad: debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27001:2022).

SIGLAS

- **DAFP:** Departamento Administrativo de la Función Pública
- **MIPG:** Modelo Integrado de Planeación y gestión
- **MECI:** Modelo Estándar de Control Interno
- **KRI:** Indicador Clave de Riesgo (Key Risk Indicator)
- **KPI:** Indicador Clave de Desempeño (Key Performance Indicator)
- **ISO:** Organización Internacional de Normalización (International Organization for Standardization)
- **ISO/IEC:** Organización Internacional de Normalización / Comisión Electrotécnica Internacional
- **TIC:** Tecnologías de la Información y las Comunicaciones

4. NORMATIVIDAD ASOCIADA

Tabla 1. Referentes normativos y documentales

Tipo	Instrumento	Aporte para la guía
Guía técnica (referente metodológico)	Guía para la gestión integral del riesgo en entidades públicas (Versión 7)	Define el enfoque, etapas y criterios metodológicos para la gestión integral del riesgo en entidades públicas; se usa como

Tipo	Instrumento	Aporte para la guía
		base para la estructura y desarrollo de la presente guía.
Norma	Decreto Único Reglamentario del Sector Función Pública	Compila el marco reglamentario del Sector Función Pública, incluyendo disposiciones relacionadas con gestión y control en entidades públicas.
Norma	Decreto 1499 de 2017 (modifica el Decreto 1083 de 2015 en lo relacionado con el Sistema de Gestión – MIPG)	Referente normativo para el Sistema de Gestión y su articulación institucional (MIPG).
Norma	Decreto 648 de 2017 (modifica y adiciona el Decreto 1083 de 2015)	Ajusta disposiciones del Decreto 1083, incluyendo desarrollos asociados al esquema de control interno y gestión institucional.
Documento de política pública	CONPES 167 de 2013: Estrategia nacional de la política pública integral anticorrupción	Referente orientador de política pública anticorrupción.

Fuente: elaboración propia con base en las referencias normativas y documentales citadas en este apartado.

5. DESARROLLO

La gestión integral del riesgo en todos los procesos y niveles de la Agencia constituye un elemento estratégico para la planeación y para la gestión cotidiana, considerando los contextos externos, interno y de procesos que inciden en la naturaleza y operación de la entidad.

En concordancia con lo anterior, la metodología para la gestión integral de los riesgos de gestión, fiscales, seguridad digital e integridad pública – corrupción se estructura con base en la Guía para la gestión integral del riesgo en entidades públicas del Departamento Administrativo de la Función Pública (DAFP), en su versión vigente, adoptando sus lineamientos y orientaciones metodológicas como referente institucional.

5.1. Criterios Operativos

5.1.1. La gestión de riesgos de la entidad debe estar enfocada al cumplimiento de los objetivos institucionales y es estratégica dentro de la organización. Todos los riesgos que sean identificados deben estar enfocados a riesgos estratégicos de la entidad, es decir a aquellos relacionados con la misión y el cumplimiento de los objetivos estratégicos y de procesos.

5.1.2. La identificación de los riesgos de los procesos se realiza partiendo del análisis de contexto interno, externo y de procesos de la entidad. Los análisis del Contexto interno y externo de la entidad pueden ser consultados en el Documento Análisis de Contexto Estratégico Institucional y el Contexto de Procesos, este último se puede consultar en el Anexo No. 1 de esta guía.

5.1.3. La Subgerencia de Planeación establece directrices para la identificación, análisis, evaluación y tratamiento de los riesgos. También realiza monitoreo al cumplimiento de los compromisos frente a la gestión de riesgos, así como de la materialización de estos, la aplicación de sus

controles y el cumplimiento a los planes de tratamiento. La información de los riesgos relacionada con estas directrices queda registrada en el formato de matriz de riesgos.

5.1.4. El líder de cada proceso es el responsable de la gestión integral de los riesgos en la Agencia y deben desarrollar e implementar actividades de control a través de la identificación, análisis, evaluación, tratamiento y monitoreo de la gestión de riesgos de los procesos a su cargo.

5.1.5. El líder del Proceso será responsable de adelantar, al cierre de la vigencia y al interior de su proceso, mesas de trabajo con el equipo técnico para revisar la gestión de riesgos. Con base en los resultados de dicho ejercicio, deberá presentar a la Subgerencia de Planeación la proyección de la gestión de riesgos de su proceso para la siguiente vigencia, en cumplimiento de las directrices establecidas en la presente guía.

5.1.6. La aprobación de las matrices de riesgos de gestión, fiscal, seguridad digital, sus controles y planes de tratamiento se realiza mediante comunicación enviada por el líder de proceso al Subgerente de Planeación, y las matrices de riesgos de Integridad Pública - Corrupción deben ser presentadas para aprobación al Comité Institucional de Gestión y Desempeño.

5.1.7. Una vez las matrices de riesgos son aprobadas, cada líder de proceso debe iniciar el seguimiento y revisión de los controles establecidos y las acciones de sus planes de tratamiento para garantizar su cumplimiento con oportunidad y calidad. Así como realizar los reportes requeridos para el seguimiento de la gestión institucional.

5.1.8. Los líderes deben comunicar al interior del proceso correspondiente, los riesgos a su cargo, así como los planes de tratamiento adoptados para su mitigación.

5.1.9. La revisión general de los mapas de riesgos de gestión, fiscal, seguridad digital e integridad pública - corrupción de la entidad la debe hace el líder de Proceso una vez al año al finalizar la vigencia, No obstante, en el transcurso de la vigencia pueden presentarse modificaciones (identificación o modificación de riesgos, controles y planes de tratamiento) a la gestión de los riesgos siempre y cuando sean para su fortalecimiento. Dichas modificaciones deben ser aprobadas por el líder del proceso correspondiente y remitidas en el Formato Control de Cambios a la Gestión de Riesgos, para su validación por la Subgerencia de Planeación. Cuando el Líder de Proceso considere la eliminación de un riesgo de gestión o fiscal, debe presentar previamente la debida justificación a la Subgerencia de Planeación con el fin de realizar análisis conjunto frente a la procedencia de la eliminación del riesgo.

Para los riesgos de integridad pública – corrupción, toda modificación avalada por el líder del Proceso deberá ser presentada para aprobación del Comité Institucional de Gestión y Desempeño. Una vez aprobada, la versión oficial del Mapa de Riesgos de Corrupción deberá publicarse en el enlace de “Transparencia y acceso a la información” del sitio web institucional, a más tardar el 31 de enero de cada vigencia, conforme a los lineamientos aplicables.

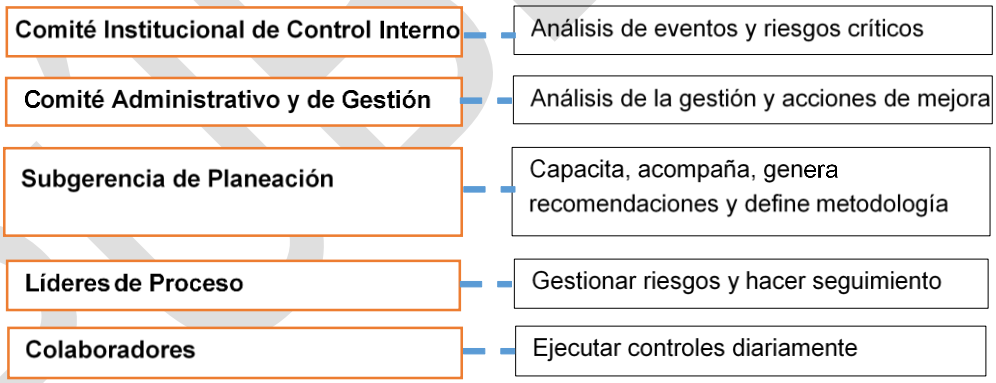
5.1.10. Las modificaciones de planes de tratamiento o de las fechas de cumplimiento de los planes de tratamiento para los riesgos Gestión, Fiscal, Seguridad Digital, durante la vigencia deberán realizarse a más tardar treinta (30) días calendario antes de la fecha de corte para monitoreo de la gestión de riesgos vía correo electrónico remitido por el líder del proceso, con la justificación correspondiente para validación y ajuste por la Subgerencia de Planeación, siempre y cuando las actividades no se encuentren vencidas.

5.1.11. Las modificaciones de planes de tratamiento o de las fechas de cumplimiento para los riesgos de Integridad pública - corrupción deben ser solicitadas por correo electrónico con la debida justificación y propuesta de ajuste dirigida a la Subgerencia de Planeación, máximo hasta el 30 de abril del respectivo año de vigencia del Plan. Estas modificaciones deben ser presentadas por el líder de Proceso para aprobación y revisión del Comité Institucional de Gestión y Desempeño.

5.1.12. Cuando haya lugar a la gestión de acciones de mejora por la materialización de riesgos, incumplimiento de los planes de tratamiento, o a partir de la calificación del diseño y ejecución de los controles, estas deben ser gestionadas a través de lo establecido en el procedimiento de gestión de acciones de mejora.

5.1.13. Responsabilidades en el marco del cumplimiento a las directrices establecidas por el Departamento Administrativo de la Función Pública, enfocadas en la administración de riesgos:

Figura 1. Responsabilidades en la gestión de riesgos

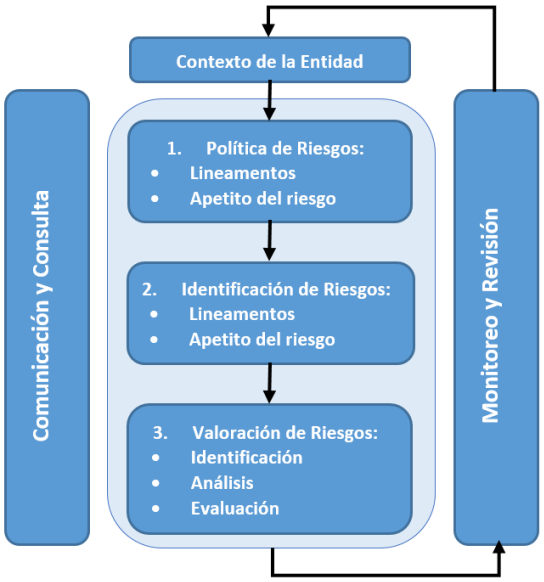


Fuente: adaptado de Guía para la gestión integral del riesgo en entidades públicas (Departamento Administrativo de la Función Pública).

5.2. Gestión Integral de Riesgos: Gestión, Fiscal, Seguridad Digital, Integridad Pública - Corrupción.

La gestión de riesgos de gestión, fiscal, seguridad digital e integridad pública - corrupción comprende las fases descritas en la siguiente figura:

Figura 2. Diagrama de gestión de riesgos



Fuente: elaboración propia con base en la *Guía para la gestión integral del riesgo en entidades públicas* (Departamento Administrativo de la Función Pública).

5.2.1. Contexto de la Entidad

El contexto en términos generales relaciona los aspectos que se deben tener en cuenta para gestionar los riesgos de acuerdo con el entorno externo e interno en el cual se desarrolla el proceso. Al identificar dichos aspectos, se tienen en cuenta las diferentes partes interesadas y grupos de valor para la Agencia, que pueden incidir en los cambios institucionales que se presentan en la entidad o que la impactan. A partir del contexto es posible establecer las causas de los riesgos a identificar. El contexto se aborda desde 3 frentes a partir de lo siguiente:

Contexto Externo: como su nombre lo indica, se busca identificar los factores externos significativos que tienen injerencia en la entidad y pueden llegar a ser una fortaleza o amenaza para el cumplimiento de los objetivos y metas. Se pueden considerar factores políticos, económicos, socioculturales, tecnológicos, medioambientales y legales.

Contexto Interno: corresponde al entorno en el cual se propone alcanzar unos objetivos y para poder lograrlo se analizan ciertos factores desde las oportunidades y debilidades que puede presentar la entidad. Se pueden considerar factores financieros y físicos; normativos y de procedimientos; de talento humano; sistemas tecnológicos; planeación y estrategia; y comunicación interna.

Contexto de Procesos: se determinan las características o aspectos esenciales de los procesos y sus interrelaciones. Se pueden considerar factores como: diseño del proceso, interacciones con otros procesos, transversalidad, procedimientos asociados, líderes del proceso y comunicación entre los procesos.

5.2.2. Identificación de Riesgos

Con esta etapa inicia la gestión integral de riesgos de la entidad (gestión, fiscal, seguridad digital e integridad pública - corrupción). Su objetivo es determinar los riesgos a los cuales está expuesta la entidad a partir de su análisis de contexto interno, externo y de procesos.

5.2.2.1. Identificación de Riesgos de Gestión, Fiscal, Seguridad Digital e Integridad Pública - Corrupción

Identificación de Áreas de Impacto

El área de impacto de un riesgo corresponde a la consecuencia a la cual se ve expuesta la entidad en caso de que este se materialice, esta puede ser económica (afectación o perdida de recursos económicos) o reputacional (afectación de la imagen y/o credibilidad Institucional.). A partir del área de impacto de un riesgo se puede establecer el impacto de su materialización.

Para los riesgos fiscales, el área de impacto siempre corresponderá con una consecuencia económica sobre el patrimonio público en caso de que se produzca su materialización. De otra parte, es importante aclarar que no todos los riesgos cuya materialización conlleve la afectación o pérdida económica corresponden a riesgos fiscales.

Identificación de Puntos de Riesgo

En el marco de la gestión de los procesos pueden ser identificadas actividades[1] cuya ejecución potencialmente puede generar la materialización de un riesgo. A partir de la identificación de puntos de riesgo se realiza la estimación de la probabilidad de un riesgo en la etapa de Análisis.

Para los riesgos fiscales, el DAPF a partir de un análisis adelantado con la participación de la Contraloría General de la República, identificó los siguientes puntos de riesgo fiscal:

Tabla 2. Puntos de riesgo fiscal.

Id Referencia	Puntos de riesgo fiscal actividad en la que potencialmente se origina el riesgo fiscal	Circunstancia inmediata situación por la que se presenta el riesgo
1	Cumplimiento de las normas y obligaciones ante autoridades	Pago de multas, cláusulas penales o cualquier tipo de sanción
2	Cumplimiento de obligaciones	Pago de Intereses moratorios
3	Desplazamientos de los funcionarios y de los contratistas a lugares diferentes al domicilio de la entidad.	Pago de viáticos, honorarios o gastos de desplazamiento sin justificación o por encima de los valores establecidos normativamente
4	Liquidación de impuestos	Mayor valor pagado por concepto de impuestos

[1] Los puntos de riesgo fiscal incluyen actividades de "administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas", de acuerdo con el Artículo 3 Ley 610 de 2000.

Id Referencia	Puntos de riesgo fiscal actividad en la que potencialmente se origina el riesgo fiscal	Circunstancia inmediata situación por la que se presenta el riesgo
5	Operaciones, actas o actos en los que se reconocen saldos a favor de la entidad	Saldos o recursos a favor no cobrados
6	Custodiar de los bienes muebles de la entidad	Pérdida, extravío, hurto, robo o declaratoria de bienes faltantes pertenecientes a la Entidad
7	Avalúos a bienes inmuebles de la entidad	Error en los avalúos, afectando el valor de venta y/o negociación de un bien público
8	Custodiar de los bienes muebles de la entidad	Daño en bienes muebles de propiedad de la entidad
9	Suscripción de contratos cuyo objeto es o incluye la representación judicial o extrajudicial de la entidad	Valor pagado por concepto de honorarios de apoderado cuando ocurre vencimiento de términos en los procesos judiciales o cualquier otra omisión del apoderado
10	Pago de sentencias y conciliaciones	Intereses moratorios por pago tardío de sentencias y conciliaciones
11	Instrucción del Comité de Conciliación para iniciar acción de repetición	Caducidad de la acción de repetición o falencias en el ejercicio de esta acción, generando la imposibilidad de recuperar los recursos pagados por el Estado
12	Informe que acredite o anuncie la existencia de perjuicios generados a la entidad	Omisión en la obligación de impulsar acción judicial para cobrar clausula penal u otros perjuicios
13	Contratación de bienes o servicios	Contratación de bienes y servicios no relacionados con las funciones de la entidad y que no generan utilidad
14	Contratación de bienes	Compra o inversión en bienes innecesarios o suntuosos
15	Contratación de estudios y diseños	Estudios y diseños recibidos y pagados y que no cumplen condiciones de calidad
16	Suscripción de contratos de estudios y diseños	Estudios y diseños con amparo de calidad vencido al momento de contratar la obra y/o al momento de la ocurrencia
17	Suscripción de contratos	Sobrecostos en precios contractuales
18	Suscripción de contratos	Pagos efectuados a causa de riesgos previsibles que debieron ser asignados al contratista en la matriz de riesgos previsibles y no se le asignaron
19	Suscripción de contratos	No incluir en el contrato de seguros -amparo de bienes de la entidad- todos los bienes muebles e inmuebles de la entidad
20	Suscripción de contratos	No exigir garantía única de cumplimiento contractual
21	Suscripción de contratos respecto de los cuales la ley establece un cubrimiento mínimo en los amparos de la garantía única de cumplimiento	Exigir garantía única de cumplimiento contractual con un cubrimiento inferior al exigido por la ley
22	Pagos efectuados a contratistas	Pagar bienes, servicios u obras a pesar de no cumplir las condiciones de calidad.
23	Constancias de recibo a satisfacción de bienes, servicios u obras, firmadas por supervisor o interventor	Bienes, servicios u obras inconclusos, infuncionales y/o que no brindan utilidad o beneficio
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y

Id Referencia	Puntos de riesgo fiscal actividad en la que potencialmente se origina el riesgo fiscal	Circunstancia inmediata situación por la que se presenta el riesgo
		cuyos costos colaterales asume la entidad contratante
25	Giros efectuados por concepto de anticipo contractual	Mal manejo o fallas en la legalización de anticipos, no amortización del anticipo
26	Giros efectuados por concepto de anticipo contractual	Rendimientos financieros de recursos de anticipo o de cualquier recurso público no devueltos al tesoro público
27	Reconocimiento y pago de desequilibrio contractual	Reconocimiento y pago de desequilibrio contractual por causa imputable a la entidad
28	Firma de actas contractuales de recibo parcial o final	Errores o imprecisiones en las actas de recibo parcial o final
29	Firma de adiciones de ítems, actividades o productos no previstos (contratos adicionales)	Adición de ítem, actividad o producto no previsto sin estudio de mercado y/o con sobrecosto
30	Firma de adiciones de ítems, actividades o productos inicialmente previstos (adiciones)	Mayores cantidades reconocidas y pagadas con valores unitarios superiores al pactado en el contrato
31	Actos administrativos sancionatorios contractuales emitidos y ejecutoriados	Cuantificación errada de multa o clausula penal
32	Obras recibidas a satisfacción	Colapso o fallas en la estabilidad de la obra
33	Pagos finales efectuados a contratistas	Ejecución de un alcance inferior al contratado y pago total del contrato
34	Actas de recibo final a satisfacción firmadas	Infuncionalidad de lo ejecutado
35	Contratos finalizados	Bienes, servicios u obras inconclusas y/o que no brindan utilidad o beneficio
36	Pagos efectuados a contratistas	Inadecuada deducción de impuestos, tasas o contribuciones al contratista
37	Pagos por concepto de comisión a éxito	Pago de comisiones a éxito sin debida justificación
38	Actas de liquidación suscritas	Suscripción de acta de liquidación con imprecisiones de fondo
39	Actas de liquidación suscritas	Suscripción de acta de liquidación sin relacionar las sanciones impuestas al contratista
40	Contratos finalizados en los que se contemplaba o requería liquidación.	Pérdida de competencia para liquidar por vencimiento del plazo legal, con saldos a favor de la entidad
41	Actas de liquidación suscritas	Liquidación de mutuo acuerdo con recibo a satisfacción, habiendo imprecisiones o falsedades
42	Bienes u obras recibidas a satisfacción	Deterioro del bien u obra por indebido mantenimiento
43	Actas de recibo final a satisfacción firmadas	Suscripción de acta de recibo final con imprecisiones de fondo
43	Reintegro de saldos a favor de la entidad o pagos por parte de deudores	Reintegro de saldos a favor de la entidad sin indexación (reintegro sin actualización del dinero en el tiempo)
44	Predios adquiridos	Adquisición de predios sin las especificaciones técnicas requeridas
45	Pérdida de tenencia de bienes de la entidad	Pérdida de la tenencia de bienes inmuebles de la entidad

Id Referencia	Puntos de riesgo fiscal actividad en la que potencialmente se origina el riesgo fiscal	Circunstancia inmediata situación por la que se presenta el riesgo
46	Pago de subsidios, transferencias o beneficios a particulares	Bases de datos con falencias de información que genera pagos de subsidios u otros beneficios sin el cumplimiento de requisitos y condiciones
47	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidio u otros beneficios a personas fallecidas
48	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios u otros beneficios a personas que no tienen derecho a los mismos a la luz de requisitos de ley
49	Pago de subsidios, transferencias o beneficios a particulares	Pago de subsidios por encima del beneficio otorgado
50	Deudas a favor de la entidad	Vencimiento de plazos para la labor de cobro directo (persuasivo o coactivo) o judicial

Fuente: anexo 3, capítulo "identificación y valoración de riesgos fiscales y diseño de controles para su prevención y mitigación", guía para la gestión integral del riesgo en entidades públicas, DAFP.

Identificación de Factores de Riesgo

Los factores de riesgo son las fuentes generadoras de riesgo, es decir el elemento a partir del cual se puede producir un evento o situación que impacte negativamente la gestión de la entidad. A continuación, se presentan algunos ejemplos de factores de riesgo que puede tener la entidad:

Tabla 3. Factores de riesgo.

Factor	Definición	Descripción
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional	Falta de aplicación de los procedimientos
		Falta de Segregación de funciones
		Errores de grabación, autorización
		Falta de supervisión o interventoría
		Errores en cálculos para pagos internos y externos
		Alta rotación o insuficiencia de personal
		Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
		Acciones contrarias a las leyes o acuerdos contractuales
		Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un	Contrapartes de la entidad (naturales o jurídicas)

Factor	Definición	Descripción
(aplica para LA/FT/FP	bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica	Productos (bienes o servicios) que oferta/requiere
		Canales utilizados para la operación
		Jurisdicciones (nacional o territorial)
Talento Humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.	Fraude interno
		Soborno
		Gestión inadecuada de conflicto de Intereses
		Corrupción
	.	Hurtos activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de sistemas de información y aplicaciones
		Caída de redes
		Errores en hardware o software
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad	Derrumbes
		Incendios
		Inundaciones
	.	Daños a activos fijos
Evento Externo	Situaciones externas que afectan la entidad.	Fraude Externo
		Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

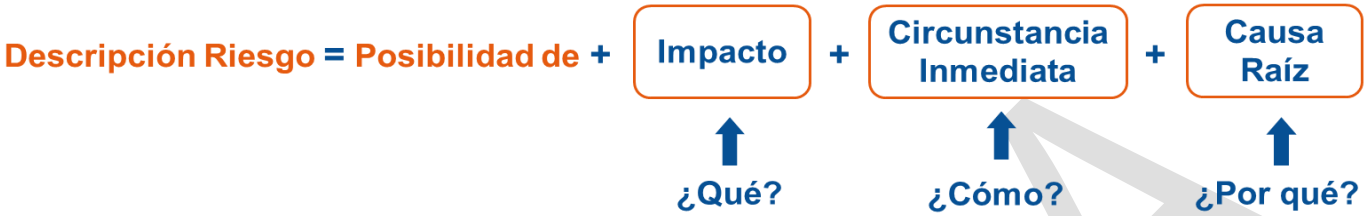
Fuente: adaptado de Guía para la gestión integral del riesgo en entidades públicas, DAFP.

Descripción de Riesgos de Gestión, Fiscal, Seguridad Digital, Integridad Pública - Corrupción

Una vez determinada las áreas de impacto (consecuencias), puntos de riesgos (actividades a partir de las cuales se puede materializar un riesgo) y factores de riesgo (causas o fuentes de riesgo), se debe describir el riesgo. La descripción de los riesgos debe contener la información suficiente para que el líder del proceso, así como los colaboradores de la entidad comprendan la manera como se puede manifestar el riesgo y las causas que lo producen, lo cual es de gran importancia al momento de definir los controles.

Para evitar subjetividades y contar con toda la información necesaria para comprender el riesgo el DAFP propone la siguiente estructura para la redacción de la descripción de los riesgos:

Figura 3. Estructura propuesta para la redacción del riesgo



Fuente: adaptado de Guía para la gestión integral del riesgo en entidades públicas - DAFP

- **Impacto:** es la consecuencia de la materialización del riesgo (directamente relacionado con el área de impacto identificada).
- **Circunstancia Inmediata:** circunstancia o Situación más evidente sobre la cual se puede presentar el riesgo, esta no constituye la causa principal para que se presente el riesgo.
- **Causa Raíz:** es la causa o razón principal por la cual se puede presentar el riesgo, a partir de esta se realiza la definición de los controles en la etapa de evaluación del riesgo.

5.2.2.2. Ejemplo Riesgos Gestión

Tabla 4. Redacción de riesgos de gestión

Posibilidad de afectación reputacional por sanciones de los entes reguladores debido a la baja apropiación del Sistema de Gestión.	**Impacto**	**Afectación reputacional**
	Circunstancia Inmediata	Sanciones de entes reguladores
	Causa Raíz	Baja apropiación del Sistema de Gestión.

Fuente: elaboración propia.

5.2.2.3. Ejemplo Riesgo Fiscal

Tabla 5. Redacción de riesgos fiscal.

Posibilidad de efecto dañoso sobre los recursos de la entidad por la generación de intereses moratorios en contrato de arrendamiento a causa de la omisión en el pago oportuno del canon pactado.	**Impacto**	**Recursos de la entidad**
	Circunstancia Inmediata	Generación de intereses moratorios en contrato de arrendamiento
	Causa Raíz	Omisión en el pago oportuno del canon pactado.

Fuente: elaboración propia.

5.2.2.4. Riesgos para la Integridad Pública (SIGRIP) – Corrupción

Tabla 6. Redacción de riesgos de corrupción.

Posibilidad de afectación económica por corrupción en la evaluación de los procesos de selección para la contratación de bienes y servicios de la entidad, a causa del direccionamiento y/o favorecimiento de la contratación hacia un proponente específico.	**Impacto**	**Afectación económica por corrupción**
	Circunstancia Inmediata	evaluación de los procesos de selección para la contratación de bienes y servicios de la entidad
	Causa Raíz	Direccionamiento y/o favorecimiento de la contratación hacia un proponente específico

Fuente: elaboración propia.

5.2.2.5. Identificación riesgos de Seguridad Digital

Identificación de Activos de Información

La identificación de riesgos de seguridad digital inicia con el reconocimiento y registro de los activos de información asociados a cada proceso. Esta etapa permite establecer un inventario detallado de activos con base en su criticidad, tipo, dueño y nivel de sensibilidad. Esta actividad se desarrollará siguiendo los lineamientos establecidos en la Guía de Identificación, Actualización y Clasificación de Activos de Información de la entidad.

Cada activo deberá estar clasificado conforme a su naturaleza (información, software, hardware, servicios, personal o instalaciones), e incluir atributos como: proceso al que pertenece, responsable (dueño del activo), custodio, nivel de criticidad e impacto sobre la confidencialidad, integridad y disponibilidad de la información.

Identificación de las Amenazas – (causa Inmediata)

Las amenazas corresponden a eventos o situaciones con el potencial de causar daño a los activos de información, comprometiendo su confidencialidad, integridad o disponibilidad. Representan la causa inmediata de un posible incidente de seguridad.

En el contexto de la gestión de riesgos de seguridad digital, es importante identificar de manera sistemática las amenazas relevantes para cada activo, considerando su naturaleza (física, tecnológica, humana, organizacional o ambiental) y su origen (deliberadas, ambientales o fortuitas).

A continuación, se presentan ejemplos de amenazas comunes que pueden afectar la seguridad digital y que deben tenerse en cuenta al describir el escenario de riesgo:

Tabla 7. Amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F, D, A
	Agua	F, D, A
	Contaminación	F, D, A
	Accidente Importante	F, D, A
	Destrucción del equipo o medios	F, D, A
	Polvo, corrosión, congelamiento	F, D, A
Eventos naturales	Fenómenos climáticos	A
	Fenómenos sísmicos	A
	Fenómenos volcánicos	A
	Fenómenos meteorológicos	A
	Inundación	A
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado	A
	Perdida de suministro de energía	A
	Falla en equipo de telecomunicaciones	D, F
Perturbación debida a la radiación	Radiación electromagnética	D, F
	Radiación térmica	D, F
	Impulsos electromagnéticos	D, F
Compromiso de la información	Interceptación de señales de interferencia comprometida	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	D, F
	Datos provenientes de fuentes no confiables	D, F
	Manipulación con hardware	D
	Manipulación con software	D
	Detección de la posición	D, F
Fallas técnicas	Fallas del equipo	F
	Mal funcionamiento del equipo	F
	Saturación del sistema de información	F
	Mal funcionamiento del software	F
	Incumplimiento en el mantenimiento del sistema de información.	F
Acciones no autorizadas	Uso no autorizado del equipo	D

Tipo	Amenaza	Origen
	Copia fraudulenta del software	D
	Uso de software falso o copiado	D
	Corrupción de los datos	D
	Procesamiento ilegal de datos	D
Compromiso de las funciones	Error en el uso	D, F
	Abuso de derechos	D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	D

Fuente. Ministerio de Tecnologías de la Información y las Comunicaciones.

Identificación de las vulnerabilidades – (Causa raíz)

Las vulnerabilidades son debilidades inherentes a un activo, proceso o control que pueden ser explotadas por una o más amenazas, aumentando la probabilidad de un incidente y/o su impacto sobre la confidencialidad, integridad o disponibilidad de la información. A continuación, se relacionan las posibles vulnerabilidades de acuerdo con su tipo.

Tabla 8. Vulnerabilidades Comunes.

Tipo	Vulnerabilidad
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro

Tipo	Vulnerabilidad
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad

Fuente: adaptado de la Gruía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP.

La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.

A continuación, se presentan ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas:

Tabla 9. Ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o medios
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Perdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurtos medios o documentos
	Falla de cuidado en la disposición final	Hurtos medios o documentos
	Copia no controlada	Hurtos medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de sesión" cuando se abandona la sesión de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de los datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de los datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del Software
	especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del Software
	Ausencia de control de cambios eficaz	Mal funcionamiento del Software
	Descarga y uso de software no controlado	Manipulación del Software
	Ausencia de copias de respaldo	Manipulación del Software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Fallas en la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envió o recepción de mensajes	Negación de acciones

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
	Líneas de comunicación sin protección	Escucha encubierta
	Trafico sensible sin protección	Escucha encubierta
	conexión deficiente de los cables	fallas del equipo de telecomunicaciones
	Punto único de fallas	fallas del equipo de telecomunicaciones
	Ausencia de identificación y autenticación del emisor y receptor	Falsificación de derechos
	Arquitectura insegura de red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Recurso Humano	Ausencia de personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto del Hardware y Software	Error en el uso
	Falla de conciencia acerca de seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Acceso Físico (lugar)	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	
	Ubicación en área susceptible de inundación	
	Red energética inestable	
	Ausencia de protección física de la edificación, puertas y ventanas	
Acceso Logico (organización)	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia del proceso formal para la revisión de los derechos de acceso	Abuso de los derechos
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a seguridad)	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información	Abuso de los derechos
	Ausencia de auditorias	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Ausencia de procedimiento formal para la autorización de la información disponible al publico	Datos provenientes de fuentes no confiables

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en bitácoras	Error en el uso
	Ausencia de los procesos disciplinarios en casos de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de activos que se encuentran fuera de las instalaciones	Hurto de equipo
	Ausencia de política sobre limpieza de escritorio y pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para las brechas de seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos de cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falsificado o copiado

Fuente: International Organization for Standardization & International Electrotechnical Commission (ISO/IEC). (2009). ISO/IEC 27005:2009.

Redacción del riesgo de seguridad

Tabla 10. Estructura para la formulación de riesgos de seguridad digital

Tipo de riesgo	Descripción y clasificación del riesgo	Estructura
se debe identificar que atributo de la triada de la información se ve afectado: Pérdida de disponibilidad, pérdida de integridad o pérdida de confidencialidad	Describa el escenario de riesgo e incluya un nombre breve y estandarizado (clasificación) coherente con el tipo de riesgo de la triada afectada.	Pérdida de [Disponibilidad/Integridad/Confidencialidad] del [activo/proceso] por [amenaza, causa inmediata], aprovechando [vulnerabilidad, causa raíz], lo que podría [consecuencia/impacto operacional o institucional

Fuente: elaboración propia.

Ejemplos:

- Caída del Sistema de Información Misional - SICORE[2]. Pérdida de Disponibilidad del sistema SICORE por falla en la infraestructura en nube, aprovechando ausencia de redundancia, lo que podría interrumpir la atención al ciudadano.
- Alteración de registros maestros. Pérdida de Integridad del SICORE por acceso con privilegios excesivos, aprovechando segregación de funciones deficiente, lo que podría generar información incorrecta de elegibles.
- Exposición de datos personales. Pérdida de Confidencialidad del repositorio documental por acceso indebido, aprovechando controles de acceso laxos y cifrado ausente, lo que podría derivar en afectación reputacional.

Asignación y análisis de controles de seguridad

Se registrarán el(los) control(es) aplicable(s) del Anexo A (ISO/IEC 27001:2022) o controles internos, indicando cómo se implementan, quién es responsable, su alcance/frecuencia, evidencias y el efecto esperado sobre el riesgo (probabilidad/impacto). Puede listar varios controles separados por ";".

El control se detallará de la siguiente manera,

- Control ISO (Anexo A): indique el número del control (p. ej., *A.8.28*), nombre y la descripción. (remítase al anexo 2)
- Control interno (no listado en Anexo A): use prefijo INT-## (p. ej., *INT-01*), asigne nombre y describa su implementación según la necesidad.

Clasificación de Riesgos

Una vez determinados los riesgos, estos pueden ser clasificados de acuerdo con su tipología, lo cual permite que los encargados de realizar su gestión puedan entender mejor la naturaleza de este y su enfoque. En la siguiente tabla se definen las categorías:

Tabla 11. Categorías de riesgos

Categoría	Descripción
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a Activos fijos / eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

[2] SICORE: sistema de información transaccional, desarrollado a la medida para la Agencia, el cual simplifica, estandariza y automatiza; los procesos definidos por la Gerencia de Educación Posmedia en las diferentes convocatorias que ejecuta la entidad.

Categoría	Descripción
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fiscal	Efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública.
Seguridad Digital	Amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Fuente: adaptado de Guía para la gestión integral del riesgo en entidades públicas (Departamento Administrativo de la Función Pública).

5.2.3. Valoración de Riesgos

Esta etapa de la gestión de riesgos consiste en calcular el nivel de riesgo de la Agencia, iniciando con el establecimiento de la probabilidad de ocurrencia, así como el nivel de impacto que tendría en caso de materializarse, con el propósito de establecer el nivel de riesgo inherente, es decir nivel de riesgo al que se enfrenta la entidad en caso de no aplicar controles, y finalizando con la definición del riesgo residual, es decir el nivel de riesgo de la entidad una vez aplicados los controles.

A partir de esto para el desarrollo de esta etapa se deben a su vez desarrollar dos fases:

- Análisis de riesgos (determinar el riesgo inherente).
- Evaluación de riesgos (determinar el riesgo residual).

5.2.3.1. Análisis de Riesgos

El análisis del riesgo busca establecer la probabilidad de ocurrencia de estos y el impacto de sus consecuencias, sin ningún tipo de control de los procesos, lo que se denomina riesgo inherente, calificándolos y evaluándolos, con el fin de obtener información para establecer el nivel de criticidad del riesgo y las acciones que se van a implementar.

Análisis de riesgos de Gestión, Fiscal, Seguridad Digital e Integridad Pública – Corrupción.

Determinar la Probabilidad

La probabilidad de ocurrencia de un riesgo es la posibilidad de que se produzca una situación o circunstancia que afecte negativamente la gestión de la entidad. En este sentido la probabilidad de un riesgo identificado se calcula teniendo en cuenta el número de veces que se pasa por el punto de riesgo, es decir las de veces que se realiza la actividad a partir de la cual se puede producir el riesgo en un periodo de un año de acuerdo con la siguiente escala:

Tabla 12. Criterios de Probabilidad

Nivel	Frecuencia de la Actividad	Probabilidad
Muy Baja	Actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	Actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	Actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año	60%
Alta	Actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5.000 por año	80%
Muy Alta	Actividad que conlleva el riesgo se ejecuta más de 5.000 veces al año.	100%

Fuente: adaptado de Guía para la gestión integral del riesgo en entidades públicas (Departamento Administrativo de la Función Pública).

Determinar el Impacto

El impacto de in riesgo se refiere a las consecuencias de su materialización para la entidad, en ese sentido para su estimación se tienen establecidas dos áreas de impacto definidas en la etapa de identificación de riesgos, a saber, la Afectación Económica y el Impacto Reputacional, sobre las cuales el impacto será calculado teniendo en cuenta el nivel de afectación de acuerdo con la siguiente tabla:

Tabla 13. Criterios de Impacto

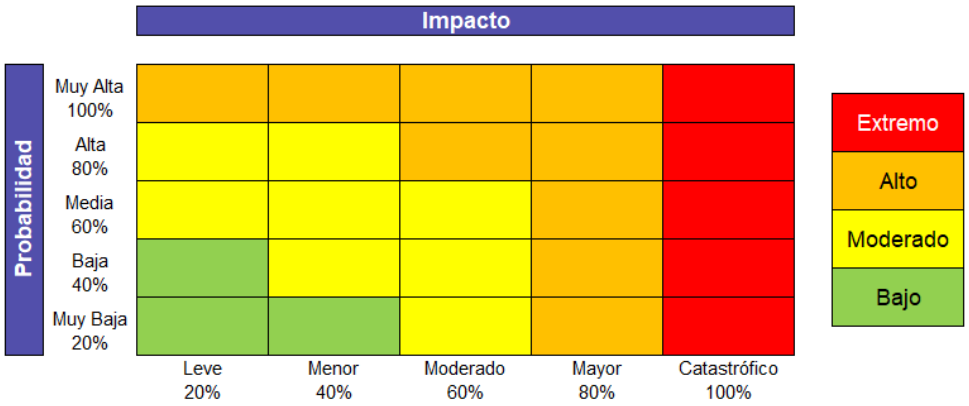
Nivel	Afectación Económica	Afectación Reputacional	Peso Porcentual (%)
Leve	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad	20%
Menor	Entre 11 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, de Junta Directiva y Accionistas y/o Proveedores	40%
Moderado	Entre 51 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	60%
Mayor	Entre 101 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de Sector Administrativo, Nivel Departamental o Municipal	80%
Catastrófico	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a Nivel Nacional, con Efecto publicitario sostenido a Nivel País	100%

Fuente: guía para la administración de los riesgos y el diseño de controles en entidades públicas. DAFP

Nivel de Riesgo Inherente

El nivel de riesgo inherente se puede entender como la valoración del riesgo establecida a partir de la estimación de la probabilidad de ocurrencia y el nivel de impacto de este, y se calcula cruzando estas dos variables en una matriz o mapa de calor, obteniendo así la severidad de este dependiendo de la zona en la cual se ubique.

Figura 4. Mapa de Calor Riesgos



Fuente: guía para la administración de los riesgos y el diseño de controles en entidades públicas. DAFP

Ejemplo: análisis de riesgos de gestión, fiscal, seguridad digital e integridad pública - corrupción

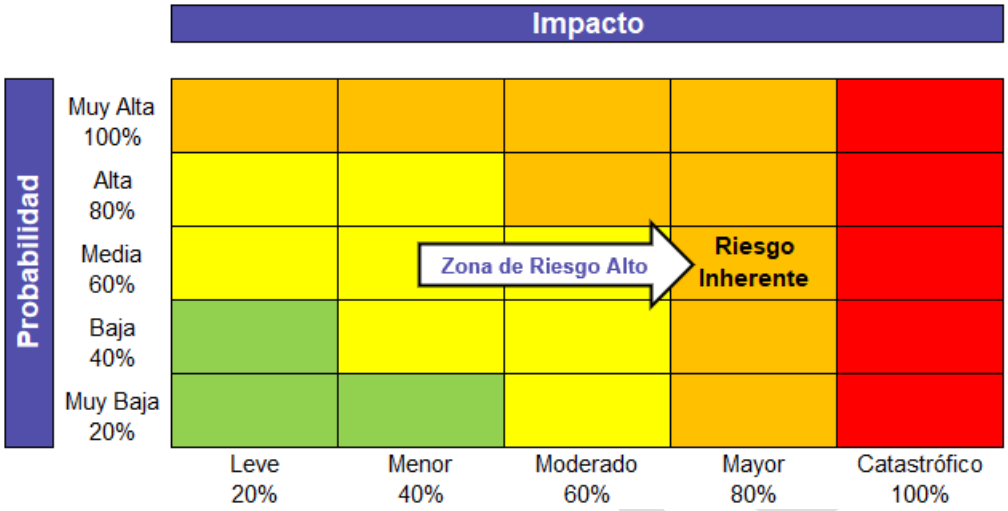
Tabla 14. Ejemplo análisis de riesgo

Campo	Descripción
Riesgo	Posibilidad de afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.
Punto de riesgo	Suscripción de contratos.
Probabilidad (frecuencia)	La actividad se realiza 120 veces al año, a razón de 10 contratos mensuales.
Nivel de probabilidad	Media (60%).
Impacto (consecuencia)	De llegar a materializarse, tendría una afectación económica de 500 SMLMV.
Nivel de impacto	Mayor (80%).

Fuente: adaptado de guía para la gestión integral del riesgo en entidades públicas - DAFP.

Con base en la información del riesgo se puede determinar el nivel de riesgo inherente en el mapa de calor, ubicando el espacio correspondiente a la calificación de probabilidad “Media 60%” (tercera fila) y un impacto “Mayor 80%” (cuarta columna de izquierda a derecha), obteniendo así un riesgo inherente “Alto” como se muestra a continuación:

Figura 5. Ejemplo calificación nivel riesgo inherente



Fuente: elaboración propia.

5.2.3.2. Evaluación de Riesgos

Evaluación de riesgos de gestión, fiscal, seguridad digital e integridad pública - corrupción

Identificación de Controles

Un control es una medida que permite reducir o mitigar un riesgo. En otras palabras, acciones que permitan verificar e identificar situaciones que conduzcan al riesgo y tratarlas oportunamente, o bien acciones que una vez materializado el riesgo disminuyan el impacto de este sobre la entidad. La responsabilidad de la implementación y el monitoreo de los controles recae en los líderes de los procesos con el apoyo de su equipo.

La identificación de controles debe realizarse para cada riesgo identificado por los líderes de proceso o servidores expertos en el quehacer de este, y cada riesgo puede contar con varios controles para su mitigación.

Descripción de un Control

Para redactar de manera adecuada la descripción de un control se emplea la siguiente estructura:

- **Responsable de ejecutar el control:** es el cargo o rol del servidor que ejecuta el control, para controles de tipo automático en este apartado se relaciona el sistema que realiza el control.
- **Acción:** describe el acto realizado para ejecutar o aplicar el control.

- **Complemento:** son los detalles adicionales necesarios para identificar y entender claramente el propósito del control.

Tabla 15. Ejemplo redacción de control

Enunciado del control	Estructura del control
El profesional de contratación verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos acorde con el tipo de contratación, a través de una lista de chequeo donde están los requisitos de información y la revisa con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.	**Responsable**: profesional de contratación.
	Acción: verificar que la información suministrada por el proveedor cumpla con los requisitos establecidos de acuerdo con el tipo de contratación.
	Complemento: a través de una lista de chequeo donde están los requisitos de información y la revisa con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

Fuente: adaptado de guía para la gestión integral del riesgo en entidades públicas. DAFP

Caracterización de Controles

Una vez identificados y descritos los controles, para continuar con su análisis es necesario clasificarlos de acuerdo con sus características con el fin de entender la manera como mitigan el riesgo, así como complementar su información, para lo anterior se establecen dos tipos de atributos, los atributos de eficiencia, y los atributos informativos que complementaran la información del control.

Atributos de eficiencia:
clasificación de controles de acuerdo con los atributos de eficiencia, esta clasificación permite analizar los controles a través de dos tipologías:

La primera consiste en identificar en qué momento del ciclo de procesos se aplica el control, lo cual permite identificar qué tipo de control es y de qué forma mitiga el riesgo, las tipologías de esta clasificación son:

- **Preventivo:** este tipo de controles se ejecutan al inicio o entrada de los procesos, es decir previo a pasar por el punto de riesgo (actividad a partir de la cual se genera el riesgo), y se enfoca en prevenir las causas que generan el riesgo, mitigando la probabilidad de ocurrencia de este.
- **Detectivo:** es un control que se aplica durante la realización del proceso (mientras se ejecuta la actividad que genera el riesgo) con el propósito de detectar desviaciones y actuar inmediatamente para corregirlas, con lo cual reducen la probabilidad de ocurrencia al no permitir la materialización del riesgo. Este tipo de controles generan reprocesos.
- **Correctivo:** este tipo de controles se ejecutan en la salida del proceso y posterior a la materialización del riesgo, están enfocados en reducir las consecuencias de dicha materialización, con lo cual se enfocan en reducir el impacto del riesgo.

La segunda clasificación corresponde a la forma como se implementa o ejecuta el control.

- **Manual:** control aplicado por personas**.**
- **Automático:** control ejecutado por un sistema o software previamente programado diseñado.

Atributos Informativos[3]**:**
son características de los controles que buscan complementar la información de estos, con el fin de conocer el entorno y complementar el análisis del control, están divididos en:

- **Documentación:** a través de esta característica se establece si el control se encuentra definido en un documento oficial de la Agencia.
- **Frecuencia:** este atributo informa cuando se aplica el control
- **Evidencia:** indica si se guarda registro de la aplicación del control.
- **Ejecución:** informa si la fuente de ejecución del control es interna, externa o mixta.

Calificación de Controles*:* La calificación de los controles se realiza a partir de los atributos de Eficiencia e Informativos. De acuerdo con el tipo de control se establece el eje de la matriz de calor en el cual se desplazará el riesgo al momento de calcular su nivel de riesgo residual. En la siguiente tabla se relaciona el peso de cada atributo:

Tabla 16. Ponderación Atributos de Eficiencia

Tipo de Atributo	Características		Peso
Eficiencia	Tipo	Preventivo	25%
		Detectivo	15%
		Correctivo	10%
	Implementación	Automático	25%
		Manual	15%

Fuente: adaptado de guía para la gestión integral del riesgo en entidades públicas (Departamento Administrativo de la Función Pública).

Ejemplo calificación de un control:

Tabla 17. Calificación de Controles- Ejemplo

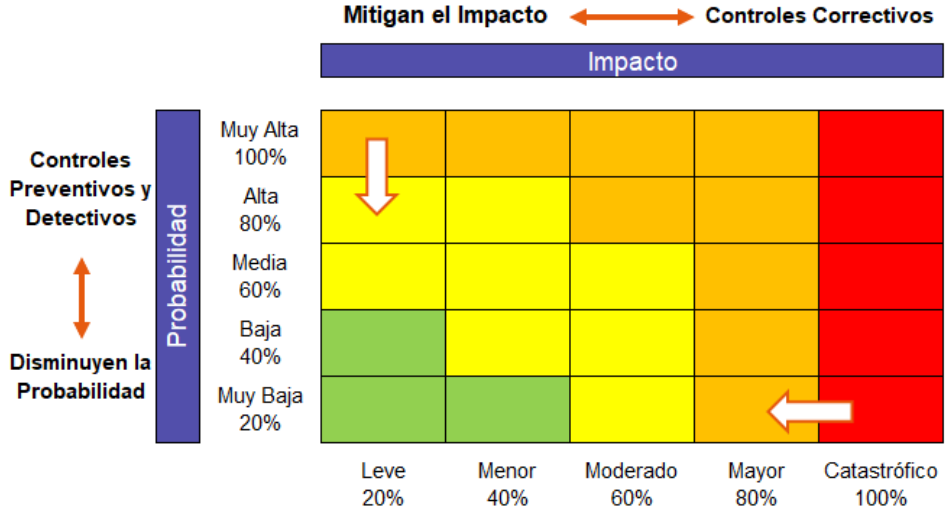
Control	Características del Control			Peso
Control 1	Tipo	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	**Automático**	X	25%
		Manual		
Total, Valoración del Control				**40%**

Fuente: elaboración propia.

[3] estos atributos no aportan a la calificación del control.

Cuando un control reduce o mitiga el impacto (tipo correctivo) la ubicación del riesgo se moverá hacia la izquierda, mientras que cuando reduce la probabilidad de ocurrencia (tipo preventivo o detectivo) se moverá hacia abajo, a continuación, se ejemplifica esto:

Figura 6. Movimiento en la Matriz de Riesgos Acorde al Tipo de Control



Fuente: guía para la administración de los riesgos y el diseño de controles en entidades públicas. DAFP

Nivel de Riesgo Residual

El nivel de riesgo residual corresponde a la calificación del riesgo una vez aplicados los controles. Para establecer este nivel de riesgo se debe calcular de forma acumulada aplicando cada control, es decir se calcula la probabilidad y el impacto de acuerdo con la calificación del primer control y sobre este resultado se aplica el segundo control, y así sucesivamente para cada uno de los controles.

A continuación, se desarrolla un ejemplo de la calificación del nivel de riesgo residual de un riesgo de acuerdo con la metodología.

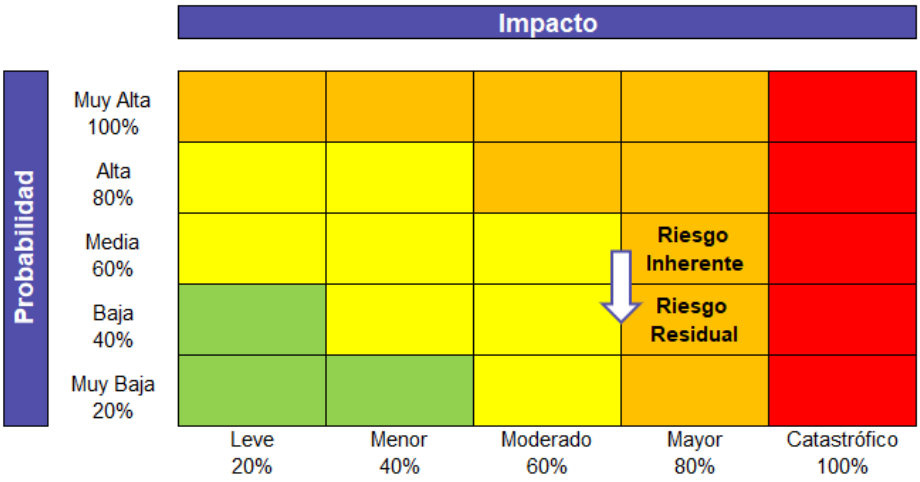
Tabla 18. Ejemplo Calificación Nivel de Riesgo Residual

Riesgo	Calificación Riesgo Inherente		Valoración de Controles		Cálculos
posibilidad de afectación 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%	**Control 1** Preventivo – Manual – Sin Documentar - Con Registro	40%	60%*40% = 24% 60%-24% = **36%**
	Valor Probabilidad tras aplicar el control 1	36%	Control 2 Detectivo – Manual – Documentado – Con Registro	30%	36%*30% = 108% 36% - 10.8% = **25.2%**
	Probabilidad Residual				**25.2%**
	Impacto Inherente	80%	NA	NA	NA
	Impacto Residual				**80%**

Fuente: adaptado de guía para la gestión integral del riesgo en entidades públicas, DAFP.

A partir de los valores de probabilidad e impacto residuales, se procede a ubicar el riesgo en su nueva posición en el mapa de calor de acuerdo con las indicaciones establecidas en la etapa de análisis como se muestra a continuación:

Figura 7. Ejemplo Riesgo Inherente



Fuente: elaboración propia.

Como resultado de la aplicación conjunta de los dos controles, se evidencia una disminución de la probabilidad del riesgo en **un nivel**, al pasar de **"Media"** a **"Baja"**.

En consecuencia, es importante precisar que los riesgos con probabilidad e impacto residual clasificados en niveles bajo o muy bajo no requieren la formulación de planes de tratamiento adicionales, en la medida en que se ubican dentro del umbral de aceptabilidad definido en la metodología institucional de gestión del riesgo, sin perjuicio del seguimiento y monitoreo periódico.

Controles Asociados a Riesgos de Seguridad Digital

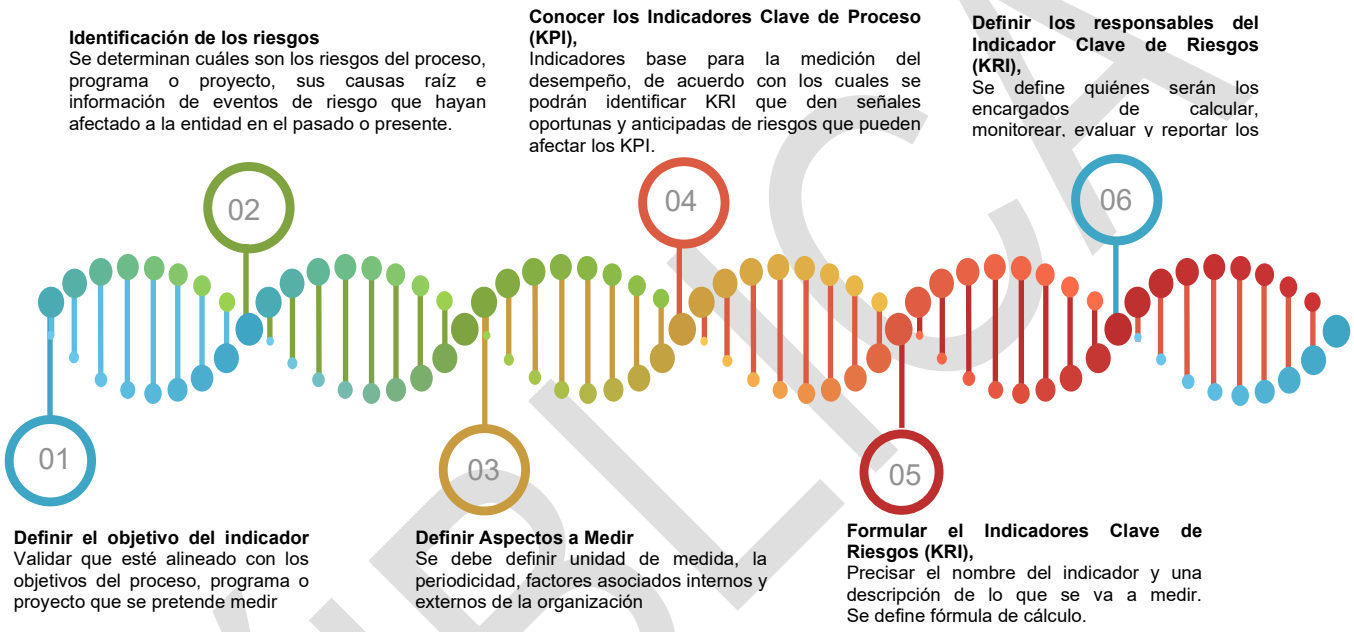
En cuanto a la identificación y selección de controles asociados a los riesgos de seguridad digital, se deben tener en cuenta los definidos en la ISO 27001, los cuales se encuentran descritos en el Anexo No. 2 Identificación y selección de controles en los riesgos de seguridad de la información, según la Norma ISO 27001: 2022.

5.2.4. Indicadores Clave de Riesgo KRI

Estos indicadores permiten registrar la ocurrencia de un evento que se asocia a un riesgo identificado previamente, lo cual permite llevar un registro de eventos y evaluar a través de su tendencia la efectividad de los controles que se disponen para mitigarlos.

Para la definición y construcción de los Indicadores Clave de Riesgos (KRI), se proponen los siguientes pasos que se despliegan en la figura 8:

Figura 8 Pasos para la construcción de Indicadores Clave de Riesgos (KRI)



Fuente: adaptado de Guía para la gestión integral del riesgo en entidades públicas (Departamento Administrativo de l Función Pública).

Para el desarrollo de los anteriores pasos se debe tener en cuenta:

1. Definir el objetivo del indicador, el cual debe estar alineado con los objetivos del proceso, plan, programa o proyecto que se pretende medir.
2. Identificar los riesgos, en este paso se determinan cuáles son los riesgos del proceso, plan, programa o proyecto, sus causas raíz e información de eventos de riesgo que hayan afectado a la entidad en el pasado o presente. Sobre la gestión de eventos, se trata de un riesgo materializado, donde 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. Algunas fuentes para establecer una base histórica de eventos pueden ser: i) mesas de ayuda; ii) PQRD (peticiones, quejas, reclamos, denuncias); iii) Oficina jurídica; iv) Líneas internas y externas de denuncia.
3. Definir los aspectos a medir, para lo cual se deben establecer la unidad de medida, la

periodicidad, los factores internos o externos de la entidad y especialmente, que se pretende medir.
4. Conocer los Indicadores Clave de Proceso (KPI), teniendo en cuenta que estos son la base de medición del desempeño del proceso, programa o proyecto.
5. Formular el Indicador Clave de Riesgo (KRI), se debe precisar como mínimo lo siguiente:

- El nombre del indicador
- Descripción de lo que se va a medir
- Fórmula de cálculo
- Fuente de información para el cálculo del indicador, por ejemplo: sistemas internos, reportes de auditoría, bases de datos internas y/o externas u otras fuentes
- Frecuencia de medición y seguimiento
- Umbrales de alerta.

En este punto se deben establecer los umbrales de alerta, ya que no todos los cambios en los KRI requieren acción inmediata, por lo que, es fundamental que el líder del proceso, plan, programa o proyecto defina los umbrales de alerta que señalen cuándo un KRI alcanza un nivel que requiere atención, lo que permite a la entidad priorizar las actividades que necesitan intervención inmediata y distinguirlas de aquellas situaciones donde los riesgos están bajo control.

Para este efecto, para cada KRI se debe definir una semaforización que permita distinguir entre valores aceptables, riesgosos o críticos, así:

- Valor Bajo (Verde): Valor mínimo deseado
- Valor Moderado (Amarillo): Valor que indica riesgo potencial
- Valor Alto (Rojo): Valor crítico o inaceptable

Cuando en los KRI se identifica alguna desviación y/o reporte de materialización de riesgos se hace necesario formular el respectivo Plan de tratamiento para la mitigación del riesgo, aplicando lo establecido en el procedimiento de gestión de acciones de mejora.

5.2.5. Tratamiento de Riesgos

Una vez completada la valoración de los riesgos, estos deben ser tratados, requiriendo que el líder de proceso defina planes de tratamiento de acuerdo con los siguientes criterios:

1. Atributo de formalización - Documentación: cuando el control no esté documentado.
2. Nivel de probabilidad: cuando la calificación del nivel de probabilidad residual sea media, alta o muy alta.
3. Indicador clave de riesgo: si durante o al cierre de la vigencia el resultado del KRI se encuentra en el umbral "en riesgo" o "crítico".

5.2.6. Monitoreo y Revisión

La entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de riesgos de la entidad. Para lograr este objetivo se establecen las responsabilidades, teniendo en cuenta lo establecido en la Guía para la gestión integral del riesgo en entidades públicas (Departamento Administrativo de la Función Pública).

Por lo anterior se definen las responsabilidades para el monitoreo y revisión así:

Dirección General

- Definir el marco general y metodológico para la gestión y el control del riesgo, así como revisar su cumplimiento.
- Revisar los informes presentados por los líderes de proceso, de los eventos que han materializado riesgos en la entidad, así como las causas que dieron origen. Igualmente, el cumplimiento de los planes de acción derivados para evitar en lo posible la repetición del evento.

Oficina de Control Interno

- Debe adelantar seguimiento a la gestión de riesgos de corrupción.
- Proporcionar información sobre la efectividad del Sistema de Control Interno, la operación del proceso con enfoque basado en riesgos.
- Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad.
- Alertar sobre la probabilidad de riesgo de fraude o corrupción en los procesos auditados.
- Informar al Comité Institucional de Control Interno sobre los cambios que podrían tener un impacto significativo en el SCI, identificados durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna.
- Reportar el seguimiento a riesgos, en los instrumentos definidos, tiempos y metodología establecida.

Subgerencia de Planeación

- Establecer directrices para la identificación, análisis, evaluación y tratamiento de los riesgos, y realizar monitoreo al cumplimiento de la gestión de riesgos.
- Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para eliminar la causa de materialización y evitar nuevas desviaciones.

Líder de proceso

- Identificar y valorar los riesgos de gestión, fiscales e integridad pública - corrupción, que pueden afectar el logro de los objetivos y metas institucionales.
- Revisar los cambios en el Direccionamiento Estratégico o en el entorno que puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos.
- Definir para cada vigencia la gestión de riesgos de sus procesos, de acuerdo con la metodología adoptada por la Agencia.
- Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos.
- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
- Revisar y reportar a la Oficina de Control Interno, los eventos de riesgos que se han materializado en la entidad, así como las causas que dieron origen a esos eventos de riesgos materializados y definir los planes de acción correspondientes.
- Revisar y hacer seguimiento al cumplimiento de las actividades y planes de tratamiento definidos para la vigencia con relación a la gestión de riesgos y realizar el reporte correspondiente a la Subgerencia de Planeación y la Oficina de control Interno, cuando así se requiera.

Subgerencia de Tecnologías de Información y Comunicaciones

Será la responsable de realizar seguimiento a la gestión de riesgos de seguridad digital y a los controles definidos con el fin de verificar la adecuada implementación y mitigación de los riesgos así mismo debe actualizar el análisis de riesgo cada vez que se presente.

- La inclusión, modificación o eliminación de activos de información asociados a los procesos cubiertos por el alcance del Seguridad Digital.
- Una vulnerabilidad y/o amenaza no tratada adecuadamente.

5.3. Comunicación y Consulta

Esta actividad se desarrolla de manera transversal en las diferentes etapas de la gestión del riesgo en la entidad, con el fin de generar un proceso participativo. Se refiere al conocimiento que deben tener quienes participan en la gestión del riesgo, con el fin de lograr que las decisiones en la materia se tomen con base en información pertinente y actualizada, para lo cual se estructuran y realizan divulgaciones y socializaciones.

Los documentos de identificación y análisis de riesgos de gestión, fiscales, e integridad pública - corrupción se encuentran publicados en la carpeta “Gestión del Proceso” del Mapa de Procesos y pueden ser consultados a través de la página web institucional. De manera complementaria, la Subgerencia de Planeación conserva la versión aprobada de las matrices de riesgos, junto con los

reportes de seguimiento, las evidencias asociadas y, cuando aplique, la documentación soporte del plan de tratamiento.

De otra parte, el consolidado de riesgos de Integridad Pública – Corrupción, puede ser consultado a través del menú de Transparencia y acceso a la información pública (4.3. Plan de acción) de la página web de la entidad, como anexo del Plan de Transparencia y Ética Pública -PTEP de cada vigencia. La matriz de riesgos de Seguridad Digital se encuentra disponible para consulta en el SharePoint de la Subgerencia de Tecnologías de la Información y las Comunicaciones, con acceso restringido y bajo el principio de necesidad de conocer.

Lo anterior, teniendo en cuenta que su contenido incluye información sensible sobre activos, vulnerabilidades, escenarios de riesgo y controles, cuya divulgación podría incrementar la exposición de la entidad y representar un riesgo para la seguridad. Por tal motivo, su consulta se realiza de manera controlada por los responsables autorizados.

5.4. Registro y reporte de incidentes - Seguridad Digital

Es importante contar con el registro de los incidentes de seguridad de la información digital que se hayan materializado, con el fin de analizar sus causas, identificar posibles fallas o debilidades en los controles implementados y evaluar las pérdidas o afectaciones que puedan derivarse.

El propósito del registro de incidentes es asegurar que se adopten acciones oportunas y adecuadas para prevenir su recurrencia o reducir su probabilidad e impacto, así como retroalimentar y fortalecer la identificación y gestión de los riesgos asociados. Adicionalmente, este registro permite consolidar estadísticas sobre amenazas y vulnerabilidades, facilitando la toma de decisiones y la definición o ajuste de controles.

Lo anterior se desarrolla de conformidad con lo establecido en la Guía de Gestión de Incidentes de Seguridad de la Información Digital adoptada por la entidad.

6. ANEXOS

- Anexo No. 1. Contexto de Procesos.
- Anexo No. 2. Identificación y selección de controles en los riesgos de seguridad digital, según la Norma ISO 27001.
- Anexo No. 3. Matriz RACI Guía de Gestión Integral de Riesgos.

7. DOCUMENTOS DE REFERENCIA

- Documento Análisis de Contexto Estratégico Institucional de la Agencia Atenea: https://agenciaatenea.gov.co/transparencia-acceso-informacion-publica/1-informacion-de-la-entidad/13-mapas-y-cartas-descriptivas-de-los-procesos-2023/procesos-estrategicos/direccionamiento-estrategico

- Documento de Anexo 4. Lineamientos para la gestión de riesgos de seguridad digital en entidades Públicas, 2018, Ministerio de Tecnologías de la Información y Comunicaciones.
- Documento Plan Institucional de Participación Ciudadana de la Agencia Atenea: https://agenciaatenea.gov.co/transparencia-acceso-informacion-publica/6-participa.
- Guía de Gestión de Incidentes de Seguridad de la Información ,
- Guía para la gestión integral del riesgo en entidades públicas V7-2025, Departamento Administrativo de la Función Pública, 2025.
- Guía de identificación, clasificación y actualización de activos.
- Manual Operativo del Modelo Integrado de Planeación y Gestión del Departamento Administrativo de la Función Pública DAFP.
- Procedimiento de gestión de acciones de mejora.

8. RELACIÓN DE FORMATOS

CODIGO	NOMBRE DEL FORMATO
F1_G1_DE	Matriz de riesgos
F3_G1_DE	Formato Control de Cambios en la Gestión de Riesgos

9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
19/07/2024	G1_DE V3	Los principales cambios están asociados a las directrices definidas por el Departamento Administrativo de la Función Pública en la Guía para la gestión integral del riesgo en entidades públicas V7-2025. Incluye entro otros temas, conceptos relacionados con la gestión de riesgos de integridad pública, estandarización de la calificación de controles, Indicadores Clave de Riesgo (KRI) y criterios para la definición de acciones de tratamiento. Estos cambios, en consecuencia, conllevan a la modificación del formato F1_G1_DE en el cual se realiza el registro de la información de los riesgos producto de la aplicación de metodología, así como la anulación del formato F2_G1_DE Matriz de Riesgos de corrupción. Esta versión no incluye los riesgos de Integridad Pública LAFT, dado que su alcance implica, un análisis detallado a partir de la implementación de un nuevo procedimiento, la articulación de diferentes directrices, herramientas y en general la consolidación de información que permita definir la metodología que debe ser adoptada por la Agencia.
23/11/2023	G1_DE V2	Se incluye la información relacionada con la gestión de riesgos fiscales. Se realiza un ajuste general en la redacción del documento y se reorganiza por capítulos teniendo en cuenta las fases para realizar la gestión de riesgos. Se incluyen las definiciones de circunstancia inmediata, punto de riesgo, programa de transparencia y ética pública, y riesgos fiscales.

		Los criterios de operación 9, 10 y 11 (versión 2), se consolidan en el criterio 5.1.9 (versión 3). Se incluyen los criterios de operación 5.1.13 y 5.1.15.
14/09/2023	G1_DE V1	Se incluye la información relacionada con las responsabilidades de las líneas de defensa y aclaraciones adicionales en el riesgo residual ante la gestión de los riesgos de lavado de activos y financiación del terrorismo. De igual manera, se incluye la información relacionada con la ejecución de controles para los riesgos de corrupción y se crea el formato Control de Cambios en la Gestión de Riesgos, con el fin de que los procesos puedan registrar las solicitudes de modificación, eliminación e inclusión de riesgos.

VALIDACIÓN	NOMBRE	CARGO	FECHA
Elaboró	Andrés Felipe Rodríguez Plazas	Profesionales contratista Subgerencia de Planeación	30/01/2026
	Claudia Johanna Casallas Larrottta	Profesionales contratista Subgerencia de Planeación	30/01/2026
	Diana María Vargas Barón	Profesionales contratista Subgerencia de Planeación	30/01/2026
	María Alejandra del Pilar Suárez Rojas	Subgerente de Tecnologías de la Información las Comunicaciones	30/01/2026
Revisó	Ana María García Cañadulce	Profesional contratista Subgerencia de Planeación	30/01/2026
	Carlos Andrés Ballesteros	Subgerente de Tecnologías de la Información y las Comunicaciones	30/01/2026
Aprobó	Ximena Pardo Peña	Subgerente de Planeación	30/01/2026

Firmado digitalmente por Ximena Pardo

NOMBRE Y FIRMA DEL LÍDER DE PROCESO

ANEXO NO. 1 CONTEXTO DE PROCESOS

Ante el establecimiento del contexto de procesos, es importante determinar las características o aspectos principales de cada uno de los procesos y sus interrelaciones, dentro de los cuales es importante resaltar los objetivos, alcance, relaciones, responsables y documentos asociados. Al momento de identificar los riesgos tanto de gestión como de corrupción, deben tenerse en cuenta aquellos aspectos que puedan influir tanto positiva como negativamente en el cumplimiento de los objetivos del proceso, por lo cual se detallan a continuación estos aspectos:

1. **Diseño del Proceso:** En primer lugar, es necesario conocer la definición de proceso, el cual es entendido como el conjunto de actividades interrelacionadas que parten de uno o más elementos de entrada que se transforman, generando un resultado o una salida
   A partir de esto, la definición de mapa de procesos se refiere a la representación gráfica otorgada a los procesos que componen la organización ordenados en el ciclo productivo de la entidad para mostrar la relación que nace desde las necesidades del cliente y terminando el ciclo con la entrega del producto/servicio al cliente. Los procesos se clasifican en estratégicos, misionales, de apoyo y de evaluación. En la Agencia Atenea, se pueden consultar en el siguiente enlace: https://agenciaatenea.gov.co/transparencia-acceso-informacion-publica/1-informacion-de-la-entidad/13-mapas-y-cartas-descriptivas-de-los-procesos-2023.

2. **Interacción con otros procesos:** El mapa de procesos permite visualizar fácilmente cuáles son y cómo se relacionan los procesos de una entidad y adicionalmente, presenta las siguientes ventajas:
   - Implica la definición de roles y responsabilidades en la entidad.
   - Mejora el flujo de información entre las diferentes funciones.
   - Al tener objetivos definidos en todos los niveles, se propicia que todos los niveles estén alineados con su visión general.
   - Con funciones y procesos orientados en una cadena de valor, los objetivos definidos en todos los niveles están alineados a la visión organizacional.
   - A partir del mapa de procesos se consiguen indicadores claves de desempeño y se pueden identificar oportunidades de mejora.

Con todo lo anterior, se establecen las interacciones entre todos los procesos de la Agencia, se visualiza como se entrecruzan entre sí y cómo unos dependen de otros para lograr las salidas esperadas. El Mapa de Procesos de la Agencia Atenea se puede consultar en el siguiente enlace: https://agenciaatenea.gov.co/transparencia-acceso-informacion-publica/1-informacion-de-la-entidad/13-mapas-y-cartas-descriptivas-de-los-procesos-2023.

3. **Transversalidad:** La gestión basada en procesos implica enfocarse en el desarrollo de las actividades de la entidad para lograr la mejora continua y el cumplimiento de objetivos. A partir de esto y de lo reflejado en el mapa de procesos, el insumo principal para desarrollar todas las

actividades derivadas de la Agencia Atenea se centra en la información detallada como entradas, las cuales se refieren a las necesidades y expectativas de partes interesadas y grupos de valor.

Con todo lo anterior, se entiende que todas las actividades y gestión realizadas por la Agencia Atenea deben apuntar a que la necesidad y expectativas de las partes interesadas y los grupos de valor sean satisfechas, teniendo en cuenta que la gestión de procesos funciona con un objetivo común para toda la entidad y a partir de ahí se generan las actividades que generan valor para el cliente.

4. **Procedimientos Asociados:** A partir de lo descrito en el artículo 3 del Decreto 273 de 2020, se indica que la Agencia tiene por objeto fortalecer, promover, financiar y propiciar oferta educativa del nivel superior, privilegiando la educación superior a través de las Instituciones de Educación Superior Pública, desde la educación media a la técnica, tecnológica y universitaria, en todas las modalidades; articular la oferta educativa con la demanda laboral del sector privado, el sector público y las organizaciones sociales y culturales de la ciudad; así como la promoción de la ciencia y la tecnología, de los proyectos de investigación científica de grupos de investigación reconocidos por el Ministerio de Ciencia, Tecnología e Innovación en el Distrito Capital.

   Por lo anterior y para aportar al cumplimiento de este objeto, cada uno de los procesos se encuentra documentando la información de su gestión, a partir de o descrito en el Procedimiento de Elaboración, Modificación o Anulación y Control de Documentos.

   La documentación que se ha originado en el marco del mapa de procesos de la entidad, es publicada en el siguiente enlace: https://agenciaatenea.gov.co/transparencia-acceso-informacion-publica/1-informacion-de-la-entidad/13-mapas-y-cartas-descriptivas-de-los-procesos-2023.

   De igual manera, con el fin de llevar un control en toda la documentación de la entidad, la Subgerencia de Planeación, en el marco del Proceso de Direccionamiento Estratégico y a partir de lo descrito en el Procedimiento de Elaboración, Modificación o Anulación y Control de Documentos, creó una herramienta denominada listado maestro de documentos, en la cual se detallan todos los tipos de documentos creados por cada uno de los procesos tanto en versión vigente como obsoleta, a partir de las diferentes mejoras o cambios que se hayan presentado en los mismos. El listado maestro se puede consultar en este mismo enlace.

5. **Líderes del Proceso:** Con el fin de describir la operación de las actividades de la Agencia y a partir del diseño organizacional definido en el Acuerdo 003 de 2021, aprobó el Modelo de Operación por Procesos de la Agencia, que describe la operación de la entidad a través del Modelo de Operación.

En estos procesos se establecen roles, responsabilidades, puntos de control, metodologías y herramientas para la generación de información, análisis e identificación de acciones de mejora en el marco de la gestión de la entidad y el cumplimiento de lo descrito en el decreto 273 de 2020 y a partir de esta estructura y sus modificaciones se define y actualiza la documentación de la operación de los diferentes procesos de la entidad.

Cada uno de los procesos, cuenta con un documento de caracterización, en el cual se detallan los responsables de la operación de la entidad y los líderes. La caracterización de cada proceso se puede consultar en la carpeta Gestión del Proceso en https://agenciaatenea.gov.co/transparencia-acceso-informacion-publica/1-informacion-de-la-entidad/13-mapas-y-cartas-descriptivas-de-los-procesos-2023.

6. **Comunicación entre los Procesos:** La comunicación entre los procesos es muy importante, teniendo en cuenta la necesidad de que todos los procesos- al igual que se mencionó en el apartado de interacción-, se comuniquen y trabajen de manera conjunta ante la consecución de los objetivos de la entidad, sea por el uso de insumos compartidos o por la necesidad de que los procesos sean ejecutados de manera sincronizada para la finalización de las actividades.

   A partir de esto, en el mapa de procesos de la Agencia Atenea se evidencian las interrelaciones y la comunicación que existe entre los diferentes tipos de procesos, los cuales son representados con flechas entre sí, dando cuenta de la importancia de los aportes que cada tipo de proceso puede brindarle a los demás. De igual manera, las flechas dan cuenta del inicio de la gestión y de las actividades de la Agencia Atenea a partir de las entradas y de la finalización y cumplimiento de estas al pasar por la gestión de todos los procesos, representadas en las salidas.

ANEXO NO. 2. IDENTIFICACIÓN Y SELECCIÓN DE CONTROLES EN LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN, SEGÚN LA NORMA ISO 27001: 2022

Núm.	Nombre	Descripción / Justificación
A.5	**Controles organizacionales**	
A.5.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes, que integren controles de ciberseguridad específicos para detectar y responder a incidentes, para garantizar un enfoque coordinado en la protección del ciberespacio
A.5.2	Roles y responsabilidades en la seguridad de la información	Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
A.5.3	Segregación de tareas	Control: Deben segregarse los deberes y las áreas conflictivos de responsabilidad.
A.5.4	Responsabilidades de gestión	Control: La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.
A.5.5	Contacto con las autoridades	Control: Se deben mantener los contactos apropiados con las autoridades pertinentes.
A.5.6	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.5.7	Inteligencia de amenazas	Control: La información relacionada con las amenazas a la seguridad de la información debe recopilarse y analizarse para generar información sobre amenazas. Se sugiere establecer un procedimiento formal de Inteligencia de amenazas de la seguridad de la información.
A.5.8	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.5.9	Inventario de activos de información y otros asociados a la misma	Control: Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios
A.5.10	Uso aceptable de activos de información y otros asociados a la misma	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.5.11	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
A.5.12	Clasificación de la información	Control: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
A.5.13	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
A.5.14	Intercambio de la información	Control: Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
A.5.15	Control de Acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
A.5.16	Gestión de la identidad	Control: Debe gestionarse el ciclo de vida completo de las identidades.

Núm.	Nombre	Descripción / Justificación
A.5.17	Información de autenticación	Control: La asignación de la información secreta se debe controlar por medio de un proceso de gestión formal, además se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
A.5.18	Derechos de acceso	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.5.19	Seguridad de la información en la relación con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deberían documentar.
A.5.20	Requisitos de seguridad de la información en contratos con terceros	Control: Los requisitos de seguridad de la información pertinentes deben establecerse y acordarse con cada proveedor en función del tipo relación con el proveedor.
A.5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC (Tecnologías de Información y Comunicación)	Control: Deben definirse e implementarse procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.
A.5.22	Gestión del cambio, revisión y monitoreo de los servicios del proveedor o suministrador	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
A.5.23	Seguridad de la información para el uso de servicios en la nube (cloud)	Control: Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.
A.5.24	Planeamiento y preparación de la gestión de incidentes de seguridad de la información	Control: Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.
A.5.25	Evaluación y decisión en los eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
A.5.26	Respuesta a los incidentes de seguridad de la información	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.5.27	Aprendizaje sobre los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
A.5.28	Recolección de evidencia	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.5.29	Seguridad de la información durante interrupciones	Control: La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.
A.5.30	Preparación de las TIC para la continuidad de negocio	Control: La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.
A.5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Control: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

Núm.	Nombre	Descripción / Justificación
A.5.32	Derechos de propiedad intelectual	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.5.33	Protección de registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
A.5.34	Privacidad y protección de la PII (Información Identificable Personal)	Control: La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales. Se recomienda incluir dentro del procedimiento de gestión de incidentes las actividades pertinentes para atender de manera diligente los incidentes relacionados con información personal de acuerdo con lo establecido en la ley 1581 del 2012.
A.5.35	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
A.5.36	Cumplimiento con las políticas, reglas y normas de la seguridad de la información	Control: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.5.37	Procedimientos operacionales documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.
A.6	**Controles de personas**	
A.6.1	Revisión de antecedentes	Control: Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal deben llevarse a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables, y deben ser proporcionales a los requisitos comerciales, la clasificación de la información a la que se accede y los riesgos percibidos.
A.6.2	Términos y condiciones de empleo	Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.6.3	Concientización, educación y entrenamiento en seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberán recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
A.6.4	Proceso disciplinario	Control: Se debe contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra colaboradores que hayan cometido una violación a la seguridad de la información.
A.6.5	Responsabilidades luego de la finalización o cambio de empleo	Control: Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.6.6	Acuerdos de confidencialidad o no revelación	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.6.7	Trabajo remoto	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza trabajo remoto.

Núm.	Nombre	Descripción / Justificación
A.6.8	Reportes de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.
A.7	**Controles físicos**	
A.7.1	Perímetros de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
A.7.2	Entrada física	Control: Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
A.7.3	Seguridad de oficinas, despachos e instalaciones	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.7.4	Supervisión de la seguridad física	Control: Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.7.5	Protección contra amenazas físicas y ambientales	Control: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.7.6	Trabajo en áreas seguras	Control: Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.7.7	Escritorio y pantalla limpios	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
A.7.8	Emplazamiento y protección de equipos	Control: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
A.7.9	Seguridad de activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
A.7.10	Medios de almacenamiento	Control: Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
A.7.11	Servicios de suministro	Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
A.7.12	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debe estar protegido contra interceptación, interferencia o daño.
A.7.13	Mantenimiento de equipos	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
A.7.14	Eliminación o reutilización segura de equipos	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
A.8	**Controles tecnológicos**	
A.8.1	Dispositivos terminales de usuario	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.8.2	Derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
A.8.3	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A.8.4	Acceso al código fuente	Control: Se debe restringir el acceso a los códigos fuente de los programas.

Núm.	Nombre	Descripción / Justificación
A.8.5	Autenticación segura	Control: Las tecnologías y los procedimientos de autenticación segura deben implementarse en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.
A.8.6	Gestión de la capacidad	Control: Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
A.8.7	Protección contra código malicioso (malware)	Control: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
A.8.8	Gestión de vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
A.8.9	Gestión de la configuración	Control: Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.
A.8.10	Borrado de información	Control: La información almacenada en sistemas de información, dispositivos o en cualquier otro medio de almacenamiento debe ser eliminada cuando ya no sea necesaria.
A.8.11	Enmascarado de datos	Control: Cuando sea aplicable, se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes. Se deben aplicar medidas como el cifrado, el control de acceso y el monitoreo del acceso y uso de estos datos, en alineación con legislaciones de privacidad relevantes ej: GDPR en Europa. Además, se deben aplicar técnicas de anonimización de datos cuando sea posible, siguiendo los lineamientos de la guía de anonimización de datos estructurados del archivo general de la nación u otras guías aplicables al respecto, reduciendo la cantidad de información personal que se almacena o se transmite innecesariamente.
A.8.12	Prevención de filtración de datos	Control: Las medidas de prevención de fuga de datos deben aplicarse a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.
A.8.13	Respaldo de información	Control: Se deben hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
A.8.14	Redundancia de las instalaciones de procesamiento de información	Control: Las instalaciones de procesamiento de información se debe implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.8.15	Registro	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
A.8.16	Actividades de supervisión	Control: Se deben producir, almacenar, proteger y analizar registros que registren actividades, excepciones, fallas y otros eventos relevantes.
A.8.17	Sincronización de reloj (clock)	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
A.8.18	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.
A.8.19	Instalación de software en sistemas operacionales	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

Núm.	Nombre	Descripción / Justificación
A.8.20	Seguridad en redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
A.8.21	Seguridad de servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
A.8.22	Segregación de redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.8.23	Filtrado web	Control: El acceso a sitios web externos debe administrarse para reducir la exposición a contenido malicioso.
A.8.24	Uso de criptografía	Control: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.8.25	Ciclo de vida de desarrollo seguro	Control: Deben establecerse y aplicarse reglas para el desarrollo seguro de software y sistemas.
A.8.26	Requerimientos de seguridad en aplicaciones	Control: Los requerimientos relacionados con seguridad de la información se deben incluir en los requerimientos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
A.8.27	Principios de arquitectura de sistemas e ingeniería seguras	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.8.28	Generación de código seguro	Control: Los principios de codificación segura deben aplicarse al desarrollo de software.
A.8.29	Prueba segura en el desarrollo y aceptación	Control: La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.
A.8.30	Desarrollo tercerizado	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
A.8.31	Separación de entornos de desarrollo, prueba y producción	Control: Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.8.32	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
A.8.33	Información de prueba	Control: Asegurar la protección de los datos usados para pruebas.
A.8.34	Protección de sistemas de información durante pruebas de auditoría	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.