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.

Esta guía presenta la metodología establecida por la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología - Atenea para la gestión de sus riesgos de corrupción, gestión, fiscales, de seguridad de la información, y lavado de activos y financiación del terrorismo – LA/FT; 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 ejercicios de 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, corrupción, fiscales, de seguridad de la información, y lavado de activos y financiación del terrorismo – LA/FT, 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 de los riesgos de gestión, corrupción, fiscales, de seguridad de la información y LA/FT.

3. DEFINICIONES

Activo: En el contexto de seguridad de la información 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.

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.

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

Circunstancia 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: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

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

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.

Control: Medida que permite reducir o mitigar un riesgo.

Controles Automáticos: 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: Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

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

Factores de Riesgo: Son las fuentes generadoras de riesgos

Gestión del Riesgo de Corrupción: Es el conjunto de "Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo" de corrupción.

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.

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

Integridad: Propiedad de exactitud y completitud.

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 poder ser 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

Programa de Transparencia y Ética Pública – PTEP: como el conjunto de acciones o iniciativas que se desarrollan para promover la transparencia, la ética, la integridad y la lucha contra la corrupción, desde el marco institucional y legal en el que se inscriben las entidades públicas distritales y bajo una perspectiva de corresponsabilidad en la prevención, detección y sanción de actos asociados a la corrupción.

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 el periodo de 1 año.

Punto de riesgo: es una actividad dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Reducir el Riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

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

Riesgos Fiscales: 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.

Riesgo LA/FT: Es la posibilidad de pérdida o daño que puede sufrir la Entidad por ser utilizada como instrumento para el LA/FT. Se expresa en términos de probabilidad (oportunidad o frecuencia de la ocurrencia del riesgo) e impacto (consecuencia en caso de ocurrir o materializarse).

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.

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. Para el riesgo de corrupción la tolerancia es inaceptable.

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.

4. NORMATIVIDAD ASOCIADA

- Conpes No. 167 de 2013- Estrategia Nacional de la Política Pública Integral Anticorrupción.

- Decreto 1499 de 2017, por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

- Decreto 648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.

- Decreto 1083 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.

5. DESARROLLO

La gestión del riesgo en todos los procesos y los niveles de la Agencia es un elemento estratégico para la planeación, así como de la gestión cotidiana, dado el contexto externo, interno y de procesos en el que se desenvuelve, la particularidad y naturaleza de la entidad.

La metodología para la gestión de riesgos de gestión, corrupción, fiscales, de seguridad de la información y LA/FT está construida a partir de la “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" (Riesgos de Gestión, Corrupción y Seguridad de la Información) emitida por el Departamento Administrativo de la Función Pública - DAFP. De igual manera, ante LA/FT se incluyen las orientaciones otorgadas en el documento técnico “Adaptación de medidas de prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del Distrito Capital”, de la Secretaría General de la Alcaldía Mayor de Bogotá.

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 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 puede ser consultar en el Anexo No. 1 de esta guía.

5.1.3. Las responsabilidades de la gestión de riesgos en la Agencia se describen en los mapas de riesgos publicados en la página web. Los líderes de cada proceso desarrollan e implementan actividades de control a través de la identificación, análisis, evaluación, tratamiento y monitoreo de la gestión de riesgos.

5.1.4. La Subgerencia de Planeación establece directrices y realiza apoyo técnico en las etapas de identificación, análisis, evaluación y tratamiento de los riesgos, también realiza monitoreo al cumplimiento de cada una las etapas de la gestión de riesgos, así como de la materialización de estos, la aplicación de sus controles y el cumplimiento a los planes de tratamiento.

5.1.5. La gestión de riesgos inicia con la definición de la Política de Riesgos, luego se realiza la identificación de los riesgos basados en los objetivos de los procesos, el análisis de riesgos a través del cual se realiza la calificación de los riesgos para calcular el riesgo inherente y finalmente el análisis y definición de controles para su mitigación, así como las actividades y fechas de cumplimiento para los planes de tratamiento definidos por parte del líder de cada proceso, cuando aplique.

5.1.6. La aprobación de las matrices de riesgos de gestión, fiscales, LA/FT y de Seguridad de la Información, 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 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 de los procesos deben socializar 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, corrupción, fiscales, de Seguridad de la Información y LA/FT de la entidad se hace una vez al año al finalizar la vigencia, liderada por la Subgerencia de Planeación. 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 fortalecer esta. 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 quién acompañará las actividades para modificar las matrices correspondientes.

Para los riesgos de corrupción las modificaciones avaladas por el líder de proceso deben ser aprobadas en el Comité Institucional de Gestión y Desempeño.

5.1.10. Las modificaciones de planes de tratamiento o de las fechas de cumplimiento de los planes de tratamiento para los riesgos de gestión, fiscales, de Seguridad de la Información y LA/FT,

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 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 y aprobadas por el 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. Cuando un riesgo LA/FT se materializa posterior a la vinculación de su contraparte, es obligación del administrador del sistema hacer un Reporte de Operaciones Sospechosas inmediatamente se entera de este suceso.

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

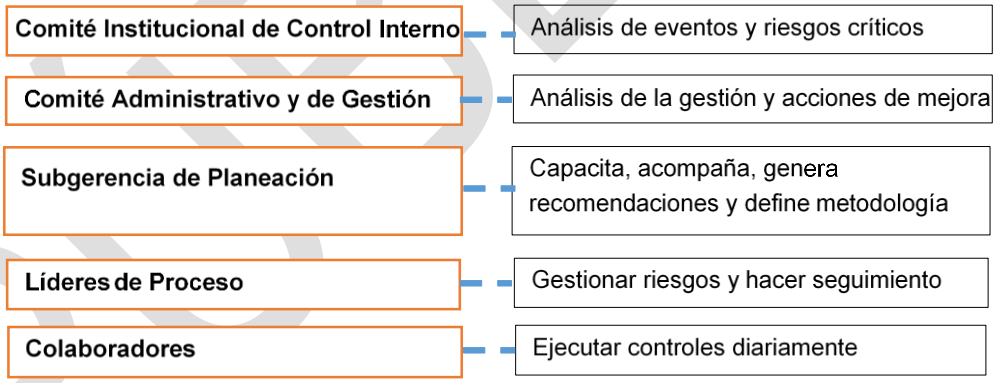

Figura 1. Responsabilidades en la gestión de riesgos

5.1.15. Las directrices definidas en esta guía aplican a la gestión de riesgos a partir de su publicación, para la gestión de los riesgos aprobada para la vigencia 2024 aplica lo estipulado en la versión 2 del 23 de noviembre de 2023.

5.2. Gestión de Riesgos de Gestión, Corrupción, Fiscales, de Seguridad de la Información y LA/FT

La gestión de riesgos de gestión, corrupción, fiscales, de seguridad de la información y LA/FT comprende las fases descritas en la siguiente figura:

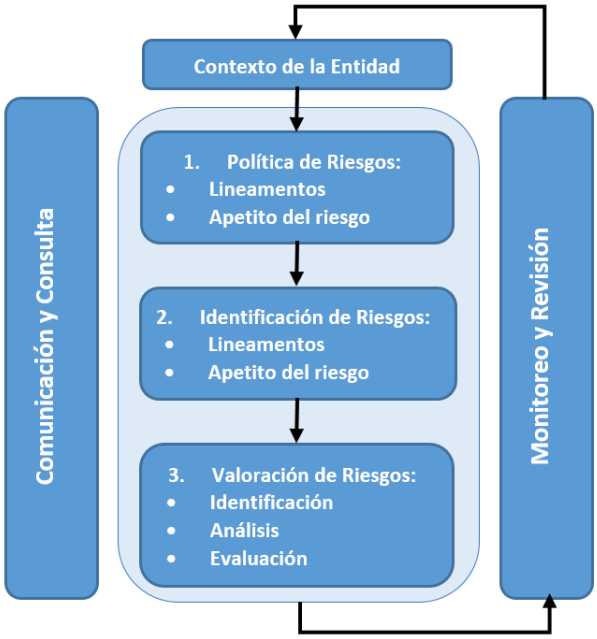

Figura 2. Diagrama de gestión de riesgos. Elaboración propia.

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 identificadas por la Agencia, que pueden incidir en los cambios 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 como: 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 como: Financieros y físicos, normativos y de procedimientos, 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 de riesgos de la entidad (de gestión, corrupción, fiscales, de seguridad de la información y LA/FT) y 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, Fiscales y LA/FT

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 pueden establecer el impacto de su materialización.

Para los riesgos fiscales su 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, pudo identificar los siguientes 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

[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*
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
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

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*
24	Modificaciones contractuales firmadas	Modificaciones contractuales cuyas causas son imputables al contratista total o parcialmente y 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 contratistas
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

Tabla 1. Puntos de riesgo fiscal.
Fuente: ANEXO 1 CAPÍTULO: Identificación y valoración de Riesgos Fiscales y Diseño de Controles para su Prevención y Mitigación - Guía para la Administración del Riesgo y el Diseño de Controles 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:

Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos
		Falta de capacitación
Talento Humano	Eventos relacionados la actuación e interacción de los colaboradores de la entidad. Incluye seguridad y salud en el trabajo. *Se analiza posible dolo e intención frente a la corrupción.	Falta de competencia en una labor
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.	Daño de equipos
		Caída de aplicaciones
		Caída de redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes
		Incendios
		Inundaciones
		Daños a activos fijos
	Situaciones externas que afectan la entidad.	Suplantación de identidad

Factor	Definición	Descripción
Evento Externo		Asalto a la oficina
		Atentados, vandalismo, orden público

Tabla 2. Factores de riesgo.
Fuente: Adaptado de la Gruía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP.

Para riesgos LA/FT se entenderán como clasificación de riesgos los factores relacionados con eventos externos, a partir de la siguiente clasificación:

Factor de Riesgo	Descripción
Contraparte	Son los Proveedores, Contratistas, Empleados, Estudiantes, Donantes, Asociados y demás terceros que puedan actuar en nombre de o relacionarse con ATENEA en el marco de sus actividades.
Circunscripción	Es la ubicación geográfica en el Distrito Capital, donde se realicen operaciones del objeto de la entidad y en las cuales se puedan determinar un mayor o menor nivel de riesgo al LA/FT.
Servicios	Son los productos o servicios que ofrece o adquiera ATENEA en desarrollo de su objeto social.
Canales de Atención	Son los canales a través de los cuales ATENEA entrega los servicios a los estudiantes.

Tabla 3. Factores de Riesgo LA/FT. Elaboración propia

Descripción de Riesgos de Gestión, Fiscales y LA/FT

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 riego el DAFP propone la siguiente estructura para la redacción de la descripción de los riesgos:

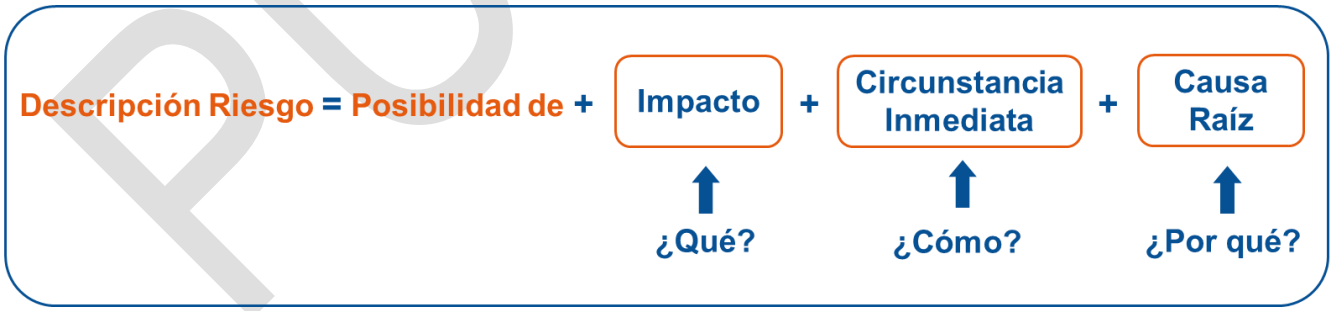

Figura 3. Estructura propuesta para la redacción del riesgo
Fuente: Adaptado de la Gruía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP.

Impacto: *es la consecuencia de la materialización del riesgo (directamente relacionado con el área de impacto identificada).*

Circunstancia Inmediata: *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.*

Ejemplo:

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.

Tabla 3. Redacción de riesgos. Elaboración propia.

5.2.2.2. Definición Riesgos de Corrupción

Los riesgos de corrupción se establecen a partir de la posibilidad de que por acción u omisión se use el poder para desviar la gestión pública hacia un beneficio privado. Teniendo en cuenta lo anterior una vez identificado un riesgo para que este se clasifique como de corrupción deben concurrir los siguientes elementos:

Figura 4. Estructura propuesta para la redacción de un riesgo de corrupción
Fuente: Adaptado de la Gruía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP.

Así mismo en la descripción de un riesgo de corrupción deben poder identificarse los componentes anteriormente mencionados antecedidos por la expresión “posibilidad de”.

Ejemplo:

Riesgo de Corrupción	Componentes Riesgo de Corrupción	
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de autorizar alojamientos, viajes y/o transportes	Acción u Omisión	Recibir o solicitar
	Uso del Poder	Autorizar alojamientos, viajes y/o transportes
	Desviación de la Gestión de lo Público	Dádiva o beneficio
	Beneficio Privado	A nombre propio o de terceros

Tabla 4. Aspectos definición Riesgos de Corrupción.
Fuente: Adaptado de la Gruía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP.

5.2.2.3. Identificación riesgos de Seguridad de la Información

Identificación de Activos de Información

El primer paso para la determinar los riesgos de seguridad de la información es identificar los activos de información del proceso, de manera que se pueda establecer un inventario de activos de información de acuerdo con su criticidad; esto se realiza conforme lo establecido en el la Guía de Identificación, Actualización y Clasificación de Activos de Información.

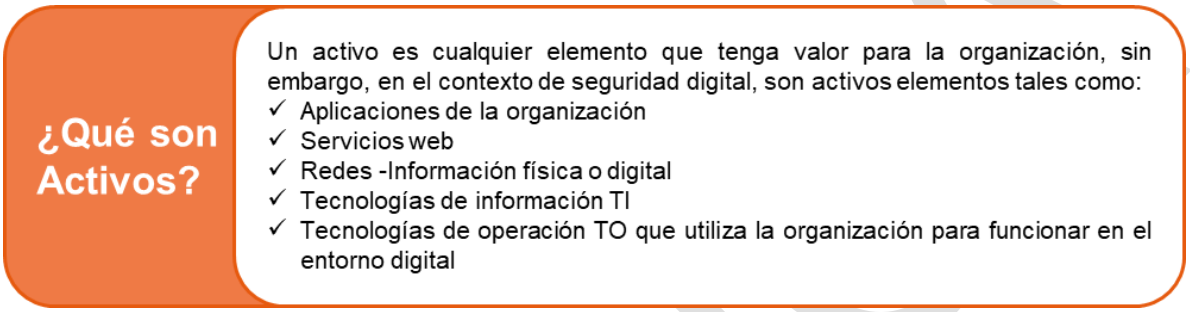

Figura 5. Activos de Información
Fuente: Adaptado de la Gruía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP.

Identificación de las Amenazas – Seguridad de la Información

Las amenazas representan situaciones o fuentes que pueden hacer daño a los activos de información. A continuación, se relacionan algunos ejemplos de las amenazas más comunes para tener en cuenta en la redacción del riesgo de seguridad de la información.

Tipo	Amenaza
Daño físico	Fuego
	Agua
	Contaminación
	Accidente Importante
	Destrucción del equipo o medios
	Polvo, corrosión, congelamiento
Eventos naturales	Fenómenos climáticos
	Fenómenos sísmicos
	Fenómenos volcánicos
	Fenómenos meteorológicos
	Inundación
Perdida de los servicios esenciales	Fallas en el sistema de suministro de agua o aire acondicionado
	Perdida de suministro de energía
	Falla en equipo de telecomunicaciones

Tipo	Amenaza
Perturbación debida a la radiación	Radiación electromagnética
	Radiación térmica
	Impulsos electromagnéticos
Compromiso de la información	Interceptación de señales de interferencia comprometida
	Espionaje remoto
	Escucha encubierta
	Hurto de medios o documentos
	Hurto de equipo
	Recuperación de medios reciclados o desechados
	Divulgación
	Datos provenientes de fuentes no confiables
	Manipulación con hardware
	Manipulación con software
	Detección de la posición
Fallas técnicas	Fallas del equipo
	Mal funcionamiento del equipo
	Saturación del sistema de información
	Mal funcionamiento del software
	Incumplimiento en el mantenimiento del sistema de información.
Acciones no autorizadas	Uso no autorizado del equipo
	Copia fraudulenta del software
	Uso de software falso o copiado
	Corrupción de los datos
	Procesamiento ilegal de datos
Compromiso de las funciones	Error en el uso
	Abuso de derechos
	Falsificación de derechos
	Negación de acciones
	Incumplimiento en la disponibilidad del personal
Dirigidas por el hombre	Pirata informático
	Intruso ilegal
	Ciber criminal
	Terrorismo
	Espionaje industrial
	Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)

Tabla 5. Identificación de Amenazas ambientales, deliberadas y por caso fortuito
Fuente: ISO 27005:2009

Identificación de las vulnerabilidades – Seguridad de la Información

Las vulnerabilidades son conocidas como la debilidad que tiene un activo de información, la cual al ser conocida puede ser explotada por una o más amenazas. A continuación, se relacionan las posibles vulnerabilidades de acuerdo con su tipo.

TIPO	VULNERABILIDAD
Hardware	Mantenimiento insuficiente
	Instalación fallida de los medios de almacenamiento
	Ausencia de esquemas de reemplazo periódico
	Susceptibilidad a la humedad, el polvo y la suciedad
	Sensibilidad a la radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración
	Susceptibilidad a las variaciones de voltaje
	Susceptibilidad a las variaciones de temperatura
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Defectos bien conocidos en el software
	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Ausencias de pistas de auditoria
	Asignación errada de los derechos de acceso
	Software ampliamente distribuido
	En términos de tiempo utilización de datos errados en los programas de aplicación
	Interfaz de usuario compleja
	Ausencia de documentación
	Configuración incorrecta de parámetros
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autentificación, como la autentificación de usuario
	Tablas de contraseñas sin protección
	Gestión deficiente de las contraseñas
	Habilitación de servicios innecesarios
	Software nuevo o inmaduro
	Especificaciones incompletas o no claras para los desarrolladores

TIPO	VULNERABILIDAD
	Ausencia de control de cambios eficaz
	Descarga y uso no controlado de software
	Ausencia de copias de respaldo
	Ausencia de protección física de la edificación, puertas y ventanas
	Fallas en la producción de informes de gestión
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Tráfico sensible sin protección
	Conexión deficiente de los cables
	Punto único de fallas
	Ausencia de identificación y autentificación de emisor y receptor
	Arquitectura insegura de la red
	Transferencia de contraseñas en claro
	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)
	Conexiones de red pública sin protección
Personal	Ausencia del personal
	Procedimientos inadecuados de contratación
	Entrenamiento insuficiente en seguridad de la información
	Uso incorrecto de software y hardware
	Falta de conciencia acerca de la seguridad de la información
	Ausencia de mecanismos de monitoreo
	Trabajo no supervisado del personal externo o de limpieza
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
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)
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Ausencia de proceso formal para la revisión de los derechos de acceso
	Ausencia de disposición en los contratos con clientes o terceras partes (con respecto a la seguridad)
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de la información
	Ausencia de auditorias
	Ausencia de procedimientos de identificación y valoración de riesgos
	Ausencia de reportes de fallas en los registros de administradores y operadores
	Respuesta inadecuada de mantenimiento del servicio
	Ausencia de acuerdos de nivel de servicio o insuficiencia de los mismos

TIPO	VULNERABILIDAD
	Ausencia de procedimientos de control de cambios
	Ausencia de procedimiento formal para la documentación del SGSI
	Ausencia de procedimiento formal para la supervisión del registro del SGSI
	Ausencia de procedimiento formal para la autorización de la información disponible al público
	Ausencia de asignación adecuada de responsabilidades en seguridad de la información
	Ausencia de planes de continuidad
	Ausencia de políticas sobre el uso de correo electrónico
	Ausencia de procedimientos para la instalación de software en los sistemas operativos
	Ausencia de registros en bitácoras
	Ausencia de procedimientos para el manejo de información clasificada
	Ausencia de responsabilidad en seguridad de la información en la descripción de los cargos y/o contratos
	Ausencia de los procesos disciplinarios definidos en caso de incidentes de seguridad de la información
	Ausencia de política formal sobre la utilización de computadores portátiles
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de política sobre limpieza de escritorio y pantalla
	Ausencia de autorización de los recursos de procesamiento de información
	Ausencia de mecanismos de monitoreo establecidos para las brechas en seguridad
	Ausencia de revisiones regulares por parte de la dirección
	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales.

Tabla 6. Activos, vulnerabilidades y Amenazas.
Fuente: ISO 27005:2009

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:

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

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión y congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	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

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
	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
	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
PERSONAL	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 FISICO (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

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
	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
	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

Tipo de Activo	Ejemplos de Vulnerabilidades	Ejemplos de Amenazas
	Ausencia de procedimientos de cumplimiento de las disposiciones con los derechos intelectuales	Uso de software falsificado o copiado

Tabla 7. Ejemplos de relación entre vulnerabilidades de acuerdo con el tipo de activos y las amenazas.
Fuente: ISO/IEC 27005:2009

5.2.2.4. 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 mejora la naturaleza del mismo y así enfoquen su gestión. En la siguiente tabla se definen las categorías:

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.
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.
LA/FT	Pérdida o daño que puede sufrir la Entidad por ser utilizada como instrumento para el Lavado de Activos y el Financiación del Terrorismo.
Seguridad de la Información	Amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Tabla 8. Categorias de riesgos.
Fuente: Adaptado de la Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

5.2.3. Valoración de Riesgos

Esta etapa de la gestión de riesgos consiste en calcular el nivel de riesgo de la entidad, iniciando con el establecimiento de la probabilidad de ocurrencia, así como el nivel de impacto que tendría en la

entidad 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, Fiscales, LA/FT y de Seguridad de la Información

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:

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 24 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%

Tabla 9. Criterios de Probabilidad Riesgos de Gestión, Fiscales, LA/FT y de Seguridad de la Información
Fuente: Guía para la Administración del riesgo y el diseño de Controles en Entidades Públicas. DAFP

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:

Nivel	Afectación Económica	Afectación Reputacional	Peso Porcentual (%)
Leve	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización	20%
Menor	Entre 11 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, 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%

Tabla 10. Criterios de Impacto Gestión, Fiscales, LA/FT y de Seguridad de la Información
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.

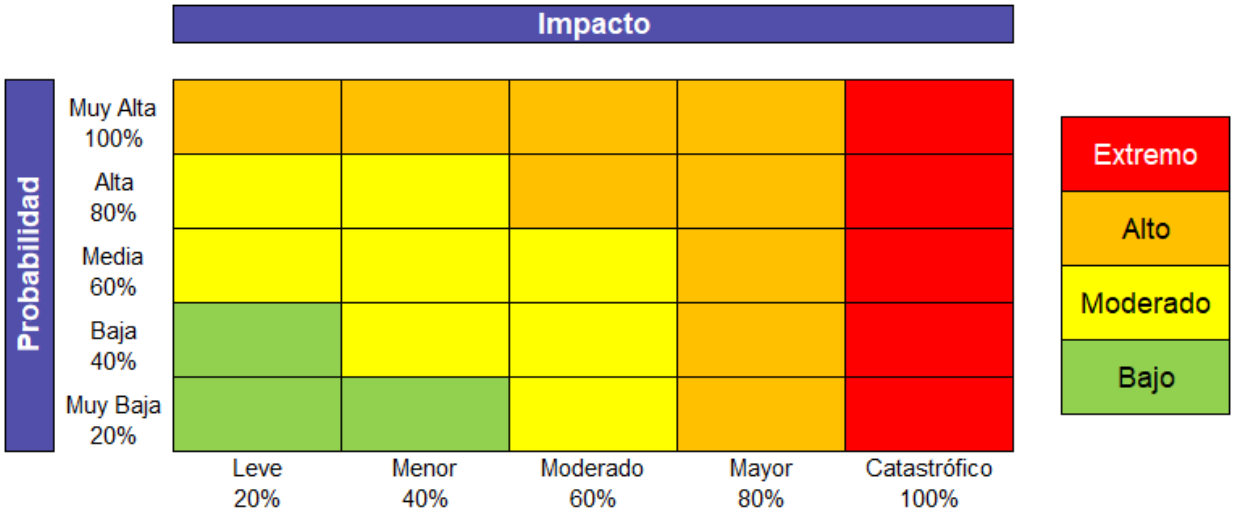

Figura 6. Mapa de Calor Riesgos de Gestión, Fiscales, LA/FT y de Seguridad de la Información
Fuente: *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP*

Ejemplo análisis de riesgos de gestión, fiscales, LA/FT y de Seguridad de la Información

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: la actividad se realiza 120 veces al año, a razón de 10 contratos mensuales.	**Media 60%**

Impacto: de llegar a materializarse, tendría una afectación económica de 500 SMLMV.	**Mayor 80%**

Tabla 11. Ejemplo análisis de riesgo
Fuente: Adaptado de la Guía para la Administración de los Riesgos y el Diseño de Controles 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:

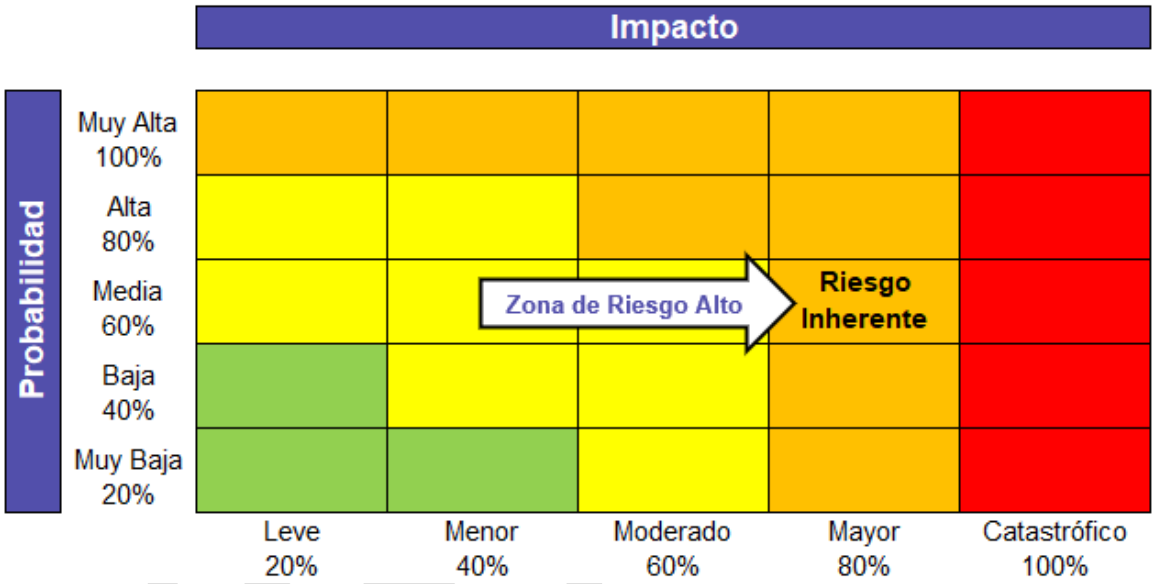

Figura 7. Ejemplo calificación nivel riesgo inherente. Elaboración propia.

Análisis de Riesgos de Corrupción

Determinar la Probabilidad

Teniendo en cuenta la particularidad de los riesgos de corrupción, su probabilidad se estimará basándose en la frecuencia o factibilidad de ocurrencia de este, entendiendo la frecuencia como el número de eventos de materialización registrados en un periodo determinado, y la factibilidad será la posibilidad de que llegase a ocurrir un evento de materialización teniendo en cuenta el análisis de factores tanto interno como externos.

Para estimar la probabilidad de un riesgo de corrupción se emplea la siguiente escala de medición:

Nivel	Probabilidad de Ocurrencia	Descripción	Frecuencia
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años

3	Posible	El evento podrá ocurrir en cualquier momento	Al menos 1 vez en los últimos 2 años
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año

Tabla 12. Criterios de Probabilidad Riesgos de Corrupción
Fuente: Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

Determinar el Impacto

Para determinar el impacto de los riesgos de corrupción se cuantifica a partir de las respuestas afirmativas a las siguientes preguntas.

No	Pregunta: Si el riesgo de corrupción se materializa…	Respuesta	
		SI	NO
1	¿Afecta al grupo de funcionarios del proceso?		
2	¿Afecta el cumplimiento de las metas y objetivos de la dependencia?		
3	¿Afecta el cumplimiento de la misión de la entidad?		
4	¿Afecta el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Genera pérdida de confianza en la entidad, afectando su reputación?		
6	¿Genera pérdida de recursos económicos?		
7	¿Afecta la generación de los productos o la prestación de servicios?		
8	¿Da lugar al detrimento de la calidad de vida de la comunidad por la pérdida del bien o servicio, o recurso público?		
9	¿Genera pérdida de información de la entidad?		
10	¿Genera intervención de los órganos de control, de la fiscalía, u otro ente?		
11	¿Da lugar a procesos sancionatorios?		
12	¿Da lugar a procesos disciplinarios?		
13	¿Da lugar a procesos Fiscales?		
14	¿Da lugar a procesos penales?		
15	¿Genera pérdida de credibilidad en el sector?		
16	¿Ocasiona lesiones físicas o pérdida de vidas humanas?		
17	¿Afecta la imagen regional?		
18	¿Afecta la Imagen nacional?		
19	¿Genera daño ambiental?		

Tabla 13. Criterios de Impacto Corrupción
Fuente: Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

Importante: *Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico. Por cada riesgo de corrupción identificado, se debe diligenciar una tabla de estas.*

El impacto para los riesgos de corrupción se establece en la Matriz de Riesgos, de acuerdo con el número de respuestas afirmativas frente a las 19 preguntas mencionadas anteriormente, según los siguientes criterios:

CRITERIO	CALIFICACIÓN
Moderado	0-5
Mayor	6-11
Catastrófico	12-19

Tabla 14. Criterios calificación impacto Riesgos de Corrupción.
Fuente: Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

Tratándose de riesgos de corrupción el impacto siempre será altamente negativo; en este orden de ideas, **no aplica la calificación de impacto leve y menor**.

Nivel de Riesgo Inherente Riesgos de Corrupción

El nivel de riesgo Inherente (antes de aplicar controles) se puede calcular como la relación entre la probabilidad y el impacto, ya que a través del cruce de estas variables se obtiene la ubicación en la matriz de calor, la cual dependiendo de su ubicación en una de las 3 zonas indicara la clasificación del nivel de riesgo, el cual está asociado a la severidad de este. A continuación, se presentan el mapa de calor.

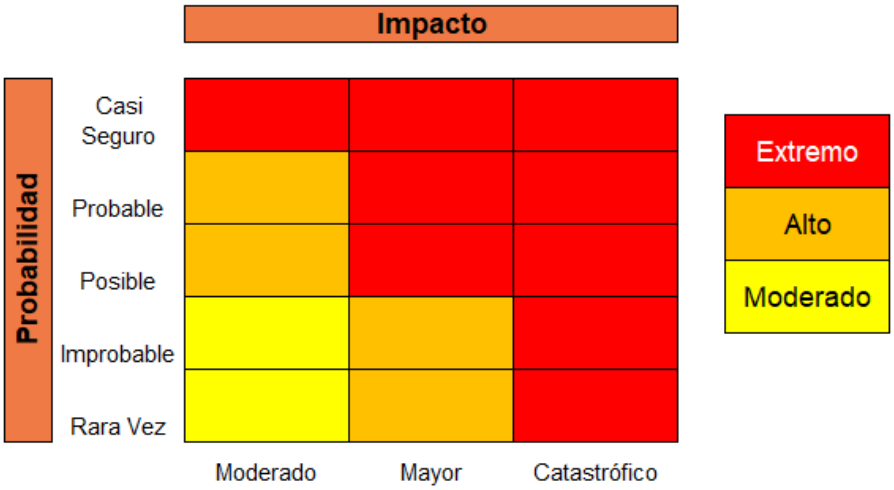

Figura 8. Mapa de Calor Riesgos de Corrupción
Fuente: *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP*

Ejemplo Análisis de Riesgos de Corrupción

Riesgo: Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de beneficiar o girar recursos adicionales sin el debido cumplimiento de obligaciones a Instituciones de Educación Superior u Operadores.	
Probabilidad: se estableció que el nivel de probabilidad del riesgo es "Improbable", lo cual nos indica que el evento podrá ocurrir en algún momento, o que ha ocurrido al menos una vez en los últimos 5 años.	Improbable

Impacto: Después de contestar las preguntas se obtuvo respuestas afirmativas en 8 de ellas lo cual nos ubica en un impacto mayor.	Mayor

Tabla 15. Ejemplo análisis de riesgo de corrupción
Fuente: Adaptado de la Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

Con base en esta en la valoración de probabilidad e impacto se procede a ubicar el riesgo en el mapa de calor, lo cual lo ubica en la segunda fila (de abajo hacia arriba) y la segunda columna, correspondientes a una calificación de probabilidad “Improbable” y un impacto “Mayor” quedando así en un nivel de riesgo “Alto”, como se muestra a continuación:

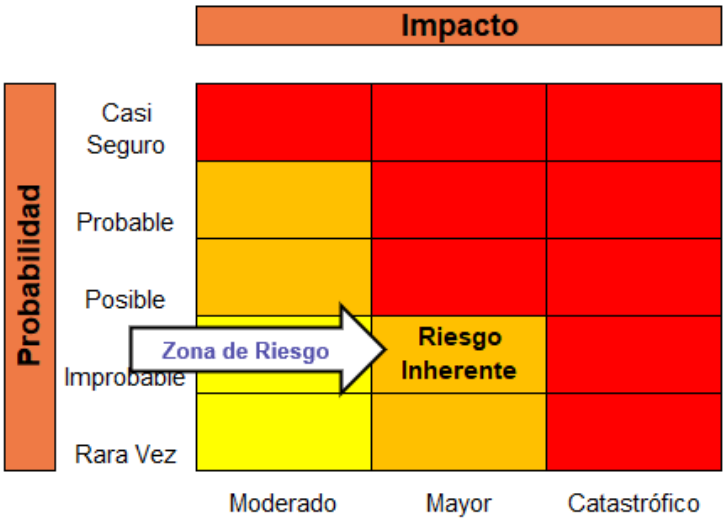

Figura 9. Ejemplo calificación nivel de riesgo de corrupción inherente. Elaboración propia.

5.2.3.2. Evaluación de Riesgos

Evaluación de Riesgos de Gestión, Fiscales y LA/FT

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.

Ejemplo redacción de un 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.*

Tabla 16. Ejemplo redacción de control
Fuente: Adaptado de la Guía para la Administración de los Riesgos y el Diseño de Controles 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 que momento del ciclo de procesos se aplica el control, lo cual permite identificar que tipo de control es y de que 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 aplicado por un sistema o aplicativo sin la necesidad que intervengan personas.

Atributos Informativos: 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.

- **Evidencia:** indica si se guarda registro de la aplicación del control.

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:

Tipo de Atributo	Características		Peso
Eficiencia	**Tipo**	*Preventivo*	20%
		Detectivo	15%
		Correctivo	10%
	Implementación	*Automático*	20%
		Manual	15%
Informativo	**Documentación**	*Documentado*	10%
		Sin Documentar	0%
	Evidencia	*Con Registro*	5%
		Sin Registro	0%

Tabla 17. Ponderación Atributos de Eficiencia
Fuente: Adaptado de la Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

Ejemplo calificación de un control:

Control	Características del Control			Peso
Control 1	**Tipo**	Preventivo		
		Detectivo	X	15%
		Correctivo		
	Implementación	Automático	X	20%
		Manual		
	Documentación	Documentado	X	10%
		Sin Documentar		
	Evidencia	Con Registro	X	5%

		Sin Registro		
Total Valoración del Control				**50%**

Tabla 18. Calificación de Controles. Elaboración propia.

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:

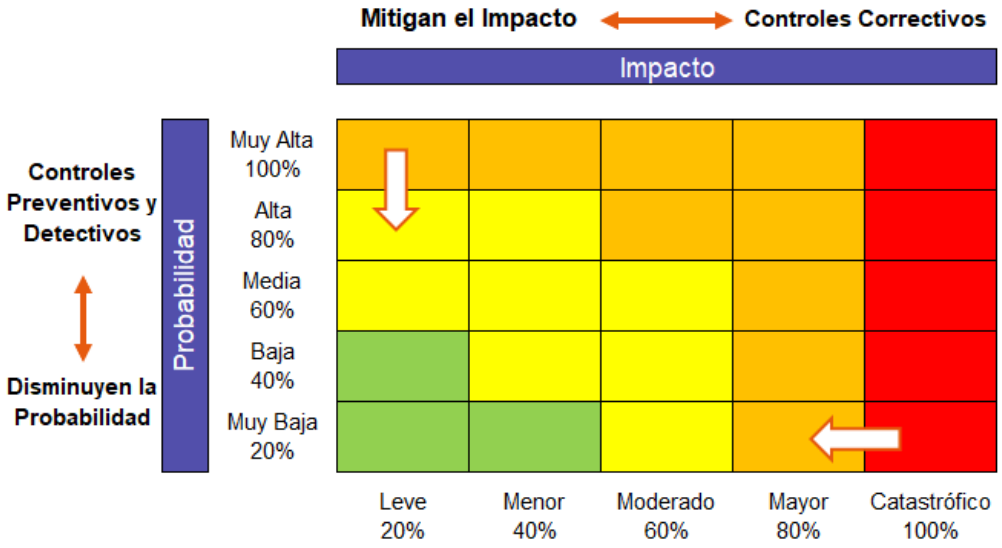

Figura 8. Movimiento en la Matriz de Riesgos Acorde al Tipo de Control
Fuente: *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP*

Nivel de Riesgo Residual

El nivel de riesgo residual corresponde con 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.

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	30%	36%*45% = 16.2% 36% - 16.2% = **19.8%**

			Detectivo – Manual – Documentado – Con Registro		
	Probabilidad Residual				**19.8%**
	Impacto Inherente	80%	NA	NA	NA
	Impacto Residual				**80%**

Tabla 19. Ejemplo Calificación Nivel de Riesgo Residual
Fuente: Adaptado de la Guía para la Administración de los Riesgos y el Diseño de Controles 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:

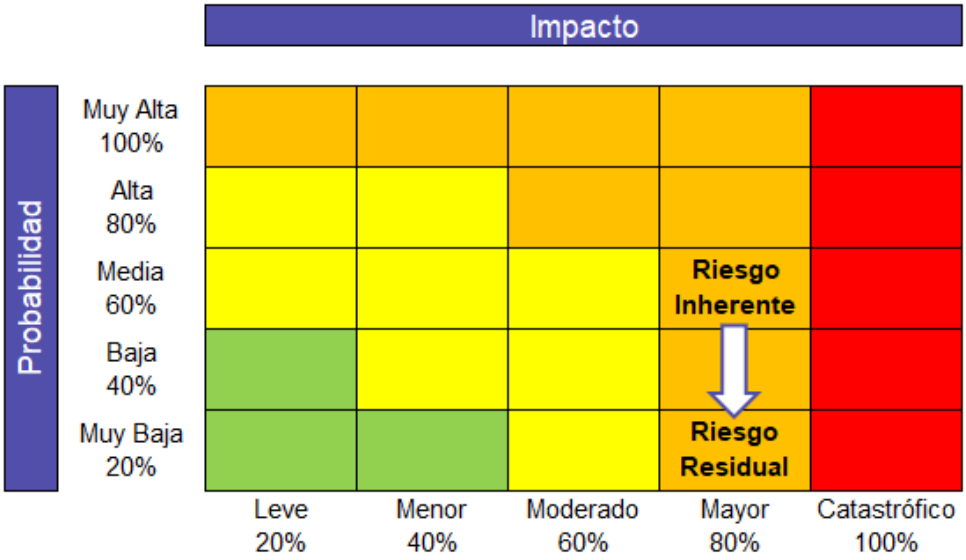

Figura 9. Ejemplo Riesgo Inherente. Elaboración propia.

Como se observa a partir de la aplicación de los dos controles el riesgo bajo su probabilidad en dos niveles pasando de “Media” a “Muy Baja”.

Evaluación de Riesgos de Corrupción

Identificación de Controles

La identificación de controles asociados a los riesgos de corrupción se debe realizar de acuerdo con lo descrito en el Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas del DAFP en su versión 4 de 2018, donde se establece la estructura que debe tener la descripción de estos, la cual debe incluir los criterios de diseño y ejecución, como se muestra a continuación:

Figura 10. Estructura para Describir Controles Asociados a Riesgos de Corrupción
Fuente: Adaptado de la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. DAFP*

Ejemplo de descripción de controles asociados a riesgos:

El profesional de central de cuentas mensualmente valida los requisitos para el trámite de pagos, verificando los soportes recibidos conforme a los lineamientos para la ejecución financiera y presupuestal generando la cuenta por pagar y obligación, en caso de evidenciar inconsistencias se devuelve al supervisor, la evidencia de esto reposa en el gestor documental de la entidad.	***Responsable:*** *profesional de central de cuentas*
	Periodicidad: *mensualmente.*
	Propósito: *validar los requisitos para el tramite de pagos.*
	Como se Realiza: *verificando los soportes recibidos conforme a los lineamientos para la ejecución financiera y presupuestal generando la cuenta por pagar y obligación*
	Observaciones y/o Desviaciones: *en caso de evidenciar inconsistencias se devuelve la solicitud al supervisor.*
	Evidencia: *a gestión documentada a través del gestor documental.*

Tabla 20. Ejemplo redacción de control asociado a riesgos de corrupción.
Fuente: Adaptado de la Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

Valoración de Controles Asociados a Riesgos de Corrupción

Para realizar la calificación de los controles asociados a los riesgos de corrupción se tendrán en cuenta los criterios establecidos al momento de su identificación, a través de los cuales se podrá establecer su peso en la gestión del riesgo como se muestra en la Tabla 19.

Criterio	Aspectos a Evaluar en el Diseño Del Control	Opciones De Respuesta Y Peso En La Evaluación
1. Responsable	**¿Existe un responsable asignado a la ejecución del control?**	ASIGNADO = 15
		NO ASIGNADO = 0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	ADECUADO = 15
		INADECUADO = 0
2. Periodicidad	**¿La oportunidad en que se ejerce el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riego de manera oportuna?**	OPORTUNA = 15
		INOPORTUNA = 0
3. Propósito	**¿Las actividades que se desarrollan en el control realmente buscan por si solas prevenir o detectar las causas que pueden dar origen al riesgo? ejemplo: Verificar, Validar, Cotejar, Comparar, Revisar, etc.**	DETECTAR = 10
		PEVENIR = 15
		NO ES UN CONTROL = 0
4. Como se Realiza la Actividad de Control	**¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?**	CONFIABLE = 15
		NO CONFIABLE = 0

Criterio	Aspectos a Evaluar en el Diseño Del Control	Opciones De Respuesta Y Peso En La Evaluación
5. Que pasa con las Observaciones o Desviaciones	**¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?**	SE INVESTIGAN Y RESUELVEN OPORTUNAMENTE = 15
		NO SE INVESTIGAN Y RESUELVEN OPORTUNAMENTE = 0
6. Evidencia de la Ejecución del Control	**¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?**	COMPLETA = 10
		INCOMPLETA = 5
		NO EXISTE = 0

Tabla 21. Criterios de Diseño Controles Asociados a Riesgos de Corrupción
Fuente: Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

Para establecer la calificación del diseño de un control se deben sumar los pesos asignados a cada aspecto, y dependiendo del resultado de esta operación matemática según las siguiente escala se establecerá la fortaleza del diseño del control.

Calificación del Diseño de Control	Rangos de Calificación Cuantitativa del Diseño del Control
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Tabla 22. Rangos de Clasificación Criterios de Diseño Controles Asociados a Riesgos de Corrupción
Fuente: Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

Una vez establecida la calificación del diseño de un control asociado a un riesgo de corrupción se debe evaluar su ejecución para determinar si el control se aplica en el transcurso normal de las actividades de acuerdo con los criterios establecidos. Para realizar la medición de la ejecución de los controles se definen las siguientes categorías:

- **Fuerte:** El control se ejecuta de manera consistente por parte del responsable.
- **Moderado:** El control se ejecuta algunas veces por parte del responsable.
- **Débil:** El control no se ejecuta por parte del responsable.

Finalmente, para determinar la solidez del control se debe establecer la relación entre las calificaciones de diseño y ejecución del control según la siguiente tabla:

Calificación Diseño	Calificación Ejecución	Solidez Individual de Cada Control
Fuerte Calificación entre 96 y 100	Fuerte (siempre se ejecuta)	Fuerte + Fuerte = Fuerte (100)
	Moderado (se ejecuta algunas veces)	Fuerte + Moderado = Moderado (50)
	Débil (no se ejecute)	Fuerte + Débil = Débil (0)

Moderado Calificación entre 86 y 95	Fuerte (siempre se ejecuta)	Moderado + Fuerte = Moderado (50)
	Moderado (se ejecuta algunas veces)	Moderado + Moderado = Moderado (50)
	Débil (no se ejecute)	Moderado + Débil = Débil (0)
Débil Calificación entre 0 y 85	Fuerte (siempre se ejecuta)	Débil + Fuerte = Débil (0)
	Moderado (se ejecuta algunas veces)	Débil + Moderado = Débil (0)
	Débil (no se ejecute)	Débil + Débil = Débil (0)

Tabla 23. Criterios de Calificación Solidez de Controles Asociados a Riesgos de Corrupción
Fuente: Adaptado de la Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

Nivel de Riesgo Residual para Riesgos de Corrupción

Para determinar el nivel de riesgo residual de un riesgo de corrupción es necesario establecer la solidez del conjunto de controles asociados a este, el cual se calcula como el promedio de las calificaciones de la solidez individual de los controles. Además, dependiendo de esta calificación se definirá si se requieren acciones para fortalecer el conjunto de controles.

Solidez Conjunto de Controles	Rangos de Clasificación Solidez Conjunto de Controles	Acciones
Fuerte	**El promedio de la solidez individual es igual a 100.**	El conjunto de controles mitiga el riesgo y no requieran acciones adicionales para su fortalecimiento
Moderado	**El promedio de la solidez individual esta entre 50 y 99.**	El conjunto de controles mitiga parcialmente el riesgo, sin embargo, se requieren acciones adicionales para fortalecer los controles.
Débil	**El promedio de la solidez individual es menor a 50.**	El conjunto de controles no mitiga el riesgo, se requiere tomar revisar su viabilidad y tomar acciones para su fortalecimiento o implementar nuevos controles.

Tabla 24. Calificación Solidez Conjunto de Controles Asociados a Riesgos de Corrupción
Fuente: Adaptado de la Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

Dependiendo de la calificación de la solidez del conjunto de controles, para determinar el riesgo residual se debe ubicar el nivel de riesgo inherente en el mapa de calor y desplazarlo de acuerdo a los siguientes criterios:

Solidez del conjunto de controles Fuerte: disminuye la probabilidad de ocurrencia del riesgo de corrupción en dos (**2**) niveles, con lo cual el riesgo se desplaza dos filas en el eje de probabilidad.

Solidez del conjunto de controles Moderada: disminuye la probabilidad de ocurrencia del riesgo de corrupción en un (**1**) nivel, con lo cual el riesgo se desplaza una fila en el eje de probabilidad.

Solidez del conjunto de controles Débil: no disminuye la probabilidad de ocurrencia del riesgo de corrupción, la calificación de Riesgo Inherente es igual a la del Riesgo Residual.

Nota: *Al tratarse de riesgos de corrupción, sus controles asociados únicamente mitigan su probabilidad de ocurrencia.*

Ejemplo Calificación de Riesgo Residual de los Riesgo de Corrupción

Riesgo: Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de beneficiar o girar recursos adicionales sin el debido cumplimiento de obligaciones a Instituciones de Educación Superior u Operadores.		
Probabilidad: se estableció que el nivel de probabilidad del riesgo es "Improbable", lo cual nos indica que el evento podrá ocurrir en algún momento, o que ha ocurrido al menos una vez en los últimos 5 años.		Improbable
Impacto: Después de contestar las preguntas se obtuvo respuestas afirmativas en 8 de ellas lo cual nos ubica en un impacto mayor.		Mayor
Control 1	Calificación Diseño del Control:	Fuerte (100)
	Calificación Ejecución del Control:	Fuerte
	Calificación Solidez Individual Control 1	Fuerte (100)
Control 2	Calificación Diseño del Control:	Moderado (90)
	Calificación Ejecución del Control:	Moderado
	Calificación Solidez Individual Control 2:	Moderado (50)
CALIFICACIÓN SOLIDEZ CONJUNTO DE CONTROLES		**Moderado (75)**

Tabla 25. Ejemplo Calificación Nivel de Riesgo Residual para Riesgos de Corrupción
Fuente: Adaptado de la Guía para la Administración de los Riesgos y el Diseño de Controles en Entidades Públicas. DAFP

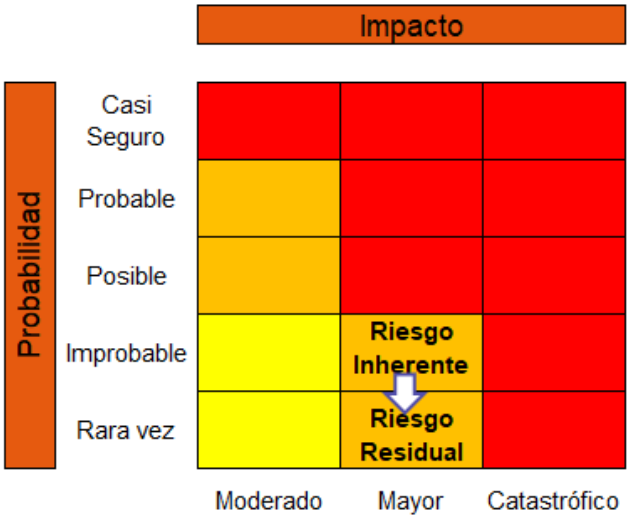

Figura 9. Ejemplo Riesgo de Corrupción Inherente. Elaboración propia.

Controles Asociados a Riesgos de Seguridad de la Información

En cuanto a la identificación y selección de controles asociados a los riesgos de seguridad de la información, se deben tener en cuenta los definidos en la ISO 27001, los cuales se encuentran descritos en el Anexo No. 2 de este documento.

5.2.4. Tratamiento de Riesgos

Una vez completada la valoración de los riesgos, estos deben ser tratados de acuerdo con el nivel de riesgo residual obtenido una vez aplicados los controles existentes.

Cuando el nivel de riesgo residual de un riesgo sea **moderado**, **alto** o **extremo**, el **líder de proceso deberá definir e implementar estrategias para realizar el tratamiento de este**; lo anterior no quiere decir que los riesgos en nivel bajo no se gestionen ya que sobre estos deberá realizarse seguimiento tanto a su materialización como a la ejecución de sus controles por lo que permanecerán en la matriz de riesgos del proceso. Para riesgos LA/FT el nivel de riesgo residual siempre se deberá aceptar[2].

Para realizar el tratamiento de riesgos se podrán emplear tres estrategias, las cuales son:

Aceptar: después de concluir el análisis y la evaluación del riesgo se determina, que este será asumido conociendo los efectos de su posible materialización. Esta estrategia de tratamiento únicamente aplica para los riesgos con un nivel de riesgo residual "Bajo" de acuerdo con la Política de Gestión de Riesgos y el apetito de riesgo definidos por la entidad.

Evitar: consiste en dejar de realizar o eliminar la actividad a partir de la cual se genera el riesgo (Punto de Riesgo), con lo cual se elimina la posibilidad de ocurrencia de la materialización de este.

Reducir: esta estrategia consiste en gestionar acciones que permitan disminuir la probabilidad de ocurrencia y el impacto de la materialización del riesgo. En el marco de la estrategia de reducción se definen dos caminos:

- **Transferir:** consiste en trasladar el riesgo a un tercero, ya sea mediante la tercerización de las actividades que generan el riesgo o mediante pólizas de seguro que mitiguen el impacto de una posible materialización. Esta estrategia únicamente transfiere el impacto económico del riesgo, por lo que no aplica para riesgos con impacto reputacional.

- **Mitigar:** Esta estrategia se fundamenta en implementar acciones disminuir el nivel de riesgo residual. En el marco de esta estrategia se debe establecer un plan de tratamiento de riesgos

[2] Por la naturaleza del riesgo LA/FT sin importar el nivel de riesgo residual que quede luego de la valoración de este, todas las situaciones relacionadas con vinculación de las contrapartes deberán ser "Aceptadas" puesto que no hay ninguna medida adicional para tratar esta situación y la materialización del mismo dependerá de una decisión externa de índole judicial.

que contemple: actividades a desarrollar, responsables, fechas de compromiso, y registro o evidencias de su realización. En la implementación de esta estrategia se pueden presentar dos escenarios:

- ***Implementar nuevos controles:*** *consiste en definir y poner en marcha nuevos controles para reducir el nivel de riesgo, a través de un plan de trabajo a desarrollar durante la vigencia, al final de la cual estos nuevos controles pasaran a hacer parte de los controles existentes y ser analizados en la etapa de evaluación de riesgos.*

- ***Plan de tratamiento para la mitigación del riesgo:*** *bajo el precepto que algunos riesgos por su naturaleza y características no pueden reducirse más, por ejemplo, riesgos con alto impacto y una probabilidad muy baja para los que no se puedan definir controles de tipo correctivo, o riesgos de corrupción con probabilidad "Rara Vez", se podrán definir un plan de tratamiento que contemple acciones complementarias a los controles que contribuyan a evitar la materialización del riesgo*.

5.2.5. 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 Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP. V6.

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, incluyendo los riesgos de corrupción, 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 las áreas auditadas.
- 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 y apoyo en la identificación, análisis, evaluación y tratamiento de los riesgos, y realizar monitoreo al cumplimiento de las etapas 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 evitar en lo posible que se vuelva a materializar el riesgo.

Líder de proceso:

- 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.
- 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 el cumplimiento de los objetivos de sus procesos, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- 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.

Subgerencia de Tecnologías de Información y Comunicaciones – TICs

Será la responsable de realizar seguimiento a la gestión de riesgos de seguridad de la información 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 de la Información.
- Una vulnerabilidad y/o amenaza no tratada adecuadamente.

Responsabilidades de las líneas de defensa para la gestión de riesgos LA/FT

Primera línea (Gestión de los líderes de proceso respecto a la operación)

Para la gestión de riegos LAFT la primera línea de defensa estará orientada a la identificación de señales de alerta y comportamientos claves para determinar situaciones que se puedan entender como

potencialmente peligrosas para la Entidad, en cuanto a la vinculación de contrapartes que puedan estar asociadas a cadenas de Lavado de Activos y Financiación del Terrorismo.

Segunda línea (De la gestión de riesgos de cumplimiento)

La segunda línea está en cabeza del administrador del sistema (gestor de cumplimiento) será la persona encargada de validar, contrastar y verificar la información identificada desde la primera línea. El gestor de cumplimiento será el responsable de diseñar, implementar y ejecutar los controles necesarios para prevenir y proteger a la entidad de eventos asociados al Lavado de Activos y la Financiación del Terrorismo.

Tercera línea (De la gestión de la Oficina de Control Interno)

Las funciones de la tercera línea para la gestión de riesgos LAFT, estarán orientadas a validar que lo que se hace en gestión de controles e identificación de amenazas concuerden con lo descrito en los documentos de la operación. Adicionalmente, estará encargada de validar y velar porque todos los reportes que sea hagan a entes externos (UIAF) se hagan en las condiciones de información idóneas que se requieren.

En cualquier etapa de revisión de los riesgos, el Líder del Proceso puede solicitar la modificación, eliminación o inclusión de riesgos. Esta solicitud la debe realizar a la Subgerencia de Planeación a través de correo electrónico adjuntando el Formato Control de Cambios en la Gestión de Riesgos debidamente diligenciado y firmado. Todas las solicitudes serán consolidadas por la Subgerencia de Planeación y las relacionadas con los riesgos de corrupción deberán ser presentadas por el Líder del Proceso en el Comité Institucional de Gestión y Desempeño.

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.

Las matrices de riesgos de gestión y corrupción se encuentran publicadas en la carpeta de Gestión del Proceso, del Mapa de Procesos y se pueden consultar a través de la página web; la matriz de riesgos de Corrupción consolidada se puede consultar en el botón de transparencia de la página web de la Entidad, las matrices de riesgos fiscales y LA/FT se conserva en las carpetas compartidas de la Subgerencia de Planeación y la matriz de riesgos de seguridad de la información se puede consultar en las carpetas compartidas de la Subgerencia de TICs.

5.4. Registro y reporte de incidentes - Seguridad de la información

Es importante contar con el registro de los incidentes de seguridad de la información que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las

pérdidas que se pueden generar, el propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles, conforme a lo definido en la Guía de Gestión de Incidentes de Seguridad de la Información definida en la entidad.

6. ANEXOS

- Anexo No. 1: Contexto de procesos

- Anexo No. 2: Identificación y selección de controles en los riesgos de seguridad de la información, según la Norma ISO 27001.

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 administración del riesgo y el diseño de controles en entidades públicas, Versión 6, Dirección de Gestión y Desempeño Institucional. Departamento Administrativo de la Función Pública, Noviembre de 2022.
- Documento Técnico- Adaptación de medidas de prevención y mitigación del riesgo del | de activos, financiación del terrorismo en las entidades del Distrito Capital, Diciembre de 2022.
- 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 de gestión, Seguridad de la Información y LA/FT
F2_G1_DE	Matriz de riesgos de Corrupción

9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
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.

Nota: *Una vez se diligencie el presente formato, recuerde borrar las instrucciones de diligenciamiento.*

VALIDACIÓN	NOMBRE	CARGO	FECHA
Elaboró	Diana María Vargas Barón Cristina Mahecha Parra Andres Felipe Rodríguez Plazas María Alejandra del Pilar Suárez Rojas	Profesionales contratista Subgerencia de Planeación Profesional contratista Subgerencia de Tecnologías de la Información y las Comunicaciones	19/07/2024
Revisó	Ana maría García Cañadulce	Profesional contratista Subgerente de Planeación	19/07/2024
Aprobó	Ximena Pardo Peña	Subgerente de Planeación	19/07/2024

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 procedimientos 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:

1.3.1 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, se cuenta con 15 procesos, los cuales 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.

1.3.2 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 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.

1.3.3 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, 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 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.

1.3.4 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 de Documentos 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 de Documentos 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.

1.3.5 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 de los 15 procesos que se han mencionado.

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 del cual se realizó la definición y actualización de 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 en los diferentes niveles de 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, para cada uno de los procesos.

1.3.6 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-, interactúen 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 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 a partir de las entradas y de la finalización y cumplimiento de las mismas 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

Dominio	Objetos de Control	Objetivo	Control
POLITICA DE SEGURIDAD			
A.5 Política de Seguridad de la Información	**A.5.1 - Orientación de la dirección para la gestión de la Seguridad de la Información**	Brindar orientación y soporte, por parte de la dirección, para la Seguridad de la Información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes	A.5.1.1 Política para la Seguridad de la Información
			A.5.1.2 Revisión de las políticas para la Seguridad de la Información
ORGANIZACIÓN SEGURIDAD DE LA INFORMACIÓN			
A.6 Organización en la Seguridad de la Información	**A.6.1 - Organización Interna**	Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de Seguridad de la Información dentro de la organización	A.6.1.1 - Roles y responsabilidades para la Seguridad de la Información
			A.6.1.2 - Separación de Deberes
			A.6.1.3 - Contacto con las autoridades
			A.6.1.4 - Contacto con grupos de interés
			A.6.1.5 Seguridad de la Información en la gestión de proyectos
	A.6.2 - Dispositivos Móviles y teletrabajo	Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles	A.6.2.1 - Política para dispositivos móviles
			A.6. 2..2 - Teletrabajo
SEGURIDAD DE LOS RECURSOS HUMANOS			
	A.7.1 - Antes de asumir el empleo	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos	A.7.1.1 - Selección

Dominio	Objetos de Control	Objetivo	Control
A.7 Seguridad de los Recursos Humanos		en los roles para los que se consideran.	A.7.1.2 - Términos y condiciones del empleo
	A.7.2 - Durante la ejecución del empleo	Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la Información y las cumplan.	A.7.2.1-Responsabilidades de la dirección
			A.7.2.2-Toma de conciencia educación y formado en la seguridad de la Información
			A.7.2.3-Proceso disciplinario
	A.7.3 - Terminación y cambio de empleo	Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.	A.7.3.1-Terminación o cambio de responsabilidades de empleo
GESTION DE ACTIVOS			
A.8 Gestión de Activos	A.8.1 - Responsabilidad por los activos	Identificar los activos organizacionales y definir las responsabilidades de protección apropiados	A.8.1.1 - Inventario de activos
			A.8.1.2 - Propiedad de los activos
			A.8.1.3- Uso aceptable de los activos
			A.8.1.4- Devolución de activos
	A.8.2 - Clasificación de la Información	Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización	A.8.2.1- Clasificación de la información
			A.8.2.2- Etiquetado de la información
			A.8.2.3 - Manejo de activos
	A.8.3 - Manejo de Medios	Etiquetado modificaciones, retiro o la destrucción no autorizados de información almacenada en los medios.	A.8.3.1- Gestión de medios removibles
			A.8.3.2- Disposición de los medios
			A.8.3.3- Transferencia de medios físicos
CONTROL DE ACCESO			
A.9 Control de Acceso	A.9.1 - Requisitos del negocio para control de acceso	Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.1- Política de control de acceso
			A.9.1.2- Acceso a redes y a servicios en red
	A.9.2 - Gestión de acceso de usuarios	Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.	A.9.2.1-Registro y cancelación del registro de usuarios
			A.9.2.2- Suministro de acceso de usuarios
			A.9.2.3- Gestión de derechos de acceso privilegiado

Dominio	Objetos de Control	Objetivo	Control
			A.9.2.4- Gestión de información de autenticación secreta. La asignación de información de autenticación secreta se debe controlar por parte de los usuarios
			A.9.2.5- Revisión de los derechos de acceso de usuarios
			A.9.2.6- Retiro o ajuste de los derechos de acceso
	A.9.3 - Responsabilidades de los usuarios	Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.	A.9.3.1- Uso de información de Control autenticación secreta
	A.9.4 - Control de Acceso a sistemas y aplicaciones	Evitar el acceso no autorizado a sistemas y aplicaciones.	A.9.4.1- Restricción de acceso a la información
			A.9.4.2- Procedimiento de ingreso seguro
			A.9.4.3- Sistema de gestión de contraseñas
			A.9.4.4- Uso de programas utilitarios privilegiados
			A.9.4.5- Control de acceso a códigos fuente de programas
CRIPTOGRAFIA			
A.10 Criptografía	**A.10.1 - Controles Criptográficos**	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.	A.10.1.1- Política sobre el uso de controles criptográficos
			A.10.1.2- Gestión de llaves
SEGURIDAD FISICA Y DEL ENTORNO			
A.11 Seguridad Física y del Entorno	**A.11.1 - Áreas seguras**	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procedimientos de información de la organización	A.11.1 .1-Perimetro de seguridad física
			A.11 .1.2- Controles de acceso físicos
			A.11 .1.3- Seguridad de oficinas, recintos e instalaciones
			A.11 .1.4- Protección contra amenazas externas y ambientales
			A.11.1.5- Trabajo en áreas seguras
			A.11 .1.6- Áreas de despacho y carga
	A.11.2 - Equipos	Prevenir la pérdida, daño, robo o compromiso de activos, y la	A.11.2.1-Ubicación y protección de los equipos
			A.11.2.2-Servicios de suministro

Dominio	Objetos de Control	Objetivo	Control
		interrupción de las operaciones de la organización	A.11.2.3- Seguridad del cableado
			A.11.2.4-Mantenimiento de equipos
			A.11.2.5- Retiro de activos
			A.11.2.6- Seguridad de equipos y activos fuera de las instalaciones
			A.11.2.7- Disposición segura o reutilización de equipos
			A.11.2.8- Equipos de usuario desatendido
			A.11.2.9- Política de escritorio y pantalla limpios
SEGURIDAD DE LAS OPERACIONES			
A.12 Seguridad de las Operaciones	**A.12.1 - Procedimientos operacionales y responsabilidades**	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.1-Procedimientos de operación documentados
			A.12.1.2- Gestión de cambios
			A.12.1.3- Gestión de capacidad
			A.12.1.4- Separación de los ambientes de desarrollo, pruebas, y operación
	A.12.2 - Protección contra códigos maliciosos	Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	A.12.2.1- Controles contra códigos maliciosos
	A.12.3 - Copias de respaldo	Proteger contra la perdida de datos	A.12.3.1-Respaldo de la información
	A.12.4 - Registro y seguimiento	Registrar eventos y generar evidencia	A.12.4.1-Registro de eventos
			A.12.4.2- Protección de la información de registro
			A.12.4.3-Registros del administrador y del operador
			A.12.4.4- Sincronización de relojes
	A.12.5 - Control de software operacional	Asegurarse de la integridad de los sistemas operacionales	A.12.5.1-Instalación de software en sistemas operativos
	A.12.6 - Gestión de vulnerabilidad técnica	Prevenir el aprovechamiento de las vulnerabilidades técnicas	A.12.6.1- Gestión de las vulnerabilidades técnicas
			A.12.6.2- Restricciones sobre la instalación de software
	A.12.7 - Consideraciones sobre auditorias de sistemas de información	Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.	A.12.7- Controles de auditorías de sistemas de información
SEGURIDAD DE LAS COMUNICACIONES			

Dominio	Objetos de Control	Objetivo	Control
A.13 Seguridad de las Comunicaciones	A.13.1 - Gestión de la seguridad de redes	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A.13.1.1- Controles de redes
			A.13.1.2- Seguridad de los servicios de red
			A.13.1.3- Separación en las redes
	A.13.2 - Transferencia de información	Mantener la Seguridad de la Información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.1- Políticas y procedimientos de transferencia de información
			A.13.2.2- Acuerdos sobre transferencia de información
			A.13.2.3- Mensajera electrónica
			A.13.2.4- Acuerdos de confidencialidad o de no divulgación
ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas	A.14.1 - Requisitos de seguridad de los sistemas de información	Asegurar que la seguridad de la información sea una parte integral de, los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.	A.14.1.1-Análisis y especificación de requisitos de Seguridad de la Información
			A.14.1 .2- Seguridad de servicios de las aplicaciones en redes públicas
			A.14.1.3- Protección de transacciones de los servicios de las aplicaciones
	A.14.2 - Seguridad en los procesos de desarrollo y soporte	Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de la información	A.14.2.1- Política de desarrollo de seguro.
			A.14.2.2- Procedimiento de control de cambios
			A.14.2.3- Revisión técnica de las aplicaciones después de cambios en la plataforma de operación
			A.14.2.4- Restricción en los cambios a los paquetes de Software.
			A.14.2.5- Principios de construcción de los sistemas seguros
			A.14.2.6- Ambiente de desarrollo seguro
			A.14.2.7 -Desarrollo contratado externamente
			A.14.2.8- Pruebas de seguridad de sistemas
			A.14.2.9- Prueba de aceptación de sistemas

Dominio	Objetos de Control	Objetivo	Control
	A.14.3 - Datos de prueba	Asegurar la protección de los datos usados para pruebas.	A.14.3.1- Protección de datos de prueba
RELACION CON LOS PROVEEDORES			
A.15 Relación con los Proveedores	**A.15.1 - Seguridad de la Información en las relaciones con los proveedores**	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores	A.15.1.1 - Política de la Seguridad de la Información para la relación con proveedores
			A.15.1.2 - Tratamiento de la seguridad dentro de los acuerdos con proveedores
			A.15.1.3 - Cadena de suministro de tecnología de información y comunicación
	A.15.2 - Gestión de la prestación de servicios de proveedores	Mantener el nivel acordado de Seguridad de la Información y de prestación del servicio en línea con los acuerdos con los proveedores.	A.15.2.1 - Seguimiento y revisión de los servicios de los proveedores
			A.15.2.2 Gestión de cambios en los servicios de proveedores
GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
A.16 Gestión de incidentes de Seguridad de la Información	**A.16.1 - Gestión de incidentes y mejoras en la Seguridad de la Información**	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades	A.16.1.1 - Responsabilidades y procedimientos
			A.16.1.2 - Reporte de eventos de Seguridad de la Información
			A.16.1.3 - Reporte de debilidades de Seguridad de la Información
			A.16.1.4 - Evaluación de eventos de Seguridad de la Información y decisiones sobre ellos.
			A.16.1.5 - Respuesta de incidentes de Seguridad de la Información
			A.16.1.6 - Aprendizaje obtenido de los incidentes de Seguridad de la Información
			A.16.1.7 - Recolección de evidencia
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO			
A.17 Aspectos de Seguridad de la Información de la gestión de continuidad de negocio	**A.17.1 - Continuidad de la Seguridad de la Información**	La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de continuidad de negocio de la organización	A.17.1.1 Planificación de la continuidad de la seguridad de la información
			A.17.1.2 Implementación de la continuidad de la seguridad de la información
			A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
	A.17.2 - Redundancias	Asegurar la disponibilidad de instalaciones de procesamiento de la información	A.17.2.1 Disponibilidad de instalaciones de procesamiento de la información

Dominio	Objetos de Control	Objetivo	Control
CUMPLIMIENTO			
A.18 Cumplimiento	**A.18.1 - Cumplimiento de los requisitos legales y contractuales**	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.1 - identificación de la legislación aplicable y de los requisitos contractuales
			A.18.1.2 Derechos de propiedad intelectual
			A.18.1.3 Protección de registros
			A.18.1.4 Privacidad y protección de información de datos personales
			A.18.1.5 Reglamentación de controles criptográficos
	A.18.2 - Revisiones de Seguridad de la Información	Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos de la Entidad.	A.18.2.1 Revisión independiente de la seguridad de la información
			A.18.2.2 Cumplimiento con las políticas y normas de seguridad
			A.18.2.3 Revisión del cumplimiento técnico