1. INTRODUCCIÓN

El Departamento Administrativo de la Función Pública, como entidad técnica, estratégica y transversal del Gobierno nacional, en articulación con la Secretaría de Transparencia y el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) pone a disposición de las entidades la metodología para la gestión integral del riesgo, la cual se actualiza con la incorporación de los lineamientos para la identificación y tratamiento de los riesgos a la integridad pública, de acuerdo con el componente programático denominado Estrategia Institucional para la Lucha Contra la Corrupción, temática 1 Administración del Riesgo desplegado en el Anexo Técnico de los Programas de Transparencia y Ética Pública, en cumplimiento de lo establecido en la Ley 2195 de 20221 y el Decreto 1122 de 2024, 2. reglamentación que modifica el capítulo relacionado con riesgos asociados a posibles actos de corrupción descrito en la versión 6 de la guía. De igual forma, en materia de seguridad de la información se incluyen las actualizaciones pertinentes para la gestión de estos riesgos de forma articulada, de acuerdo con esquema metodológico general.

La administración del riesgo ayuda al conocimiento y mejoramiento de la ESE, contribuye a elevar la productividad y garantizar la eficiencia y eficacia en los procesos, permitiendo definir estrategias de mejoramiento continuo, brindándole un manejo sistémico.

La ESE QUILISALUD, actualiza el Manual de Gestión del Riesgo, codificado MA-GES-01 versión 1 de 2021, con el fin de cumplir con los lineamientos y orientaciones que permitan a los procesos la administración del riesgo en la Institución.

La administración del riesgo fue incorporada al interior de la ESE como una política de gestión por parte de la alta dirección y cuenta con la participación y respaldo de todos los funcionarios sin importar la modalidad de la contratación.

Este manual contiene la metodología para llevar a cabo la identificación, análisis y valoración del riesgo a los que está expuesta la institución, en cada uno de los procesos, inicia con la identificación del contexto estratégico, establece los actores, responsables del proceso de administración del riesgo y define políticas de administración del riesgo aplicables a la ESE y de esta manera fortalecer el Sistema de Control Interno, permite el cumplimiento de objetivos misionales y fines esenciales del Estado.

Para la elaboración del presente Manual se tomó como referencia los lineamientos de:

- Departamento Administrativo de la Función Pública DAFP, establecidos mediante la Guía para la Gestión Integral del Riesgo en Entidades Públicas. Versión 7. 2025
- Ministerio de Tecnologías de la Información y Comunicaciones MINTIC, mediante la Guía No. 7 “Gestión del Riesgo - Seguridad y Privacidad de la Información)
- Requerimientos de la Superintendencia Nacional de Salud, regulados mediante la Circular Externa 2022151000000053-5 de 2025 que define el Sistema Integral de Administración de Riesgos de Cumplimiento (SIARC),

- Circular Externa 20211700000005-5 de 2021 sobre el Subsistema de Administración del Riesgo de Corrupción, Opacidad y Fraude (SICOF).
- Circular Externa 53-5 de 2022 relacionada con el Programa de Transparencia y Ética Empresarial (PTEE), con el enfoque transversal de Gestión Integral del Riesgo promovido por el Departamento Administrativo de la Función Pública

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Desarrollar e implementar un sistema de gestión integral del riesgo en la ESE, basado en los lineamientos de la Guía versión 7, permite identificar, analizar, valorar, tratar, monitorear y comunicar los riesgos estratégicos, corrupción, seguridad en la información, riesgos en la prestación de servicios de salud, operativos, de integridad, tecnológicos, sostenibilidad y reputacionales, con el fin de fortalecer la prevención, garantizar el uso eficiente y seguro de recursos públicos, respaldar la defensa jurídica preventiva, mejorar la calidad y continuidad de servicios de salud y consolidar la confianza de la ciudadanía.

2.2 OBJETIVOS ESPECIFICOS

- **Identificar y caracterizar los riesgos institucionales**: Reconocer los riesgos a los que está expuesto la ESE, considerando su contexto interno y externo, a través de la Construcción de un mapa de riesgos, de acuerdo con el ciclo contemplado en la Guía Versión 7 (identificación, análisis, valoración, tratamiento, monitoreo y comunicación).

- **Valora riesgos con criterios cuantitativos y cualitativos**: Establece criterios de probabilidad, impacto y severidad para cada riesgo de acuerdo con estándares técnicos homogéneos, como lo sugiere la Guía, Evalúa riesgos mediante matrices de valoración y mapas de calor, priorizando los que requieren acciones de mitigación o control.

- **Diseñar estrategias de tratamiento de riesgos**: Formular y documentar controles, planes de prevención y acciones correctivas para los riesgos identificados, incluyendo estrategias para mitigación, transferencia, aceptación o eliminación del riesgo, Alineando las estrategias de tratamiento con los objetivos institucionales del hospital, la misión del sector salud y las políticas públicas, garantizando así una gestión integrada y coherente.

- **Implementar mecanismos de monitoreo y seguimiento**: Definir indicadores clave de riesgo (Key Risk Indicators, KRI) que permitan medir la efectividad de acciones de tratamiento y la evolución de los riesgos en el tiempo. Estableciendo procedimientos periódicos de monitoreo, revisión y ajuste del sistema de gestión de riesgos, integrando auditorías internas, evaluación de controles y reportes a la alta dirección.
- **Fortalecer la cultura organizacional de gestión del riesgo**: Promover la sensibilización y capacitación de servidores públicos, profesionales y demás actores de la ESE en temas de gestión de riesgos, integridad y seguridad de la información, Fomentando la corresponsabilidad entre todas las áreas (clínicas, administrativas,

tecnológicas, etc.) para que la gestión del riesgo sea parte integrante de los procesos operativos, de planeación y evaluación institucional.

- **Garantizar la comunicación y transparencia**: Definir canales de comunicación interna y externa para informar sobre los riesgos, estrategias adoptadas y avances en su gestión, promoviendo la rendición de cuentas e Involucrando a los grupos de interés relevantes (pacientes, comunidad, autoridades de salud, órganos de control) en el proceso de gestión del riesgo, favoreciendo mecanismos de participación y retroalimentación.

- **Articular la gestión del riesgo con otros sistemas institucionales**: Vincular el sistema GIR con el Modelo Integrado de Planeación y Gestión (MIPG) de la ESE, para asegurar que la gestión de riesgos sea coherente con la planificación estratégica y los procesos de control interno y así Alinear la gestión de riesgos con las políticas de defensa jurídica preventiva, especialmente en relación con la integridad institucional y la seguridad de la información, según lo establece la Guía Versión 7.

3. ALCANCE

Aplica a todos los procesos, áreas y servicios de la ESE, tanto asistenciales como administrativos, logísticos, financieros, tecnológicos y de apoyo, e involucra a todos los servidores públicos, contratistas, directivos, personal de sindical y terceros que desarrollen actividades dentro o en nombre de la institución.

Este manual orienta la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos estratégicos, operativos, financieros, de integridad, legales, tecnológicos, ambientales, de seguridad del paciente, de continuidad del servicio y reputacionales, en concordancia con el ciclo de gestión del riesgo definido en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7.

4. REFERENTE NORMATIVO

- El 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, define que para su para la operación de El modelo integrado de planeación y gestión (MIPG), se debe articular la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por él y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, para una adecuada gestión del riesgo.
- Decreto 1008 del 2018, Art. 2.2.9.1.1.3 define que la política de Gobierno Digital se desarrollará conforme a principios que rigen la función y procedimientos administrativos adoptados en Colombia, en particular, al principio de Seguridad de la Información, busca crear condiciones de uso confiable del entorno digital, mediante un enfoque basado en gestión de riesgos, preservando: Confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y servicios que prestan al ciudadano.

- DECRETO 767 DE 2022 (Mayo 16) “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
- Ley 1523 de 2012: Establece la Política Nacional de Gestión del Riesgo de Desastres y el Sistema Nacional de Gestión del Riesgo. Define los procesos de conocimiento del riesgo, reducción del riesgo y manejo de desastres.
- Decreto 1081 de 2015: Forma parte del Decreto Único Reglamentario del Sector Presidencia y contempla obligaciones en materia de gestión del riesgo para entidades públicas. Define el deber de las entidades de integrar los procesos de gestión del riesgo con sus sistemas de gestión institucional.
- Decreto 1122 de 2024: Reglamenta el Art. 73 de la Ley 1474/2011 (modificado por la Ley 2195/2022). A Programas de Transparencia y Ética Pública (PTEP). Establece que los programas deben tener enfoque de riesgos, incluye riesgos de corrupción.
- Ley 2195 de 2022: Medidas para prevenir actos de corrupción, fortaleciendo la articulación institucional y cultura de integridad. Obliga a las entidades públicas a implementar Programas de Transparencia y Ética Pública que incluyan la gestión de riesgos de corrupción.
- Decreto 830 de 2021: Regula la administración del riesgo de lavado de activos, financiación del terrorismo y otros riesgos financieros en entidades públicas, vinculándolo con la obligación de implementar sistemas de administración de riesgos.
- Decreto 1893 de 2021: Establece lineamientos para asistencia técnica y sostenibilidad financiera en gestión del riesgo de desastres y cambio climático para entidades públicas.
- Resolución 351 de 2021 (Procuraduría): Ordena la adopción de una política institucional de administración de riesgos liderada por la alta dirección.
- Circular Externa 20211700000005-5 de 2021 sobre el Subsistema de Administración del Riesgo de Corrupción, Opacidad y Fraude (SICOF)
- Guía para la Gestión Integral del Riesgo – Función Pública Versión 7 (2025). Proporciona la metodología para gestionar riesgos institucionales, de integridad, tecnológicos, reputacionales y otros, integrando lineamientos normativos anteriores.
- Circular Externa 2022151000000053-5 de 2025 que define el Sistema Integral de Administración de Riesgos de Cumplimiento (SIARC),

5. TÉRMINOSYDEFINICIONES

- Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- Administración del Riesgo: Actividades encaminadas a la intervención de los riesgos de la entidad, a través de la identificación, valoración, evaluación, manejo y monitoreo de los mismos de forma que se apoye el cumplimiento de los objetivos de la entidad.
- Análisis de Riesgos: Determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo

- Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización
- Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito puede ser diferente para los distintos tipos de riesgo que la entidad debe o desea gestionar.
- Capacidad de riesgo: Máximo valor de nivel de riesgo que la ESE puede soportar y a partir del cual la Gerencia considera que no sea posible el logro de objetivos de la ESE.
- Causa raíz: Causa principal o básica, correspondiente a las razones por las cuales se puede presentar el riesgo.
- Subcausa: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- Consecuencia: Los efectos resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
- Control: Media que permite reducir o mitigar un riesgo.
- Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.
- Evaluación del riesgo: Comparación de resultados del análisis del riesgo con criterios del riesgo, para determinar si el riesgo y su magnitud o ambos son aceptables tolerables.
- Factores de riesgo: Son las fuentes generadoras de riesgos.
- Gestión del riesgo: Proceso efectuado por la alta dirección y por todo el personal para proporcionar a la administración un aseguramiento razonable con el logro de objetivos.
- Identificación del riesgo: Análisis para encontrar una potencial desviación de objetivos.
- Impacto: Consecuencias que puede ocasionar a la ESE la materialización del riesgo.
- Integridad: Propiedad de exactitud y completitud.5
- Mapa de calor: Plano que representan simultáneamente las escalas de medición de impacto y probabilidad, y que, como producto de su combinación, mediante colorimetría representa la importancia (nivel de severidad o criticidad) del riesgo.
- Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.
- Materialización del Riesgo: Ocurrencia o desarrollo del riesgo
- Nivel de riesgo: Es el valor que se determina a parir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional del alcanzar los objetivos.
- Oportunidad: Eventos que permiten alcanzar un resultado esperado o aumentar los efectos deseables.
- Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- Política de Administración del Riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.
- Probabilidad: 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.
- Riesgo: Efecto que causa sobre los objetivos de la ESE, debido a eventos potenciales (Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas

por deficiencias, falla o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura u ocurrencia de acontecimientos externos.

- Riesgo de gestión: Posibilidad que suceda algún evento que tendrá impacto sobre el cumplimiento de objetivos. Se expresa en términos de probabilidad y consecuencias.
- Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Riesgo de fraude: Posibilidad de que la Entidad incurra en una pérdida financiera o de otro tipo cuando una persona (que puede ser empleado, un cliente, o una persona vinculada a la Entidad) que actúa individualmente o en colusión, obtiene una ventaja o beneficio injusto en forma deshonesta o engañosa
- Riesgo de Seguridad de la Información: Posibilidad que una amenaza concreta pueda explotar una vulnerabilidad para causar pérdida o daño en un activo de información.
- Riesgo inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riego inherente, dentro de unas escalas de severidad.
- Riesgo residual: El resultado de aplicar la efectividad de controles al riesgo inherente.
- Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- Tratamiento del riesgo: Proceso para modificar el riesgo.
- Valoración del Riesgo: Establece la identificación y evaluación de los controles. En la etapa de valoración del riesgo se determina el riesgo residual.
- Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

6. ASPECTOS CLAVES ANTES DE APLICAR LA METODOLOGÍA DE RIESGOS

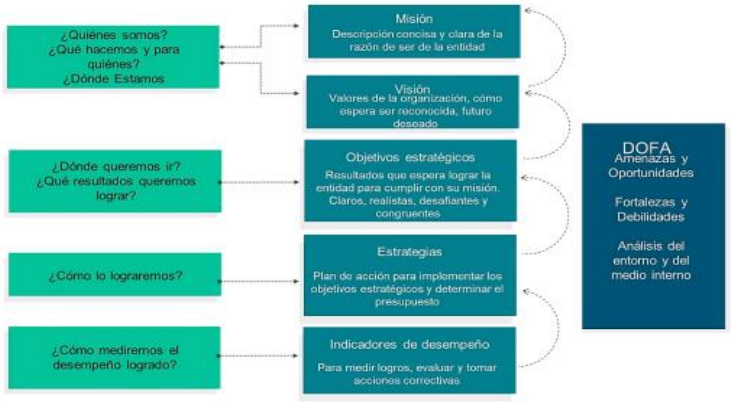
La gestión del riesgo se consolida a través de:

- El reconocimiento de la cultura;
- El desarrollo de capacidades;
- El uso de las técnicas aplicadas;
- La integración de la estrategia y el desempeño;
- La alineación con la estrategia y objetivos clave y
- La relación con el valor.

6.1 ANÁLISIS ESTRATÉGICO DE LA ENTIDAD Y SU MODELO DE OPERACIÓN BASADA EN PROCESOS:

La gestión por procesos se constituye en el eslabón que conecta la planeación estratégica, con el despliegue de la parte operativa. Para ello, toma como insumos algunos elementos de la dimensión de direccionamiento estratégico en la medida en que debe alinearse con la misión, visión y objetivos estratégicos, entre otros. A continuación, en la figura 4 se desarrolla un modelo básico de planeación estratégica, donde se precisan las preguntas que pueden orientar la construcción de cada uno de los componentes: Ver Figura No.1

Figura No. 1 Estructura de Planificación Estratégico



7. POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

7.1 DECLARACIÓN DE LA POLITICA

La Gerencia de QUILISALUD ESE, en cumplimiento de su direccionamiento estratégico y alineada con la Dimensión 7 del Modelo Integrado de Planeación y Gestión (MIPG) y los estándares del Sistema Obligatorio de Garantía de Calidad en Salud (SOGCS), declara su compromiso ineludible con la gestión preventiva y el control de los riesgos que puedan afectar la prestación de servicios de salud de baja complejidad. Reconocemos la administración del riesgo como un proceso transversal vital para la sostenibilidad y la calidad. Por ende, la institución se compromete a identificar, analizar, valorar y tratar los riesgos bajo los siguientes lineamientos integrales:

- Riesgos de Gestión y Operativos (Eficacia Institucional): Gestionaremos las incertidumbres que puedan impedir el cumplimiento de objetivos misionales y del Plan de Desarrollo, asegurando la continuidad de la prestación del servicio y la eficiencia en procesos administrativos y asistenciales, conforme a los estándares de Calidad.
- Riesgos Fiscales y Financieros (Sostenibilidad): Implementaremos controles para proteger los recursos públicos, prevenir el detrimento patrimonial y asegurar la viabilidad financiera de la E.S.E., mitigando eventos que afecten el flujo de caja, la facturación o el cumplimiento de obligaciones tributarias.
- Seguridad de Información y Ciberseguridad (Confidencialidad): Nos comprometemos a garantizar la Confidencialidad, Integridad y Disponibilidad de los activos de información, protegiendo especialmente la Historia Clínica y datos sensibles de nuestros pacientes frente a pérdidas, adulteraciones o accesos no autorizados, en cumplimiento de la Ley de Habeas Data y los lineamientos de Gobierno Digital.
- Integridad Pública - SIGRIP (Transparencia): Adoptamos una postura de TOLERANCIA CERO frente a la corrupción. Fortalecemos el Sistema de Integridad Pública para identificar y neutralizar riesgos de soborno, fraude o conflicto de intereses en contratación y gestión administrativa, promoviendo una cultura ética en todos los niveles de la ESE.

8. ESTRUCURA PARA LA ADMINISTRACIÓN DEL RIESGO

8.1 OBJETIVO

Suministrar una metodología para las áreas y servicios de la ESE, que permita gestionar de manera efectiva los riesgos que puedan presentarse y afecten el logro de los objetivos estratégicos y de proceso, definidos en el PDI 2024 – 2027, bajo la implementación de herramientas adecuadas para identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos, con el fin de determinar roles y responsabilidades de cada líder, bajo el enfoque de las tres líneas de defensa, de la Dimensión 7 de MIPG e implementación de prácticas de Gestión basadas en el marco COSO-ERM.

Esta Política tiene como propósito la institucionalidad, la toma de decisiones informadas y a la generación del valor público, asegurando la integridad, transparencia y eficiencia en la administración de recursos.

8.2 ALCANCE

La política de Gestión del Riesgo, aplica a todo el personal que desempeña funciones en la ESE, en los procesos de Direccionamiento estratégico, Misionales, Procesos de apoyo y seguimiento, ejecución de proyectos y programas institucionales, no importa el tipo de vinculación, el nivel jerárquico de todas las sedes que hacen parte de la ESE.

8.3 CONTEXTO INTERNO Y EXTERNO QUILISALUD ESE

8.3.1 Contexto Externo

- Descripciones problemáticas del sector salud en el Territorio
  - ✓ Flujo de Recursos (Crisis Financiera): La liquidación de EPS y demora en el giro directo generan una cartera de difícil cobro y afectación del flujo de caja. Pone en riesgo: Pago a proveedores y talento humano, amenazando la operación continua.
  - ✓ Transición Epidemiológica y Carga de Enfermedad: El sector enfrenta una "doble carga": la persistencia de enfermedades infecciosas y aumento acelerado de enfermedades crónicas no transmisibles (Hipertensión, Diabetes, Cáncer), dificultad implementación del modelo de promoción y prevención, desfinanciado.
  - ✓ Inestabilidad Jurídica: Los constantes cambios normativos y reformas al sistema de salud generan incertidumbre en la planeación estratégica a largo plazo

a) Datos demográficos y socioeconómicos

Santander de Quilichao se consolida como el segundo municipio más importante del departamento del Cauca y el nodo de desarrollo económico y social de la subregión Norte. Su ubicación estratégica sobre la vía Panamericana lo convierte en un puerto seco de intercambio comercial, pero también en un punto neurálgico de conflictividad social.

b) Dinámica Poblacional y Demográfica

Según proyecciones DANE ajustadas año 2025, el municipio presenta una alta densidad poblacional con una distribución particular entre su casco urbano y la ruralidad dispersa.

- Población Total Aproximada: 114.000 a 116.000 habitantes.
- Distribución Espacial:
  - ✓ Zona Urbana (Cabecera): 56% (Aprox. 64.000 hab). Concentra la actividad comercial, industrial y la oferta institucional de salud.
  - ✓ Zona Rural (Centros Poblados y Disperso): 44% (Aprox. 50.000 hab). Caracterizada por una alta dispersión en veredas, resguardos indígenas y consejos comunitarios afrodescendientes.
- Composición Étnica (Determinante Social Clave): El municipio es territorio pluriétnico y multicultural:
  - ✓ Población Afrodescendiente: Presencia mayoritaria en zona plana y consejos comunitarios.
  - ✓ Población Indígena (Pueblo Nasa): Asentada principalmente en los resguardos de la zona montañosa (Munchique, Los Tigres, Canoas, etc.).
  - ✓ Población Mestiza: Predominante en la cabecera municipal

d) Perfil Económico

Santander de Quilichao presenta una economía dual que influye en los riesgos de salud ocupacional y ambiental:

- Sector Industrial (Zona Norte): Posee el parque industrial más importante de la región (con presencia de empresas de papel, cartón, alimentos, metalmecánica y farmacéutica).
  - ✓ *Impacto en Salud:* Genera riesgos de accidentes laborales industriales y enfermedades profesionales que consultan en urgencias.
- Sector Agroindustrial (Zona Plana): Monocultivo de caña de azúcar.
  - ✓ *Impacto en Salud:* Exposición a agroquímicos y quemas controladas que afectan la calidad del aire (enfermedad respiratoria).
- Economía Campesina y Minería (Zona Rural): Café, piña, cítricos. Sin embargo, persiste la minería ilegal de oro (uso de mercurio/cianuro en fuentes hídricas) y cultivos ilícitos en zonas de ladera.
- Comercio y Servicios: Al ser ciudad región, su comercio atrae población flotante de municipios vecinos (Caloto, Corinto, Suárez, Buenos Aires), aumentando la demanda de servicios de salud no calculada en la población propia.

e) Contexto Social

- Pobreza Multidimensional: Aunque es polo de desarrollo, existen brechas profundas. La zona rural carece en gran medida de agua potable continua y saneamiento básico, lo que mantiene altos los índices de Enfermedad Diarreica Aguda (EDA) y Parasitosis.

- Infraestructura Vial: La Vía Panamericana cruza el municipio, lo que representa un alto flujo vehicular de carga pesada, siendo la principal fuente de accidentes de tránsito de alta energía que ingresan al hospital.

f) Seguridad y Orden Público (Riesgo Crítico)

Santander de Quilichao es catalogado como un municipio PDET (Programa de Desarrollo con Enfoque Territorial) debido a la afectación histórica y actual del conflicto armado.

- Actores Armados**:** Presencia e injerencia de Grupos Armados Organizados Residuales (GAO-r - Disidencias) que se disputan el control territorial del corredor que conecta la cordillera con el Pacífico (Ruta del Naya).

- Dinámicas de Violencia:

  ✓ Homicidios Selectivos: Alta tasa de sicariato y violencia instrumental.
  ✓ Extorsión: Afecta al sector comercio y transporte.
  ✓ Reclutamiento Forzado: Riesgo para niños, niñas y adolescentes en zona rural.

- Protesta Social y Bloqueos: El municipio es punto de concentración recurrente de la Minga Indígena y Paros Nacionales.

  ✓ *Impacto en Salud:* Los bloqueos en la Panamericana generan desabastecimiento de oxígeno e insumos médicos, impiden el paso de ambulancias y el traslado de personal, activando frecuentemente los planes de contingencia hospitalaria.

- Misión Médica: El personal de salud, especialmente de atención prehospitalaria (Ambulancias), opera bajo riesgo en zonas rurales profundas debido a restricciones de movilidad impuestas por actores ilegales o combates cruzados.

8.3.2 Contexto Interno

a) Plataforma Estratégica

- **MISION**: Quilisalud es una Empresa Social del Estado, que presta servicios de salud, primarios y complementarios, humanizados, seguros y de calidad, centrados en nuestro modelo de atención en salud integral con enfoque de atención primaria y gestión de riesgo con enfoque diferencial e impactando directamente al individuo, familia y comunidad.

- **VISION**: Para el año 2028 ser un prestador primario y complementario en salud referente a nivel nacional, que dé continuidad a la relación entre comunidad y la institucionalidad, impactando de manera progresiva los indicadores de salud de la población atendida, garantizando la sostenibilidad financiera y en especial la responsabilidad social de la empresa.

- **Objetivos Estratégicos**

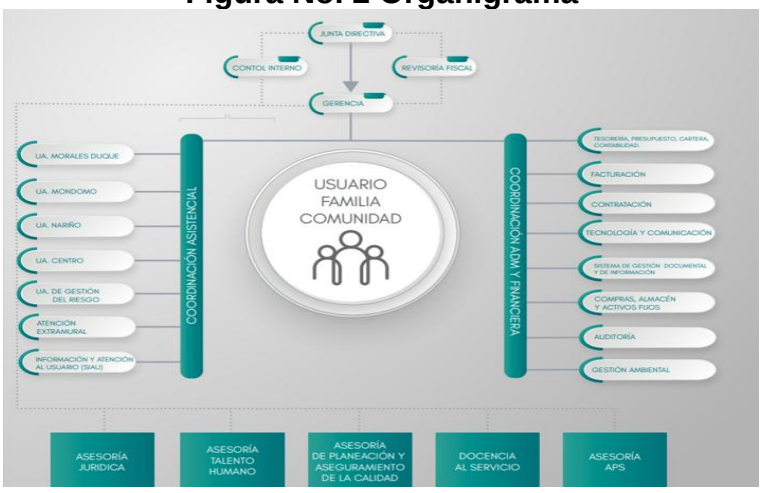
  - ✓ Contribuir en la participación efectiva de la comunidad en el control sobre los determinantes que afectan la salud individual, familiar y colectiva, basados en la promoción de la salud y la prevención de la enfermedad.
  - ✓ Aportar estrategias y herramientas de acompañamiento a los entornos de la comunidad para que opten por estilos de vida que beneficien la salud individual, familiar y colectiva aportando así al mejoramiento en su calidad de vida.
  - ✓ Mejorar continuamente la Calidad en la Prestación de los Servicios como una política Institucional con humanización y calidez

- **Líneas Estratégicas**

  - ✓ Línea Estratégica 1: Fortalecimiento Organizacional y Estandarización de Procesos.
  - ✓ Línea Estratégica 2: Sistema Obligatorio de Garantía de La Calidad en Salud, Seguridad y Humanización en la Atención.
  - ✓ Línea Estratégica 3 Gestión del Acceso a los Servicios de Salud en Atención Primaria en Salud (APS).
  - ✓ Línea Estratégica 4 Sostenibilidad Financiera
  - ✓ Línea Estratégica 5 Participación Social y Comunitaria como Proceso de la Gestión de la Salud Pública.

- **Organigrama. Ver Figura No.2**

Figura No. 2 Organigrama



Fuente: Oficina de Planeación

b) La planta y estructura de la ESE, así como la delegación de autoridad o poder decisorio discrecional, Se Articula con el Programa de Transparencia y Ética Pública.

- Planta de Personal

Tabla No. 1 Planta de Personal

NIVEL DIRECTIVO				
CODIGO	GRADO	DENOMINACIÓN	No. EMPLEOS	UBICACIÓN
85	2	Gerente Empresa Social Del Estado	1	GERENCIA
Nivel Profesional				
219	3	Profesional Universitario	1	Área Administrativa
219	3	Profesional Universitario	1	Área Asistencial
219	3	Jefe Oficina De Control Interno	1	Área Administrativa
214	4	Odontólogo	1	Área Asistencial
217	2	Profesional Servicio Social Obligatorio-Medico	1	Área Asistencial
217	2	Profesional Servicio Social Obligatorio - Odontólogo	1	Área Asistencial
217	1	Profesional Servicio Social Obligatorio – Enfermera(O)	2	Área Asistencial
Nivel Asistencial				
407	2	Auxiliar Administrativo	1	Área Administrativa
412	3	Auxiliares Área Salud	2	Área Asistencial
412	1	Auxiliares Área Salud	2	Área Asistencial
Trabajadores Oficiales				
480	2	Conductor	2	Área Administrativa
TOTAL DE EMPLEOS			**16**	

Fuente: Oficina de Talento Humano

- **Modelo de Gobernanza para la Transparencia**

Define quién manda, quién ejecuta y quién vigila la Ética Pública en la ESE Se estructura en tres niveles jerárquicos:

A. Nivel Estratégico (Toma de Decisiones)

- Junta Directiva: Aprueba el presupuesto para el Plan Anticorrupción y define el tono ético desde la cima.
- Gerente: Es el máximo responsable legal del cumplimiento del PTEP. Firma el Mapa de Riesgos de Corrupción y lidera la rendición de cuentas.
- Comité Institucional de Gestión y Desempeño: Instancia donde se aprueba y evalúa trimestralmente el avance del Programa de Transparencia y Ética Pública (PTEP).

B. Nivel Táctico (Coordinación y Asesoría)

- Oficina de Planeación: Diseña el Programa de Transparencia, consolida los informes y gestiona el Mapa de Riesgos de Corrupción.
- Oficina de Control Interno: Actúa como tercera línea de defensa, evaluando independientemente si los controles anticorrupción funcionan.

C. Nivel Operativo (Ejecución)

- Líderes de Proceso: Responsables de identificar sus riesgos de corrupción (Ej: Tesorero, Compras) y aplicar los controles.
- Equipo de Comunicaciones: Responsable de mantener actualizado el sitio web con la información pública.

- **MATRIZ DE ATRIBUCIONES Y DECISIONES (Roles En Ética)**

Esta matriz (tipo RACI) define claramente qué le corresponde hacer a cada cargo frente al Programa de Transparencia y Ética Pública.

Tabla 2 Matriz RACI

Rol / Cargo	Atribuciones (Responsabilidades)	DECISIONES (Autoridad)
Gerente	Liderar la Audiencia Pública de Rendición de Cuentas. Garantizar recursos para el PTEP.	Aprobar y firmar el Mapa de Riesgos de Corrupción y Programa de Transparencia y Ética Pública (PTEP) antes del 31 de enero.
Junta Directiva	Vigilar cumplimiento de la misión institucional bajo principios éticos.	Aprobar el Código de Integridad y Ética de la institución. Decidir sobre sanciones graves propuestas por control disciplinario.
Jefe De Planeación	Elaborar documento PTEP. Monitorear indicadores de transparencia. Consolidar Mapa de Riesgos.	Definir la metodología para identificación de riesgos de corrupción. Validar la información antes de ser publicada en la web.
Control Interno (Auditor)	Realizar el seguimiento cuatrimestral al PEPT y publicarlo. Evaluar efectividad de controles.	Reportar hallazgos de presunta corrupción a entes de control (Contraloría/Procuraduría) de manera autónoma.
Líder De Talento Humano	Socializar Código de Integridad. Gestionar los conflictos de interés de los funcionarios.	Exigir la declaración de bienes y rentas y el certificado de antecedentes a todo el personal nuevo.
SIAU (Atención al Usuario)	Administrar canales de denuncia. Garantizar la protección de la identidad del denunciante.	Clasificar si una PQRS es una queja normal o una Denuncia de Corrupción para darle el trámite legal especial.
JURÍDICA / CONTRATACIÓN	Publicar la gestión contractual en el SECOP y en la web institucional.	Rechazar procesos de contratación que no cumplan con los principios de transparencia y selección objetiva.

c) Las entidades sobre las que la organización tiene control y entidades que ejercen control sobre la organización.

La relación de "Control" se entiende en dos vías: Quién me vigila (Control Externo) y Sobre quién ejerzo supervisión (Control/Influencia).

- **MAPA DE REDES EXTERNAS: ENTIDADES QUE EJERCEN CONTROL SOBRE LA ORGANIZACIÓN**

Está conformado por organismos del Estado y sociedad civil a los cuales la ESE debe rendir cuentas. En el marco de la Ética Pública, son las entidades ante las cuales se reportan actos de corrupción o fallas administrativas. Se clasifican según Tipo de Control:

A. Control Político y Administrativo

- Alcaldía Municipal de Santander de Quilichao: Ejerce control administrativo. El Alcalde nombra al Gerente y preside la Junta Directiva.

- Concejo Municipal: Ejerce control político sobre la gestión del Gerente y aprueba presupuesto/adiciones.
- Junta Directiva: Máximo órgano de dirección evalúa plan de gestión del Gerente.

B. Control Fiscal (Dineros Públicos)

- Contraloría General del Cauca: Vigila la correcta ejecución del presupuesto y el patrimonio. Realiza auditorías fiscales para detectar detrimento patrimonial.

C. Control Disciplinario y de Conducta (Funcionarios)

- Procuraduría General de la Nación: Investiga y sanciona faltas disciplinarias de los funcionarios públicos y vigila el cumplimiento de la Ley de Transparencia.
- Personería Municipal: Ejerce control disciplinario en primera instancia y defiende los Derechos Humanos.

D. Control Técnico y Sectorial (Salud)

- Superintendencia Nacional de Salud (Supersalud): Ejerce inspección, vigilancia y control sobre la prestación del servicio, la calidad y el flujo de recursos.
- Secretaría de Salud Departamental del Cauca: Habilita servicios y vigila la salud pública.
- INVIMA: Controla los insumos, medicamentos y dispositivos médicos (Tecnovigilancia).

E. Control Social (Ciudadanía)

- Asociación de Usuarios (Alianza): Representantes de pacientes que vigilan la calidad.
- Veedurías Ciudadanas: Grupos organizados que vigilan contratos específicos (Ej: Obras de infraestructura o contratación de personal).

- **MAPA DE REDES: ENTIDADES SOBRE LAS QUE LA ORGANIZACIÓN TIENE CONTROL**

En el marco del PTEP, el "Control" se interpreta como la Supervisión y Vigilancia sobre terceros que ejecutan recursos misionales de la entidad.

A. Control Contractual (Terceros Ejecutores): La ESE ejerce autoridad, supervisión e interventoría sobre:

- Contratistas de Prestación de Servicios de Salud: Si la ESE. tiene contratos de comodato o tercerizada la lectura de laboratorio especializado, ejerce control de calidad y cumplimiento sobre estas empresas.
- Contratistas de Apoyo (Outsourcing): Empresas de Vigilancia, Aseo y Desinfección, Ruta de Residuos y Mantenimiento de Equipos. La ESE controla que sus empleados cumplan los protocolos éticos y técnicos dentro de los NAP.

- Proveedores de Insumos: Control sobre cumplimiento de especificaciones técnicas y tiempos de entrega.

- **MODELO DE RELACIONAMIENTO (Cómo interactúan)**

"El modelo de relacionamiento de la E.S.E. con su red de control se basa en los principios de Publicidad, Rendición de Cuentas y Colaboración Armónica:"

Tabla No. 3 Relacionamiento de Control

Tipo de Relación	Acciones de Transparencia y Ética	Herramienta De Reporte
Sujeto de Control (Hacia Arriba)	La ESE entrega información periódica, veraz y oportuna a los entes de control para facilitar la auditoría.	IRECI (Contraloría), RIPS/SIHO Supersalud), SECOP II (Público).
Ejecutor de Control (Hacia Abajo)	La ESE exige a sus contratistas y proveedores la firma de cláusulas de transparencia, inhabilidades e incompatibilidades, y realiza interventoría estricta.	Informes de Supervisión, Actas de Liquidación, Evaluaciones de Desempeño.
Relación Horizontal (Social)	La E.S.E. abre espacios de diálogo para que la comunidad vigile la gestión.	Audiencia Pública de Rendición de Cuentas, Oficina SIAU.

d) La naturaleza y alcance de las interacciones con entidades de otras Ramas del Poder Público, órganos de control o independientes. Así como de las interacciones con particulares que no derivan en vínculo formal, pero son recurrentes (actividad cabildeo).

La ESE QUILISALUD, interactúa con diversos actores del sistema público y privado. Estas interacciones se rigen bajo los principios de Legalidad, Publicidad e Igualdad de Trato, evitando cualquier privilegio injustificado.

- **INTERACCIONES CON OTRAS RAMAS DEL PODER PÚBLICO**

A. Rama Judicial (Jueces y Magistrados)

- ✓ Naturaleza: Es una relación de Cumplimiento Obligatorio y Colaboración. La E.S.E. no negocia con esta rama, sino que acata sus fallos.
- ✓ Alcance y Recurrencia:
  - Acción de Tutela: Interacción alta y frecuente. Respuesta a requerimientos judiciales relacionados con prestación de servicios de salud (medicamentos, remisiones).
  - Demandas (Laborales/Reparación Directa): Interacción a través de la Oficina Jurídica para la defensa de los intereses de la entidad.
  - Requerimientos Probatorios: Entrega de copias de Historias Clínicas solicitadas por Fiscalía o Jueces (bajo reserva legal).

B. Rama Legislativa (Nivel Local: Concejo Municipal)

- ✓ Naturaleza: Relación de Control Político y Presupuestal.
- ✓ Alcance:

- Citaciones de Control Político: El Gerente asiste al Concejo para rendir informes sobre la gestión, estados financieros y calidad del servicio.
- Aprobación Presupuestal: Interacción anual para la presentación y sustentación del presupuesto de la vigencia siguiente.

- **INTERACCIONES CON ÓRGANOS DE CONTROL E INDEPENDIENTES**

A. Órganos de Control (Ministerio Público y Fiscal)

- ✓ Naturaleza: Relación de Sujeción y Rendición de Cuentas.
- ✓ Alcance:
  - Defensoría del Pueblo y Personería: Interacción diaria/semanal para mediación en casos de vulneración de derechos a usuarios (Peticiones urgentes de atención).
  - Procuraduría y Contraloría: Interacción mediante el reporte de información en plataformas (SIA, SIRECI) y atención a visitas de auditoría.

B. Órganos Independientes (Comisión Nacional del Servicio Civil - CNSC)

- ✓ Naturaleza: Relación Administrativa para el Mérito.
- ✓ Alcance: Reporte de la Oferta Pública de Empleos de Carrera (OPEC) y gestión de las listas de elegibles para proveer vacantes definitivas, garantizando la transparencia en el empleo público.

- **INTERACCIONES CON PARTICULARES (ACTIVIDADES DE CABILDEO)**

Este es el punto crítico del PTEP. Se refiere a las interacciones con privados que buscan influir en las decisiones de la ESE (compras, medicamentos, contratación).

Definición Institucional de Cabildeo (Lobby): Se entiende por cabildeo cualquier actividad realizada por personas naturales o jurídicas, privadas, con el objetivo de influir en las decisiones, proyectos o contratos de la ESE.

A. Industria Farmacéutica y de Dispositivos (Visitadores Médicos)

- ✓ Naturaleza: Promoción comercial y técnica.
- ✓ Riesgo de Corrupción: Incentivos perversos (dádivas, viajes, cenas) a médicos o administrativos para inducir la compra o formulación de una marca específica.
- ✓ Alcance Regulado:
  - Las visitas de laboratorios solo se permiten con agenda previa y en horarios que no afecten la atención de pacientes.
  - Prohibición: Se prohíbe la entrega de regalos, muestras médicas no registradas o patrocinios directos a funcionarios.

B. Proveedores y Contratistas (Pre-contractual)

- ✓ Naturaleza: Interés comercial en procesos de licitación o contratación directa.
- ✓ Riesgo: Direccionamiento de contratos o "Sastrería" (ajustar pliegos a la medida).
- ✓ Alcance Regulado:
  - Toda interacción para estudios de mercado debe ser pública y por escrito (correo electrónico institucional).
  - Se prohíben las reuniones privadas a puerta cerrada entre ordenadores del gasto y posibles oferentes durante la etapa de licitación, salvo en audiencias públicas.

C. Actores Políticos y Líderes Comunitarios (Recomendaciones)

- ✓ Naturaleza: Gestión de intereses particulares (empleo o priorización de atención).
- ✓ Riesgo: Tráfico de influencias y clientelismo.
- ✓ Alcance Regulado:
  - La E.S.E. establece que la recepción de hojas de vida se hace exclusivamente a través del banco de hojas de vida institucional o convocatorias públicas, no por "recomendación directa".

- **MECANISMO DE CONTROL: REGISTRO DE CABILDEO**

Para transparentar estas interacciones informales, la ESE implementa el Registro de Agenda Pública, conforme a la Ley 1474 de 2011: "Todo funcionario del Nivel Directivo (Gerente y Jefes de Oficina) debe hacer pública su agenda. Cuando se agende una reunión con un particular (proveedor, lobista, político), se debe dejar constancia en el registro del motivo de la reunión y los participantes, garantizando que no existen acuerdos ocultos.

e) Las obligaciones generales de la entidad, con independencia de la fuente: legal, reglamentaria, contractual, extracontractual u obligaciones profesionales. Agrupando entre aquellas que son deberes (obligatorio cumplimiento), expectativas (cumplimiento facultativo) y compromisos (cumplimiento asumido).

- **OBLIGACIONES GENERALES, EXPECTATIVAS Y COMPROMISOS INSTITUCIONALES**

La ESE QUILISALUD, como entidad de naturaleza pública descentralizada, está sujeta a un régimen jurídico mixto y a múltiples fuentes de obligaciones. Para efectos de la gestión de transparencia, estas se clasifican según su grado de obligatoriedad y origen:

A) DEBERES (OBLIGATORIO CUMPLIMIENTO)

Son aquellas obligaciones de carácter imperativo y vinculante. Su incumplimiento genera sanciones disciplinarias, fiscales, penales o administrativas. No son negociables y constituyen el mínimo vital de la operación.

- ✓ Deberes Legales y Reglamentarios (Fuente: La Ley):

- Prestación del Servicio: Garantizar el derecho fundamental a la salud (Ley 1751/2015) cumpliendo los estándares de habilitación (Res. 3100/2019).
- Transparencia Activa: Publicar la información contractual, presupuestal y de gestión en la página web y en el Portal de Transparencia Económica (Ley 1712/2014).
- Gestión Financiera: Manejar los recursos públicos con austeridad y eficiencia, reportando a la Contraloría (SIRECI) y al Ministerio de Salud.
- Protección de Datos: Custodiar la reserva de la Historia Clínica y los datos personales (Habeas Data).

✓ Deberes Contractuales (Fuente: El Contrato):
- Con las EAPB (EPS): Prestar los servicios de salud pactados en los acuerdos de voluntades (Cápita o Evento) a la población afiliada.
- Con Proveedores: Pagar oportunamente las facturas por bienes y servicios recibidos, respetando los principios de la contratación estatal.

✓ Deberes Profesionales (Fuente: Ética):
- El personal asistencial (médicos, enfermeras) debe actuar bajo la *Lex Artis*, respetando el código de ética de sus profesiones (Ley 23/1981, Ley 911/2004).

- **EXPECTATIVAS (CUMPLIMIENTO FACULTATIVO O DESEABLE)**

Son aquellas conductas o resultados que los grupos de valor (comunidad, usuarios) esperan de la ESE, aunque no estén taxativamente escritas en una ley como una obligación sancionable. Su cumplimiento genera Legitimidad Social y Confianza.

✓ Humanización "Más allá del Protocolo":
- Se espera que el trato no sea solo "técnicamente correcto", sino empático, cálido y culturalmente adaptado (especialmente con población indígena y afro del Municipio).

✓ Responsabilidad Ambiental:
- Más allá de disponer los residuos (que es un deber), la comunidad espera que el Hospital lidere campañas de "Hospital Verde", ahorro de energía y papel.

✓ Participación en el Desarrollo Local:
- Se espera que la E.S.E. priorice, en igualdad de condiciones, la contratación de mano de obra local o proveedores del municipio para dinamizar la economía.

- **COMPROMISOS (CUMPLIMIENTO ASUMIDO / AUTO-IMPUESTO)**

La ESE. ha decidido adquirir voluntariamente a través de sus instrumentos de planeación. Una vez escritos y aprobados, se vuelven exigibles internamente.

✓ Compromisos de Integridad (Código de Integridad):
- La adhesión a los valores: Honestidad, Respeto, Compromiso, Diligencia y Justicia. La entidad se compromete a que sus funcionarios actúen bajo estos principios.

✓ Plan de Desarrollo Institucional:
- Las metas que el Gerente propuso en su plan de gestión (Ej: "Aumentar la satisfacción al 95%", "Renovar el parque automotor"). No lo exigía la ley, pero al ponerlo en el plan, se vuelve un compromiso de gestión.

✓ Pactos de Transparencia:
- Acuerdos firmados con la Secretaría de Transparencia o Veedurías para realizar rendiciones de cuentas adicionales a las de ley.

✓ Política de Calidad y Seguridad del Paciente:
- El compromiso de "no punibilidad" y "cultura justa" es una decisión organizacional asumida voluntariamente para mejorar.

- **REMISIÓN AL MARCO NORMATIVO**

Para consultar el detalle taxativo de los DEBERES, la E.S.E. dispone del NORMOGRAMA INSTITUCIONAL, el cual se encuentra publicado en el sitio web https://quilisalud.gov.co/home/2019/08/26/normograma-institucional/, sección Gestión Jurídica / Normatividad

En dicho instrumento se relacionan:
✓ Leyes Estatutarias y Ordinarias.
✓ Decretos Reglamentarios del Sector Salud y Función Pública.
✓ Resoluciones del Ministerio de Salud.
✓ Acuerdos Municipales y de Junta Directiva.
✓ Manuales de Funciones y Procedimientos (donde se operacionalizan los deberes).

Este marco normativo es actualizado periódicamente por la Oficina Jurídica y de Calidad para asegurar que la matriz de obligaciones legales se mantenga vigente.

f) **Información general sobre los contratos y principales proveedores de la entidad**.

Agrupa los contratos y proveedores según características como: naturaleza jurídica, modalidad de selección, valores mínimos, máximos y media de contratación, relación de cumplimiento o incumplimientos, tipos de supervisión. Ver Anexo No. 1 BD Contratos 2025.

g) Grupos de Valor

- **Grupo de Valor Primario: Ciudadanos y Usuarios**

Son los receptores directos de los servicios de salud. Dada la demografía del municipio, este grupo no es homogéneo y requiere un Enfoque Diferencial.

✓ Población Régimen Subsidiado: Clasificadas en SISBEN IV (Grupos A, B y C) sin capacidad de pago, constituyen el mayor porcentaje de facturación y demanda.

- ✓ Población Étnica (Interculturalidad):
  - *Comunidades Indígenas (Pueblo Nasa):* Usuarios que residen en resguardos, pero acuden a la ESE para urgencias o servicios no cubiertos por sus IPS indígenas (AIC). Requieren atención respetuosa de sus usos y costumbres.
  - *Comunidades Afrodescendientes:* Habitantes de consejos comunitarios de la zona plana y norte, con perfil epidemiológicos específicos (Hipertensión, Diabetes, Anemia Falciforme).

- ✓ Población Víctima del Conflicto Armado: Desplazados y víctimas asentadas en el casco urbano y rural, que requieren atención psicosocial y prioritaria según Ley de Víctimas.
- ✓ Población Materno-Infantil: Mujeres gestantes y primera infancia, foco de los programas de Promoción y Prevención (PYP) y vacunación PAI.

- **Grupo de Valor Interno: Talento Humano**

Son quienes hacen posible la prestación del servicio.

- ✓ Personal Asistencial: Médicos Generales, Médicos Especialistas, Odontólogos, Enfermeras Jefes, Odontólogos, Nutricionista, Psicólogo, Auxiliares de Enfermería, Bacteriólogos y Tecnólogos en Atención Prehospitalaria (APH).
- ✓ Personal Administrativo: Gerente, Administrador, Contador, Presupuesto, abogado, Facturación, SIAU, Almacén, Auditoria, Tesorería, Calidad, planeación, Auxiliares administrativas, auxiliares servicios generales, Técnico de mantenimiento, motoristas
- ✓ Estudiantes convenio docencia-servicio que realizan sus prácticas en la institución.

- **Partes Interesadas Institucionales (El Estado)**

Entidades que regulan, vigilan o financian la operación.

- ✓ Alcaldía de Santander de Quilichao: Es el "dueño" de la ESE. La Secretaría de Salud contrata acciones del Plan de Intervenciones Colectivas (PIC) y vigila la salud pública.
- ✓ Secretaría de Salud Departamental del Cauca (CRUE): Ente rector que regula la red de ambulancias, el sistema de referencia y contrarreferencia y habilita los servicios.
- ✓ Superintendencia Nacional de Salud: Ente de control y vigilancia sancionatoria.
- ✓ Ministerio de Salud: Define la normatividad y lineamientos técnicos (Resoluciones).

- **Entidades Responsables de Pago (EAPB / EPS)**

Son los clientes institucionales que garantizan el flujo financiero.
- ✓ EPS del Régimen Subsidiado: Principalmente Asmet Salud, Emssanar, Nueva EPS, AIC (Asociación Indígena del Cauca).
- ✓ ADRES: Administradora de los Recursos del Sistema General de Seguridad Social en Salud (Giro directo).

- **Comunidad Organizada y Control Social**

Actores sociales que ejercen vigilancia y participan en la toma de decisiones.

- ✓ Junta Directiva: Máximo órgano de dirección de la ESE.
- ✓ Asociación de Usuarios (Alianza de Usuarios): Representantes de los pacientes que velan por la calidad del servicio.
- ✓ Veedurías Ciudadanas: Grupos que vigilan la contratación y ejecución presupuestal.
- ✓ Autoridades Étnicas: Gobernadores Indígenas (Cabildos) y Representantes Legales de Consejos Comunitarios, con quienes se concerta el modelo de atención en salud.
- ✓ Juntas de Acción Comunal (JAC): Líderes barriales y veredales que gestionan brigadas de salud y mejoras en los Puestos de Salud rurales.

- **Proveedores y Aliados Estratégicos**

Empresas privadas que suministran insumos vitales para la operación.

- ✓ Proveedores de Medicamentos y Dispositivos Médicos.
- ✓ Empresas de Mantenimiento Biomédico.
- ✓ Gestores de Residuos Hospitalarios.
- ✓ Empresas de Aseo.
- ✓ Sindicatos que manejan personal
- ✓ Empresas de mantenimiento de equipo industrial

h) Sistemas Salud en el Trabajo

Gestión de Seguridad y Salud en el Trabajo (SG-SST), es implementado por la ESE y consiste en el desarrollo de un proceso lógico y por etapas, basado en la mejora continua, incluye la política, organización, planificación, aplicación, evaluación, auditoría y acciones de mejora con el objetivo de anticipar, reconocer, evaluar y controlar los riesgos que afectan la seguridad y la salud en los espacios laborales. Ver Tabla No. 4

Tabla No.4 Resultado Estándares Mínimos SGSST

cicLo	EsTáNDaR	EsTáNDaR	iTEM	Vr. Est	Puntaje	caLiFic.
Planear	1. Recursos	1.1. Recursos financieros, técnicos humanos y de otra índole requeridos para coordinar y desarrollar el Sistema de Gestión de la Seguridad y Salud en el Trabajo	1.1.1 responsable del Sistema de Gestión de Seguridad y Salud en el Trabajo SG - SST	0.50	Cumple	0.50
Planear	1. Recursos		1.1.2 Responsabilidades en del Sistema de Gestión de Seguridad y Salud en el Trabajo SG - SST	0.50	No aplica	0.50
Planear	1. Recursos		1.1.3 Asignación de Recursos para el Sistema de Gestión de Seguridad y Salud en el Trabajo SG - SST	0.50	Cumple	0.50
Planear	1. Recursos		1.1.4 Afiliación al Sistema General de Riesgos Laborales	0.50	Cumple	0.50
Planear	1. Recursos		1.1.5 Identificación de trabajadores de alto riesgo y cotización de pensión especial	0.50	No aplica	0.50
Planear	1. Recursos		1.1.6 Conformación COPASST	0.50	Cumple	0.50

Planear	1. Recursos		1.1.7 Capacitación COPASST	0.50	No aplica	0.50
Planear	1. Recursos		1.1.8 Conformación Comité Convivencia	0.50	Cumple totalmente	0.50
Planear	1. Recursos	1.2. Capacitación en el Sistema de Gestión de la Seguridad y Salud en el Trabajo	1.2.1 Programa Capacitación Promoción y Prevención	2.00	Cumple totalmente	2.00
Planear	1. Recursos		1.2.2 Inducción y reinducción en Sistema de Gestión de Seguridad y Salud en el Trabajo SG - SST Actividades de Promoción y Prevención P y P	2.00	No aplica	2.00
Planear	1. Recursos		1.2.3 responsables del Sistema de Gestión de Seguridad y Salud en el Trabajo SG - SST con curso virtual de 50 horas	2.00	No aplica	2.00
Planear	2. Gestión integral del sistema de gestión de la seguridad y salud Trabajo	2.1. Política de Seguridad y Salud en el Trabajo	2.1.1 Política del Sistema de Gestión de Seguridad y Salud en el Trabajo SG - SST firmada, fecha y comunicada al COPASST	1.00	Cumple totalmente	1.00
Planear		2.2. Objetivos del SG-SST	2.2.1 Objetivos definidos, claros, medibles, cuantificables, con metas, documentados, revisados del SG - SST	1.00	No aplica	1.00
Planear		2.3. Evaluación inicial del SG-SST	2.3.1 Evaluación e identificación de prioridades	1.00	No aplica	1.00
Planear		2.4. Plan anual de trabajo	2.4.1 Plan que identifica objetivos, metas, responsabilidad, recursos con cronograma y firmado	2.00	Cumple totalmente	2.00
Planear		2.5. Conservación de la documentación	2.5.1 Archivo o retención documental del Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST	2.00	Cumple totalmente	2.00
Planear		2.6. Rendición de cuentas	2.6.1 Rendición sobre el desempeño	1.00	No aplica	1.00
Planear		2.7. Normatividad nacional vigente y aplicable en materia de seguridad y salud en el trabajo	2.7.1 Matriz legal	2.00	No aplica	2.00
Planear		2.8. Comunicación	2.8.1 Mecanismos de comunicación, auto reporte en Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST	1.00	No aplica	1.00
Planear		2.9. Adquisiciones	2.9.1 Identificación, evaluación, para adquisición de productos y servicios en Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST	1.00	No aplica	1.00
Planear		2.10. Contratación	2.10.1 Evaluación y selección de proveedores y contratistas	2.00	No aplica	2.00
Planear		2.11. Gestión del cambio	2.11.1 Evaluación del impacto de cambios internos y externos en el Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST	1.00	No aplica	1.00

Hacer	3. Gestión de la Salud	3.1. Condiciones de salud en el trabajo	3.1.1 Descripción sociodemográfica – Diagnóstico de condiciones de salud	1.00	Cumple totalmente	1.00
Hacer			3.1.2 Actividades de Promoción y Prevención en Salud	1.00	Cumple totalmente	1.00
Hacer			3.1.3 Información al médico de los perfiles de cargo	1.00	No aplica	1.00
Hacer			3.1.4 Realización de Evaluaciones Médicas Ocupacionales -Peligros- Periodicidad- Comunicación al Trabajador	1.00	Cumple totalmente	1.00
Hacer			3.1.5 Custodia de Historias Clínicas	1.00	No aplica	1.00
Hacer			3.1.6 Restricciones y recomendaciones médico/laborales	1.00	Cumple totalmente	1.00
Hacer			3.1.7 Estilos de vida y entornos saludables (controles tabaquismo, alcoholismo, farmacodependencia y otros)	1.00	No aplica	1.00
Hacer			3.1.8 Agua potable, servicios sanitarios y disposición de basuras	1.00	No aplica	1.00
Hacer			3.1.9 Eliminación adecuada de residuos sólidos, líquidos o gaseosos	1.00	No aplica	1.00
Hacer	3. Gestión de la Salud	3.2. Registro, reporte e investigación de las enfermedades laborales, los incidentes y accidentes de trabajo	3.2.1 Reporte Accidentes de Trabajo y Enfermedad Laboral a la ARL, EPS y Dirección Territorial del MinTrabajo	2.00	Cumple totalmente	2.00
Hacer			3.2.2 Investigación de incidentes, accidentes y enfermedades laborales	2.00	Cumple totalmente	2.00
Hacer			3.2.3 Registro y análisis estadístico de accidentes y enfermedades laborales	1.00	No aplica	1.00
Hacer		3.3. Mecanismos de vigilancia de las condiciones de salud de los trabajadores	3.3.1 Medición de la frecuencia de la accidentalidad	1.00	No aplica	1.00
Hacer			3.3.2 Medición de la severidad de la accidentalidad	1.00	No aplica	1.00
Hacer			3.3.3 Medición de la mortalidad por Accidentes de Trabajo	1.00	No aplica	1.00
Hacer			3.3.4 Medición de la prevalencia de Enfermedad Laboral	1.00	No aplica	1.00
Hacer			3.3.5 Medición de la incidencia de Enfermedad Laboral	1.00	No aplica	1.00
Hacer			3.3.6 Medición del ausentismo por causa médica	1.00	No aplica	1.00
Hacer	4. Gestión de peligros y riesgos	4.1. Identificación de peligros, evaluación y valoración de los riesgos	4.1.1 Metodología identificación de peligros, evaluación y valoración de los riesgos	4.00	Cumple totalmente	4.00
Hacer			4.1.2 Identificación de peligros con participación de todos los niveles de la empresa	4.00	No aplica	4.00
Hacer			4.1.3 Identificación de sustancias catalogadas como carcinógenas o con toxicidad aguda	3.00	No aplica	3.00

Hacer			4.1.4 Realización mediciones ambientales, químicos, físicos y biológicos	4.00	No aplica	4.00
Hacer		4.2. Medidas de prevención y control para intervenir los peligros / riesgos	4.2.1 Implementación de medidas de prevención y control de peligros/riesgos identificados	2.50	No aplica	2.50
Hacer			4.2.2 Verificación de aplicación de medidas de prevención y control por parte de los trabajadores	2.50	No aplica	2.50
Hacer			4.2.3 Elaboración de procedimientos, instructivos, fichas, protocolos	2.50	No aplica	2.50
Hacer			4.2.4 Realización de inspecciones a las instalaciones, maquinaria o equipos con la participación del COPASST	2.50	No aplica	2.50
Hacer			4.2.5 Mantenimiento periódico de instalaciones, equipos, máquinas, herramientas	2.50	Cumple totalmente	2.50
Hacer			4.2.6 Entrega de Elementos de Protección Personal EPP, se verifica con contratistas y subcontratistas	2.50	Cumple totalmente	2.50
Hacer	5. Gestión de amenazas	5.1. Plan de prevención, preparación y respuesta ante emergencias	5.1.1 Se cuenta con el Plan de Prevención, Preparación y Respuesta ante emergencias	5.00	Cumple totalmente	5.00
Hacer			5.1.2 Brigada de prevención conformada, capacitada y dotada	5.00	Cumple totalmente	5.00
Verificar	6. Verificación del SG - SST	6.1. Gestión y resultados del SG - SST	6.1.1 Definición de indicadores del SG-SST de acuerdo condiciones de la empresa	1.25	No aplica	1.25
Verificar			6.1.2 La empresa adelanta auditoría por lo menos 1 al año	1.25	No aplica	1.25
Verificar			6.1.3 Revisión anual por la alta dirección, resultados y alcance de la auditoría	1.25	Cumple totalmente	1.25
Verificar			6.1.4 Planificación auditorías con el COPASST	1.25	No aplica	1.25
Actuar	7. Mejoramiento	7.1. Acciones preventivas y correctivas con base en los resultados del SG - SST	7.1.1 Definición de acciones preventivas y correctivas con base en resultados del SG-SST	2.50	No aplica	2.50
Actuar			7.1.2 Acciones de mejora conforme a revisión de la alta dirección	2.50	No aplica	2.50
Actuar			7.1.3 Acciones de mejora con base en investigaciones de accidentes de trabajo y enfermedades laborales	2.50	No aplica	2.50
Actuar	7. Mejoramiento	7.1. Acciones preventivas y correctivas con base en los resultados del SG - SST	7.1.4 Elaboración Plan de Mejoramiento e implementación de medidas y acciones correctivas solicitadas por autoridades y ARL	2.50	No aplica	2.50
Total, Valor Estándar Valores Mínimos de Calificación						100.00

Fuente: ARL Positiva

i) Sistema de Gestión de la Calidad

Sistema integrado por cuatro componentes principales: el Sistema Único de Habilitación, la Auditoría para el Mejoramiento de la Calidad, el Sistema Único de Acreditación y el Sistema de Información para la Calidad.

- **Acreditación**

Evalúa a las instituciones, buscan cumplir con estándares de alta calidad, que van más allá de los requisitos básicos de habilitación, los resultados registrados son generados por la Autoevaluación realizada por la ESE, de acuerdo al Anexo de la Resolución 5095 de 2018.

Tabla No. 5 Resultados Autoevaluación Acreditación 2025

Estándar	Calificación
8.1 Grupo de Estándares Asistenciales	1,26
8.2 Grupo de Estándares de Direccionamiento	1,23
8.3 Grupo de Estándares de Gerencia	1,22
8.4 Grupo de Estándares de Gerencia del Talento Humano	1,15
8.5. Grupo de Estándares de Gerencia del Ambiente Físico	1,22
8.6 Grupo de Estándares de Gestión de Tecnología	1,21
8.7 Grupo de Estándares de Gerencia de la Información	1,17
8.8 Grupo de Estándares de Mejoramiento de la Calidad	1,32
TOTAL DE CALIFICACIÓN	1,22

Fuente: Autoevaluación

- Sistema Único de Habilitación:

Sistema Único de Habilitación, se muestra resultado según informe generado por la Secretaria de Salud Departamental del Cauca, el 28 de agosto de 2025. Ver Tabla No. 6

Tabla No. 6 Resultados SUHC 2025

NAP	Talento Humano	Infraes.	Dota.	Mtos, DM e Insumos	Procesos Prioritarios	Historia Clínica	Interde. De Servicios	Tot Estándares
Nariño	66,7	97,78	71,43	63,41	39,02	47,62	100	69,42
Canalón	66,7	90	71,43	36,59	39,02	47,62	100	64,48
Centro	66,7	77,51	75,51	36,59	39,02	47,62	100	63,28
Mondomo	66,7	100	71,43	36,59	39,02	42,86	100	65,23
Morales	71,43	93,18	71,43	36,59	39,02	47,62	100	65,61
Total NAP	67,65	91,69	72,25	41,95	39,02	46,67	100	

Fuente: Informe SSDC

Se evidencia el no cumplimiento al Sistema Único de Habilitación, para lo cual se proyectó plan de mejoramiento para cerrar brechas que se trabajara a mediano plazo.

- Auditoria para el Mejoramiento de la Calidad (PAMEC)

Mecanismo para evaluar y mejorar continuamente la calidad de la atención que se presta, que ejecuta mediante el Plan de Auditoria para el Mejoramiento de la calidad (PAMEC), el resultado de este sistema se da de acuerdo a auditoría realizada por la Secretaria de Salud Municipal de Santander, realizada el 21 de noviembre de 2025. Ver Tabla No. 7

Tabla No. 7 Resultados Evaluación PAMEC 2025

CRITERIO	C	NC
ALCANCE DEL MEJORAMIENTO CONTINUO DE LA CALIDAD	X	
Autoevaluación	X	
Procesos A Mejorar	X	
Priorización De Procesos		X
Definición De La Calidad Esperada	X	
Definición Calidad Observada	X	
Formulación Planes De Mejoramiento	X	
Implementación De Los Planes De Mejora		
Evaluación Ejecución De Los Planes De Mejoramiento	X	
Aprendizaje Organizacional		X
Reporte Circular 012 De 2016	X	
Total Criterios	9	2
% Cumplimiento PAMEC	81,82	

Fuente: Acta No. 4 de 2025 SSMP

- Sistema de Información

Recopila datos e indicadores para monitorear la calidad de los servicios y tomar decisiones informadas, el resultado de este sistema se da de acuerdo a los resultados de la Asistencia Técnica realizada por la SSDC, el día 06 de noviembre de 2025. Ver Tabla No. 8

- Sistema Ambiental

La gestión ambiental de la ESE, está enfocada en garantizar la gestión de residuos hospitalarios, el manejo de sustancias químicas (fumigación), el consumo de agua y energía, y la minimización de la contaminación. El resultado de esta gestión se ve reflejado en el informe de visita de la CRC realizado en noviembre de 2025. Ver Tabla No. 9

Tabla No. 9 Resultado visita CRC - 2025

ASPECTOS A VERIFICAR	C	NC	NA
¿Se encuentra en la instalación el plan de gestión integral de residuos sólidos peligrosos actualizado?	x		
¿Identifican claramente en que lugares del proceso se generan residuos peligrosos?	x		
¿Los residuos están clasificados según su peligrosidad?	x		
¿Existen recipientes apropiados para la segregación en fuente de residuos (Estado, características rotulación)?	x		
¿Presentan plano de rutas internas para el movimiento interno de residuos??	x		

¿Presentan un Plan de Contingencia que Incluya la descripción de protocolos para emergencias relacionadas con el manejo de respel?	x		
¿Existen condiciones apropiadas técnicas y de manejo en el sitio de almacenamiento interno de residuos (pisos, paredes, iluminación drenajes y sistema de pesaje, etc)?	x		
¿Presentan indicadores para medir la efectividad del Plan de gestión Integral de Residuos?	x		
¿Presentan actualizado el Registro de Generadores de Residuos o Desechos Peligrosos en la Plataforma del IDEAM?	x		
¿Cuentan con permiso de vertimientos vigente?		x	
¿Cuentan con permiso de emisiones Atmosféricas vigente?			x
¿La gestión externa de residuos peligrosos es realizada por el generador o por terceros?	x		
¿Se informa nombre del transportador de residuos peligrosos o razón social de la empresa gestora?	x		
¿Existe contratos con la empresa que realiza disposición final y/o gestión externa?	x		
¿Realizan actividades de valorización y, aprovechamientos de residuos sólidos Peligrosos?			x
¿Realizan actividades de Tratamiento de residuos sólidos Peligrosos?			x
¿Realizan actividades de Disposición final de residuos Presta de servicio de Almacenamiento externo de residuos sólidos Peligrosos?			x
¿Presenta licencia Ambiental para las actividades de Aprovechamiento, Tratamiento ylo Disposición Final de Residuos Peligrosos?			x
¿Describen claramente el proceso de valorización, aprovechamientos, Tratamiento y/o Disposición final de residuos sólidos Peligrosos?			x
¿El parque automotor destinado al transporte de Residuos Sólidos Peligrosos cumple con las? especificaciones (técnicas contenidas en la normatividad			x
¿Presentan un Plan de Contingencia que incluya la descripción de protocolos para emergencias relacionadas con el Transporte de Residuos peligrosos?			x
¿Presentan certificados o soportes de gestión externa emitidas por el receptor de residuos Sólidos Peligrosos?	x		
TOTAL	13	1	8
Porcentaje Cumplimiento	92,86		

- Infraestructura Tecnológica

Se identifica los componentes de la línea base de la arquitectura tecnológica en servicios de infraestructura, con los que la ESA cuenta: Ver Ilustración No. 1

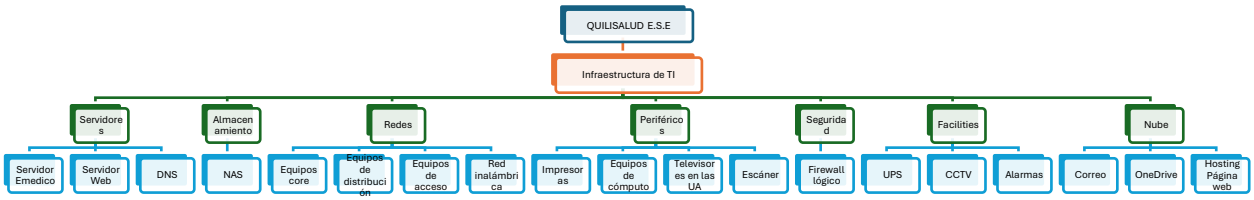


Ilustración 1 Vista conceptual de Arquitectura de Tecnología de línea Base de la ESE Quilisalud

- **Arquitectura de Infraestructura tecnológica**

- Catálogo de Servicios de Infraestructura de TI

Tabla 10 Servicios de Infraestructura de TI de la ESE Quilisalud 2025

ID servicios de infraestructura	Servicio de infraestructura	Descripción
ST.SI.01	Nube	Servicio privado donde se aloja la página web de la ESE, tiene el servicio de correo electrónico con Microsoft, almacenamiento en OneDrive y su ofimática disponible.
ST.SI.02	Redes	Servicio LAN y Wifi que le permite a los usuarios de la entidad a acceder a los sistemas de información
ST.SI.03	Seguridad	Servicio de seguridad perimetral, controlar el tráfico de red desde y a hacia Internet y protege contra ataques externos
ST.SI.04	Servidores	infraestructura de hardware para el alojamiento de aplicaciones
ST.SI.05	Almacenamiento	Servicio de infraestructura de hardware para el almacenamiento de información utilizada inicialmente con la información de respaldo del servidor HIS y ERP
T.SI.06	Facilities	Servicios asociados el centro de cómputo para garantizar la disponibilidad de los servicios alojados.
ST.SI.07	Periféricos	Servicios asociados a los equipos asignados a los usuarios finales como son computadoras e impresoras.

- Catálogo de Elementos de Infraestructura

Tabla 11 Elementos de Infraestructura de TI

Id	Elemento de infraestructura	Tipo	Servicio de Infraestructura involucrado
IT01	Servidor físico HIS y ERP	Instalado en sitio	Servicio de gestión de base de datos del sistema HIS y ERP
IT02	Servidor IIS	Instalado en sitio	Servicio de IIS del sistema HIS y ERP
IT03	Red de almacenamiento - NAS	Instalado en sitio	Servicio de almacenamiento y respaldo físico: servidor del HIS y ERP.
IT04	Antivirus	Instalado en sitio	Servicio de seguridad
IT05	Firewall lógico	Instalado en sitio	Servicio de acceso red interna
			Servicio de DMZ
IT06	Servidor RFAST	Instalado en sitio	Servicio de aplicación
IT07	Servidor DNS	Instalado en sitio	Servicio de enrutamiento
IT08	Servidor VPN	Instalado en sitio	Servicio de conexión remota
IT09	Sistema de archivos	Instalado en sitio	Servicio de almacenamiento
IT10	Certificados de seguridad	Instalado en sitio	Servicio de seguridad
IT11	Software de ofimática	Instalado en sitio y Software con servicio en la nube	Servicio de instalación de software
IT12	Servidor correo electrónico	Software servicio en la nube	Servicio de correo electrónico
IT13	Router	Instalado en sitio	Servicio de red LAN, Servicio de red WAN Y Servicio de WIFI
IT14	Switch	Instalado en sitio	Servicio de red LAN y red WAN
IT15	Ubicación física Datacenter	Instalado UA Morales Duque	Servicio de Colocación
IT16	Computador personal	Instalado en sitio	
IT17	Impresoras	Instalado en sitio	Servicio de impresión
IT18	Escáner	Instalado en sitio	Servicio de escaneo

- **Administración de la capacidad de la Infraestructura tecnológica**

Los servicios de TI de Quilisalud, son adminsitrados por la oficina de Gestión de Tecnologías, los cuales son:

- ✓ **Infraestructura - Centro de Datos :** Se cuenta con centro de datos ubicados en el NAP de Morales Duque, espacio el cual, aunque no cumple con todo el lleno de requisitos técnicos, es un espacio específico con seguridad, condiciones ambientales que aseguran el correcto ambiente para los servidores y equipos de comunicación. Actualmente la ESE está en el proceso de una nueva construcción de una unidad de atención y está en revisión si el data center será traslado para este nuevo espacio, en el cual se espera cumplir con todos las condiciones técnicas o si al terminar la evaluación, se decide por reestructurar este espacio en la actual ubicación.
- ✓ **Hardware y Software de Oficina**: Todos los equipos de cómputo son instalados y administrados mediante diferentes mecanismos como el estar dentro del Servidor de dominio, cuentan con protección antivirus gestionados por políticas en la consola de administración del antivirus. Para controlar la instalación de software no autorizado, las cuentas de usuarios finales son estándar y en caso de requerir agregar un nuevo aplicativo, debe de notificarse a la oficina de Gestión de Tecnologías de Quilisalud.
- ✓ **Conectividad:** La ESE cuenta con espacios físicos ubicados en diferentes partes del casco urbano donde por medio de canal de datos en fibra óptica se suministra acceso al data center y para el NAP de Mondomo la conexión es por medio de radio enlace.
- ✓ **Red Local e Inalámbrica:** Recientemente en todas las unidades de administración, se implantó la conexión por red local, pensando en ampliar las posibilidades de conectividad para dispositivos móviles para realizar encuestas y el diligenciamiento por medio de tabletas la captura de firmas para los consentimientos informados.
- ✓ **Red WAN:** El parque tecnológico de TI en la ESE cuenta con el servicio de conectividad con servicio de internet dedicado de 30 MB y se conduce por medio del servicio de conectividad a las sedes. De manera particular las sedes administrativas poseen alternamente el servicio por aparte.
- ✓ **IPV6:** La ESE, se encuentra trazando ruta de trabajo para implementación de este protocolo, a la par, adelantar ejercicios relacionados de modelos: MSPI y el MAE.
- ✓ **Continuidad y Disponibilidad:** La ESE cuenta con sistemas de respaldo de corriente y circuitos regulados con UPS, los cuales proporcionan elementos para la continuidad del servicio del cableado estructurado, pero en el momento sólo las UA propias cuentan con planta eléctrica propia, dejando por fuera la UA de riesgo y la sede centro. Estos sistemas ya presentan un nivel alto de obsolescencia y se trabajó en conjunto con planeación en la presentación de un proyecto para inversión en compras de UPS.
- ✓ **Gestión de ANS:** No se cuenta con sistema especial de atención de incidentes, tiene un mecanismo donde se llevan métricas y seguimientos para la gestión de incidencias.

- **Administración de la operación**

Los servicios tecnológicos de la ESE busca garantizar la disponibilidad y continuidad de servicios tecnológicos por medio de procesos, procedimientos, actividades y herramientas.

Tabla 12 Operación de los Servicios Tecnológicos

Identificador	Descripción	Sí	No
Monitoreo de la infraestructura de TI	Herramientas, actividades o procedimiento de monitoreo para identificar, monitorear y controlar el nivel de consumo de la infraestructura de TI	X	
Capacidad de la infraestructura tecnológica	Se realizan planes de capacidades que permiten proyectar las capacidades de la infraestructura a partir de la identificación de las capacidades actuales	X	
Disposición de residuos tecnológicos	Se cuenta con procesos y procedimientos para una correcta disposición final de los residuos tecnológicos	X	

Fuente: Oficina de Sistemas

La entidad implementa los procesos de soporte y mantenimiento preventivo y correctivo de los servicios tecnológicos, de acuerdo con las necesidades de su operación.

Tabla 13 Matriz de Mantenimientos

Identificador	Descripción	Sí	No
Acuerdos de Nivel de Servicios	Establece Acuerdos de Nivel de Servicios y vela por el cumplimiento	X	
Mesa de Servicio	Se tienen herramientas, procedimientos y actividades para atender requerimientos e incidentes de infraestructura tecnológica	X	
Planes de mantenimiento	Se generan y ejecutan planes de mantenimiento preventivo y evolutivo sobre la infraestructura de TI.	X	

Fuente: Oficina de Sistemas

8.4 NIVELES DE RESPONSABILIDAD DE LA GESTIÓN DEL RIESGO

8.4.1 Línea Estratégica

Responsabilidad frente al Monitoreo de Riesgos

a. Alta dirección:
   - Rediseña política de Gestión del Riesgo y la presenta ante el CGDI, para su revisión.

b. Comité de Gestión y Desempeño Institucional (CGDI):

- Encargado de revisar la propuesta de Política de Gestión del Riesgo y da su visto bueno o recomendaciones para ajuste, una vez tenga el aval pasa al CICI para su aprobación.
- Una vez aprobada la política por el CICCI, analiza periódicamente la gestión del riesgo y da lineamientos para aplicación de mejoras

c. Comité Institucional de Coordinación de Control Interno (CICCI)

- Es el encargado de aprobar la Política de Gestión del riesgo
- Se encarga también de subir el análisis de eventos y riesgos que ya se materializaron y son críticos para la ESE.
- Retroalimentar al CGDI sobre ajustes que deban hacer frente a la gestión del riesgo

Evaluar el estado del sistema de Control Interno, acorde con la información generada por parte de las instancias de 2ª línea identificadas y la actividad de control definida que materializa las líneas de reporte en cada caso, de acuerdo con el tema del cual son responsables, a fin de generar acciones y toma de decisiones con enfoque preventivo.

8.4.2 Primera Línea de Defensa

- Está conformada por los lideres y equipo que hacen parte del proceso o servicio
- Gestiona los riesgos de sus procesos y servicios y hacer seguimiento.
- Realiza autoevaluación para establecer eficiencia, eficacia y efectividad de controles
- Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo
- Diseña mapa de riesgos por proceso o servicio y lo presenta ante planeación.
- Definir, aplicar y hacer seguimiento a controles para mitigar riesgos identificados, proponer mejoras a la gestión del riesgo en su proceso y además reporta a la 2ª Línea de defensa, avances y evidencias de la gestión de riesgos en los plazos establecidos.

8.4.3 Segunda Línea de Defensa

- Está conformada por procesos transversales de la ESE (Planeación y Calidad)
- Asesorar a la línea estratégica: Analizar el contexto interno y externo, para la definir la política de riesgo, establecer los niveles de impacto y aceptación del riesgo
- capacitar, acompañar, definir metodologías y generar recomendaciones para la Gestión del Riesgo a los lideres de procesos y servicios.
- Consolidar Mapa de Riesgos (mayor criticidad frente al logro de objetivos), presentar para análisis y seguimiento al Comité de Gestión y Desempeño Institucional
- Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones
- Presentar al CICCI el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad

Consolidar mapa de riesgos institucional, con un enfoque para el análisis de riesgos de mayor criticidad frente al logro de objetivos y presentarlo periódicamente semestralmente ante la Línea Estratégica para su análisis y toma de decisiones correspondiente.

8.4.4 Tercera Línea de Defensa:

- Conformada por la oficina de control interno
- Asesorar de forma coordinada con la Oficina de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles
- Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al CICCI
- Recomendar mejoras a la política de administración del riesgo.
- Informar sobre auditorias basadas en riesgos, con énfasis en riesgos fiscales

8.5 ESQUEMA METODOLOGICO

Se consideran los siguientes elementos básicos: Tabla factores de riesgo; Tablas de probabilidad e impacto; Matriz de severidad y Tabla valoración controles.

8.5.1 Aspectos Claves

Tabla de Factores de Riesgos, probabilidad, impacto, matriz severidad. Otros elementos como Riesgo fiscal, corrupción y seguridad de la información . Ver Figura No.3

Figura No. 3 Aspectos metodológicos necesarios para Anexo Política

Fuente: Guía Gestión del Riesgo DAFP V7

8.5.2 Apetito del Riesgo

la política para la gestión integral del riesgo establece el apetito del riesgo, es necesario precisar su aplicación, para lo cual, a continuación, se definen los aspectos clave necesarios para su análisis, los cuales, en todo caso dependerán de la decisión de la Alta Dirección o Línea Estratégica en el marco del Comité Institucional de Coordinación de Control Interno, Comité de Auditoría u otra instancia de este mismo nivel jerárquico. Para poder iniciar con el análisis del apetito de riesgo, es necesario comprender la misión, visión, objetivos y estrategias, ya que este despliegue de la plataforma estratégica permite tener una perspectiva sobre el tipo y nivel de riesgo que es probable que enfrente la ESE.

En este marco general, la ESE debe relacionar el riesgo y el desempeño, ya que a partir de los resultados alcanzados es posible obtener información valiosa para la definición del apetito del riesgo, dado que, "*al observar el desempeño actual, se puede identificar cómo tendencias, relaciones y otros factores actuales están afectando el perfil de riesgo*"

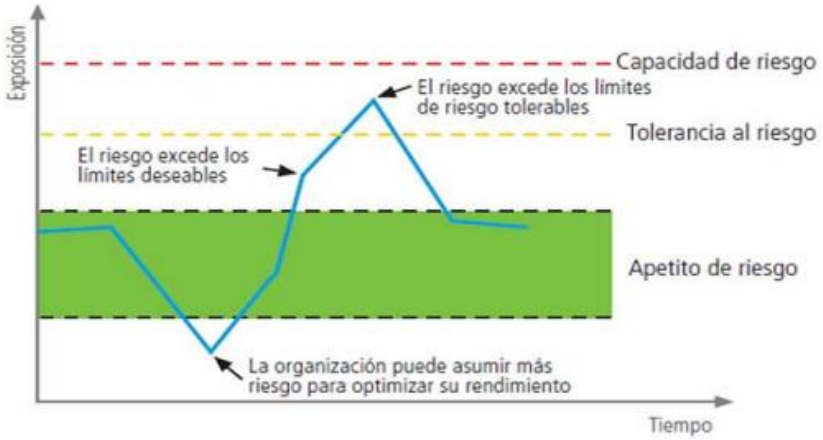
En cuanto a los parámetros a utilizar para su definición, se considera el análisis cualitativo y cuantitativo, Se debe tener en cuenta que:

- Las declaraciones cualitativas se describen los riesgos específicos de la
- Institución que está dispuesta a aceptar;
- Las declaraciones cuantitativas, describen límites, umbrales o indicadores clave de riesgo.
- Establecen cómo han de ser juzgados los riesgos y sus beneficios y/o cómo evaluar y vigilar el impacto agregado de estos riesgos.
- Asimismo, se considera aquellos elementos del apetito de riesgo que no se pueden medir y que, por tanto, podrían ser más difíciles de gestionar, como los riesgos reputacionales. Las medidas cuantitativas se combinen con las medidas cualitativas,
- Los riesgos de tolerancia cero, son: Los relacionados con incumplimientos legales o regulatorios, con seguridad de los empleados y de fuerte impacto medioambiental.

En Gobernanza, en riesgo y control, para el análisis de apetito del riesgo lo siguiente:

- **Apetito de riesgo:** Nivel de riesgo que la ESE está dispuesta a asumir en relación con sus objetivos, el marco legal y las disposiciones de Gerencia..
- **Tolerancia del riesgo:** es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- **Capacidad de riesgo:** Máximo valor del nivel de riesgo que puede soportar y a partir del cual la Gerencia considera que no sería posible el logro de objetivos de la ESE. (relacionado con la solvencia y liquidez). Ver Figura No. 4

Figura No. 4 Capacidad, Límites y Tolerancia al Riesgo



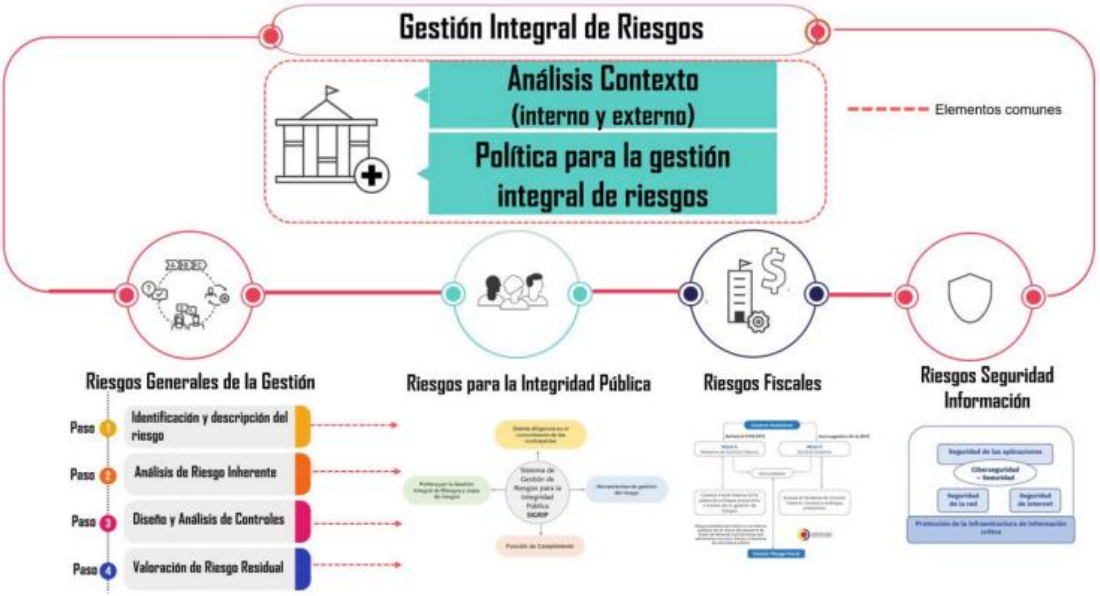
Fuente: *Superintendencia Financiera de Colombia. 2023*

8.5.3 **Articulación ámbitos para la gestión integral de riesgos:**

Se articula, el análisis integral de riesgos que afectaran el cumplimiento de funciones y objetivos de la ESE, como afectación al patrimonio público, vulneración a activos de información, afectación a la confianza de las partes interesadas en el uso del entorno digital y conductas asociadas a comportamientos no éticos que van en contravía del ejercicio íntegro del servidor. Además de los ámbitos que se involucran en la gestión del riesgo, con

sus elementos comunes que corresponden al análisis del contexto estratégico interno y externo, la definición de la política para la gestión del riesgo y los pasos metodológicos aplicables de: i) identificación y descripción del riesgo, ii) análisis del riesgo inherente, iii) diseño y análisis de controles y iv) valoración del riesgo residual

Figura No. 5 Articulación ámbitos gestión del riesgo



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

8.5.4 Riesgos Generales de Gestión

Se desarrolla en pasos necesarios para: Identificación y tratamiento de riesgos asociados a la operación, al ser propios o intrínsecos de procesos, funciones y misionalidad.

8.5.4.1 Paso 1 Identificación y descripción del riesgo

a) Identificación de riesgos claves y asociación de estos frente a los objetivos previamente identificados:

Son aquellos eventos que podrían afectar de forma previsible el logro de los objetivos del proceso. En el análisis se considera, además del objetivo, la estructura, sus actividades claves y la participación dentro de la cadena de valor o ciclo de los procesos.

b) Identificación de áreas de impacto:

Consecuencia económica o reputacional, a la que se expone a la ESE en caso de materializarse un riesgo.

c) Identificación de áreas de factores de riesgo:

Son las fuentes generadoras de riesgos. Esto es circunstancias o condiciones que aumenta la probabilidad de que ocurra el evento de riesgo, bien sea de fuente interna o externa. No son causas directas, pero incrementan el nivel de exposición.

En la Tabla 14 se establece un listado con factores de riesgo que pueden incidir en un proceso, los cuales podrán ampliarse o adecuarse de acuerdo a las características propias de cada proceso, para una adecuada identificación del riesgo.

Tabla No 14 Factores de Riesgos

Factor	Definición		Descriptores
Ejecución y administración de procesos	Eventos relacionados con la ejecución de los procesos y procedimientos determinados para la operación de la entidad, uso de sistemas de información, por errores en las actividades que deben realizar los servidores de la organización. Estructura organizacional que afecta la capacidad organizacional		Falta de aplicación de los procedimientos
			Falta segregación de funciones
			Errores de grabación, autorización
			Falta de supervisión o interventoría

Factor	Definición		Descriptores
			Errores en cálculos para pagos internos y externos
			Alta rotación o insuficiencia de personal
			Acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad en el trabajo
			Acciones contrarias a las leyes o acuerdos contractuales
			Falta de capacitación y otros temas relacionados con el personal
Transacción u Operación (aplica para LA/FT/FP	Eventos relacionados con transacciones y Operaciones realizadas por un cliente o usuario, que accede o entrega un bien o servicio a la entidad, a través de los canales dispuestos y en una jurisdicción específica.		Contrapartes de la entidad (naturales o jurídicas)
			Productos (bienes o servicios) que oferta/requiere
			Canales utilizados para la operación
			Jurisdicciones (nacional o territorial)
Talento humano	Eventos relacionados con las conductas o comportamientos de los empleados que afectan la Integridad Pública.		Fraude Interno
			Soborno
			Gestión inadecuada de conflicto de Intereses
			Corrupción

Factor	Definición		Descriptores
			Hurto activos
Tecnología	Eventos relacionados con la infraestructura tecnológica de la entidad.		Daño de equipos
			Caída de sistemas de información y aplicaciones
			Caída de redes
			Errores en hardware o software
			Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.		Derrumbes
			Incendios
			Inundaciones
			Daños a activos fijos
Evento externo	Eventos por situaciones externas que afectan la entidad.		Fraude Externo

Factor	Definición		Descriptores
			Suplantación de identidad
			Asalto a la oficina
			Atentados, vandalismo, orden público

d) Descripción del Riesgo

A partir del punto de riesgo, área de impacto y área(s) de factor(es) de riesgo identificados, se debe proceder con la descripción del riesgo.

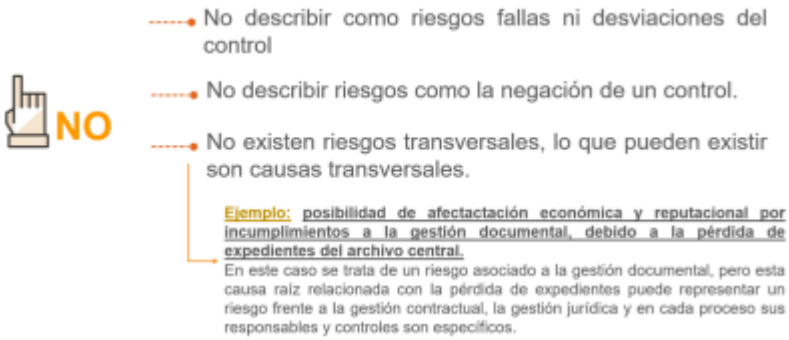
- Impacto: las consecuencias (afectación económica (o presupuestal) y/o afectación reputacional) que puede ocasionar a la organización la materialización del riesgo.

- Causa inmediata: circunstancia o situación más evidentes sobre la cual se presenta el riesgo, las mismas no constituyen la causa principal para que se presente el riesgo.
- Estos dos elementos permiten plantear el evento no deseado (¿qué puede ocurrir?), es decir la situación, acción, condición o suceso incierto que, si ocurre, podría afectar el logro de los objetivos de la entidad.
- Características clave: Debe ser específico y claro, no genérico. Expresado en términos de qué podría pasar.
- Causa raíz: Se plantea ¿por qué puede ocurrir? el evento, bajo análisis de la causa principal o básica, razones por la cuales se puede presentar el riesgo, información esencial para definición de controles, del paso 3 diseño y análisis de controles. Para un mismo riesgo pueden existir más de una causa o subcausas que se analiza.
- Las características clave: Identificar causas raíz y condiciones contribuyentes que se clasifican: humanas, tecnológicas, normativas, ambientales, organizacionales.
- Un adecuado análisis de causa raíz: Diferencia la causa raíz, de la causa inmediata, entendida esta última como las circunstancias más evidentes sobre la cual se presenta el riesgo y que en ocasiones, no constituyen la causa principal del riesgo. Para facilitar la redacción adecuada del riesgo y desplegar detalles necesarios para la identificación, se propone la siguiente estructura. Ver figura No. 6 y 7

Figura No. 6 Estructura para la redacción del riesgo

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

Figura No. 7



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

Bajo las anteriores consideraciones, una representación simplificada del modelo de descripción del riesgo contiene los siguientes elementos:

- Evento no deseado y sus posibles consecuencias: ¿Qué puede pasar?
- Causas: ¿Por qué puede pasar?
- Tipología: ¿A qué categoría pertenece?
- Factor de riesgo: ¿Qué condición aumenta su probabilidad?

8.5.4.2 Paso 2: Análisis de Riesgo Inherente

a) Determinar la probabilidad:

Posibilidad de ocurrencia del riesgo, está asociada a la exposición al riesgo del proceso o actividad. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo (1 año). Con ello se determina la frecuencia con la que se lleva a cabo la actividad que genera la exposición al riesgo identificado. Ejemplo de actividades relacionadas con la gestión, para definir escala de probabilidad: Ver Tabla No. 15

Tabla 15 Actividades relacionadas con la gestión en entidades públicas

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Muy Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

La exposición al riesgo esta asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, en la Tabla 16 se establecen los criterios para definir el nivel de probabilidad.

Tabla 16 Criterios para definir el nivel de probabilidad

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

b) Determinar el Impacto

Consecuencias de materialización del riesgo. Cómo Impactos económicos y reputacionales como variables principales, afectaciones de ejecución presupuestal, pagos de sanciones económicas, indemnización a terceros, sanciones por incumplimientos legal; afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, estos temas se agrupan en impacto económico y reputacional, para facilitar y evitar la subjetividad del análisis por parte de líderes. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional con diferentes niveles, se deberá tomar el nivel más alto. Ejemplo: Se tiene un impacto económico en nivel mayor y uno reputacional en nivel moderado, se tomará el más alto, el del nivel mayor. se establecen los criterios para definir el nivel de impacto.

Tabla 17 Criterios para definir el nivel de impacto

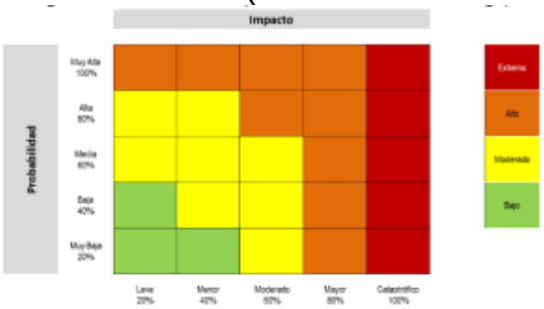
Nivel de Impacto	Afectación Económica	Afectación Reputacional
Leve-20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad.
Menor-40%	Mayor a 10 SMLMV y Menor a 50 SMLMV	El riesgo afecta la imagen de la entidad a nivel interno, de conocimiento general, de junta directiva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

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

c) Análisis de severidad:

Determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor (ver Figura No. 8

Figura No. 8 Matriz de calor (niveles de severidad del riesgo)



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar el nivel de **RIESGO INHERENTE**.

8.5.4.3 Paso 3: Diseño y Análisis de Controles

Son acciones concretas, con atributos específicos establecidas a través de políticas, procedimientos u otras directrices o documentos institucionales e implementadas con el propósito de ofrecer una seguridad razonable respecto al logro de los objetivos. Para la identificación o bien el diseño de controles se debe tener en cuenta que:

- Se diseñan y establecen para cada riesgo a través de diferentes mecanismos, entrevistas con los líderes de procesos o servidores expertos, o a través del análisis de procedimientos, manuales, guías y/o instructivos que el líder del proceso haya diseñado para la gestión de la actividad que genera la exposición al riesgo.
- Considerar los diferentes atributos de las actividades de control para asegurar: responsables de ejecución, segregación de funciones y niveles de autoridad.
- Las actividades de control atenderán las causas raíz y se enfocaran en la gestión de factores de riesgo. Estas serán mayormente efectivas cuando cuenten con todos sus atributos y cuando estén directamente relacionadas con las causas y los factores.

a) **Estructura para la Descripción del Control:** Se despliega en la figura 9.

Figura 9 Estructura para la redacción de controles

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

Desglosando la estructura propuesta tenemos el despliegue de atributos para el control así:

- Responsable: Cargo de la persona que ejecuta el control, estructura organizacional y las denominaciones de empleo (Gerente, coordinadores, profesionales, asistenciales), su despliegue en grupos de trabajo internos, incluye coordinadores de proyectos. Cuando se trate de controles automáticos se identifica el responsable de su calibración o parametrización periódica en el software a través del cual opere el control. Considerar que cuente con un nivel de autoridad apropiado de cara a la actividad de control, así como aspectos básicos de segregación de funciones para evitar que quién sea la fuente generadora de riesgo, sea el único que aplica alguna actividad de control.
- Acción: Determina para qué se realiza el control, se utilizar verbos fuertes como: Verificar, validar, conciliar, comparar, revisar, cotejar, detectar.
- Atributos Informativos o de formalización del control: Corresponde a los detalles que permiten al responsable implementar el control, tal como ha sido establecido o diseñado. Se contemplan los siguientes aspectos:

- ✓ Documentación: se refiere a la fuente documental de los controles, bien sea que su definición esté en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.
- ✓ Frecuencia: corresponde a la periodicidad con la cual se ejecuta una actividad de control debe ser adecuada para detectar o prevenir el riesgo en función de su nivel de exposición inherente. (puede ser periódica o por evento).
- ✓ Evidencia: permite contar con una trazabilidad en la ejecución del control. Puede ser registro físico manual o registro electrónico.
- ✓ Ejecución: establece cómo se ejecuta el control (fuentes de información confiables), al igual acciones a tomar en caso de desviaciones o situaciones que se detecten.

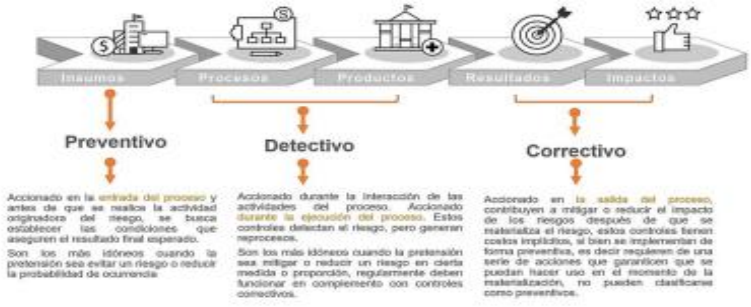
Se tiene entonces que, para la redacción del control es necesario aplicar todos los atributos acá descritos, de manera tal que se constituyan en una herramienta de control efectiva, los cuales se agrupan a través de la estructura para la redacción del control.

b) Tipologías de Controles:

Para establecer la tipología de controles para su validación, es necesario acudir al ciclo de los procesos, con el fin de precisar cuándo se activa un control y, por lo tanto, determinar si se trata de un control preventivo, defectivo o correctivo, o bien una combinación de estos.

Para comprender esta estructura conceptual, a continuación, se consideran desde la cadena de valor de los procesos, con el fin de establecer en qué momento se activa el control en función de las actividades clave del proceso, base para la definición de los controles aplicables en sus 3 tipologías que se explican más adelante (Ver figura 10):

Figura No. 10 Tipos de Controles y su aplicación



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

De acuerdo con el anterior esquema en el ciclo de un proceso, tenemos las siguientes tipologías de controles:

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

- **Control correctivo:** Accionado en la salida del proceso y después de que se materializa el riesgo, tienen costos implícitos. Se contemplan pólizas de seguro, copias de seguridad (*backup*), bancos de datos u otros mecanismos que permiten enfrentar el riesgo una vez materializado, los cuales se implementan de forma preventiva, es decir requieren de una serie de acciones que garanticen que se puedan hacer uso en el momento de la materialización pero no pueden clasificarse como preventivos, ya que sería una sobrevaloración de control que podría generar análisis errados en los niveles de severidad. En consecuencia, si bien estos controles requieren en su diseño que se apliquen actividades con un enfoque preventivo, al momento de materialización del riesgo deben ser considerados como controles correctivos. Así mismo, de acuerdo con la forma como se ejecutan tenemos:
  - ✓ **Control manual:** ejecutados por personas.
  - ✓ **Control automático:** ejecutados por un sistema o software previamente programado diseñado.

c) Valoración de Controles:

La tabla aplicable para la valoración de controles, determina la forma como se califican los atributos o características de **Eficiencia**. Los atributos informativos o de formalización del control, de la figura No. 9 Estructura para la Descripción del Control no se aplican en la valoración, pero deben analizarse para garantizar su diseño. Ver tabla No.18 y 19.

Tabla No. 18 Valoración de controles

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
*Implementación *Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

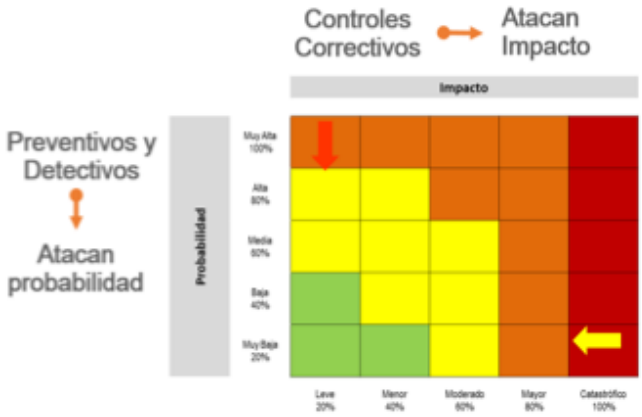
Tabla No. 19 Valoración de controles

Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

d) Aplicación de Controles en la matriz de severidad:

Teniendo en cuenta que es a partir de los controles que se dará el movimiento en la matriz de calor, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles. Ver Figura No. 11

Figura 11 Movimiento en la matriz de calor acorde con el tipo de control



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

8.5.4.4 Paso 4: Valoración de Riesgo Residual

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que, estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control. Para mayor claridad, se despliega un ejemplo, donde se observan los cálculos requeridos para la aplicación de 2 controles, uno preventivo y uno detectivo. Ver Tabla No. 19

Tabla 19 Aplicación de controles para establecer el riesgo residual

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

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

Gráficamente el movimiento en la matriz de calor se muestra en la figura 12:

Figura 12 Movimiento en la matriz de calor con el ejemplo propuesto

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

8.5.4.5 Consolidación Mapa de Riesgos Integral:

A partir de la aplicación de cada uno de los pasos metodológicos explicados se procede a la elaboración y consolidación del mapa integral de riesgos, en una matriz descriptiva, acompañada de un esquema gráfico que resume los análisis adelantados y permite contar con una visión integral de las diferentes tipologías de riesgos aplicables a cada proceso.

8.6 GESTIÓN PREVENTIVA DE RIESGOS FISCALES

Identificar y gestionar los riesgos que puedan provocar un **daño patrimonial al Estado**, el cual en los términos de la Ley 610 de 2000 está representado en el menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro de los bienes, de los recursos públicos o de los intereses patrimoniales del Estado.

Tabla 20 Concepto Gestión Fiscal - Componentes

¿Qué es?	¿Quién la realiza?	¿Qué comprende?	¿Para qué?
El conjunto de actividades económicas, jurídicas y tecnológicas	Los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos	La adecuada y correcta • adquisición • planeación • conservación • administración • custodia • explotación • enajenación • consumo • adjudicación • gasto • inversión • disposición (de los bienes públicos) • recaudación • manejo • inversión (de sus rentas)	En orden a cumplir los fines esenciales del Estado, con sujeción a los principios establecidos en artículo 3 de la Ley 610 de 2000

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

8.6.1 **Control fiscal interno y prevención del riesgo fiscal:**

El control fiscal adquiere un enfoque preventivo que se potencia con el control interno.

La denominación de **gestor fiscal** comprende los jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores de proyectos, responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros roles cuyas funciones u obligaciones incidan en la gestión fiscal.

La denominación de **gestor fiscal** comprende los jefes de entidad, ordenadores y ejecutores del gasto, pagadores, estructuradores de proyectos, responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros roles cuyas funciones u obligaciones incidan en la gestión fiscal.

El Control Fiscal Interno (CFI) se entiende como el primer nivel para la vigilancia fiscal de recursos públicos, prevención de riesgos fiscales y la defensa del patrimonio público.

El Control Fiscal Interno hace parte del Sistema de Control Interno y es responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de aseguramiento, en lo que corresponde a cada una de ellas.

La figura 13 muestra este despliegue y sus elementos de articulación que sustentan el desarrollo del presente capítulo.

Figura 13 Articulación modelo constitucional control fiscal y sistema de control interno

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

8.6.2 Definición y elementos del riesgo fiscal:

El riesgo fiscal se define de la siguiente manera: Efecto dañoso sobre recursos, bienes y/o intereses patrimoniales de naturaleza pública, a causa de un ***evento potencial.***

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

Efecto dañoso: es el daño que se generaría sobre los recursos, los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

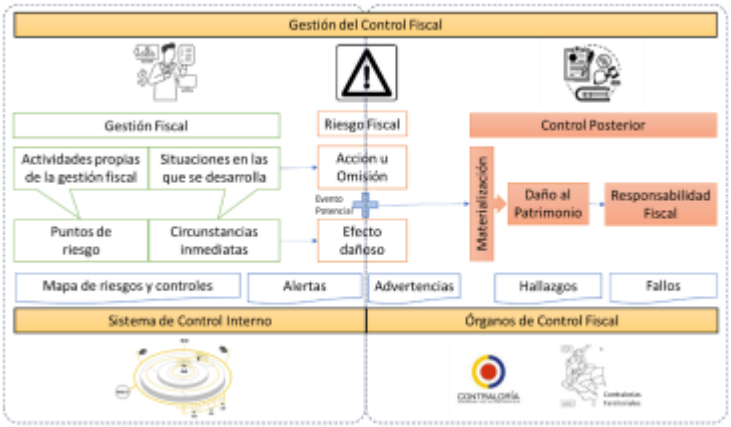
Evento Potencial: hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una acción u omisión que genera daño sobre los recursos, bienes y/o intereses patrimoniales de la entidad. Se resume de la siguiente manera:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso (Potencial Daño)

No se debe confundir el riesgo fiscal con daño patrimonial. El riesgo fiscal se relaciona con el evento de potencial efecto perjudicial sobre los recursos, bienes o intereses públicos, mientras que el daño patrimonial es la afectación real y concreta a los mismos, como resultado de una acción u omisión.

La gestión del riesgo fiscal corresponde a todos los responsables de la implementación y sostenibilidad del sistema de control interno, mientras que la determinación de hallazgos fiscales y el establecimiento de la responsabilidad sobre el daño patrimonial corresponderá al órgano de control fiscal. Su articulación y especificidad se observa en la Figura 14

Figura No. 14 Gestión del Control Fiscal



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional. 2025

8.6.3 Metodología para el levantamiento del mapa de riesgos fiscales:

Presentamos el paso a paso para realizar de forma adecuada la identificación, clasificación, valoración y control del riesgo fiscal, fundamental para la protección de los recursos, bienes e intereses patrimoniales públicos a cargo de los gestores fiscales (jefes de entidad, ordenadores y ejecutores del gasto, pagadores y responsables de la planeación contractual, supervisores, responsables de labores de cobro, entre otros), lo cual contribuye al cumplimiento de sus funciones y al aseguramiento razonable para la toma de decisiones.

8.6.3.1 Paso 1: identificación de riesgos fiscales

Para identificar el riesgo fiscal se debe tener en cuenta los siguientes pasos. Figura 15.

Figura 15 Pasos para la identificación del riesgo fiscal

a) Puntos de riesgo y las circunstancias inmediatas

Los **puntos de riesgo fiscal** son eventos en los que potencialmente se genera riesgo fiscal, es decir, son las actividades propias de la gestión fiscal (Ley 610/2000. Diario Oficial No. 44133), para lo cual es pertinente prestar especial atención a aquellas en las cuales se han generado advertencias, alertas, hallazgos fiscales o fallos con responsabilidad fiscal. En cuanto a las **circunstancias inmediatas** son aquellas situaciones en las cuales se presenta el riesgo, pero que no constituyen la causa raíz que origina el riesgo.

Por cada punto de riesgo, con frecuencia existen múltiples circunstancias inmediatas. La identificación de los puntos de riesgo y las circunstancias inmediatas han de ser el resultado del trabajo conjunto entre el personal directivo, asesor y demás servidores que por su experiencia o formación puedan aportar al análisis crítico y objetivo de la gestión fiscal. Para este ejercicio, se sugieren las siguientes preguntas orientadoras, descritas en la Tabla 21.

Tabla 21. Preguntas orientadoras para identificar puntos de riesgo fiscal y circunstancias inmediatas

Preguntas y criterios para la	Sirve para identificar
¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal)	Puntos de riesgo Fiscal
¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo 1), son aplicables a la entidad?	Puntos de riesgo fiscal y circunstancias inmediatas
Clasifique por procesos (según mapa de procesos), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno -SACI- Nota 1: Se recomienda consultar hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años. Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces. Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la	Puntos de riesgo fiscal y circunstancias inmediatas

entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado. Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno SACI, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno	
En un ejercicio autocrítico, realista y objetivo, ¿cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o fallos con responsabilidad fiscal relacionados con hechos de la entidad o sector y/o advertencias de la oficina de control interno, en los últimos 3 años? Nota: Se recomienda no copiar causas escritas por el órgano de control en hallazgo, salvo que luego del análisis propio la entidad concluya que la causa es la identificada por el órgano de control.	Circunstancias inmediatas

b) Identificación de áreas de impacto

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.

Para definir de manera correcta el área de impacto, al momento de identificar y redactar riesgos fiscales, es fundamental tener claro el concepto de patrimonio público a partir de las tres expresiones que se derivan del artículo 6 de la Ley 610 de 2000:

- ✓ **Bienes públicos:** Aquellos muebles e inmuebles de propiedad pública (bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Se clasifican en bienes de uso público (Su uso pertenece a todos los habitantes del territorio nacional) y bienes fiscales (aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos).
- ✓ **Recursos públicos:** Dineros comprometidos y ejecutados en ejercicio de la función pública.
- ✓ **Intereses patrimoniales de naturaleza pública:** Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica.

c) Identificar el efecto económico

El **efecto económico** del riesgo fiscal: Potencial menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro del patrimonio público. No todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza pública) representan efecto económico.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- Los efectos económicos del daño antijurídico, es decir los montos que se reconocen como pago de condenas y conciliaciones.
- Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de gestores fiscales, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (alguien que no tenga la calidad de gestor público)
- Multas impuestas por hechos que no comportan gestión fiscal
- Existencia de actuación de cobro coactivo por parte de la entidad.
- Pérdida de Bienes cuando a pesar de existir un deterioro o pérdida, se encuentra regulada como aceptable, normal u ordinaria, como suceden por desgaste natural.
- Perdida de bienes cuando se presenta el daño, por el riesgo normal a que se encuentran sometidos determinados equipos eléctricos o electrónicos por efecto de su “normal uso” (máquinas eléctricas, computadores, celulares, etc.).

d) identificación de la causa raíz o potencial hecho generador

- La **causa raíz** sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro.
- La causa raíz o potencial hecho generador y efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o potencial
- hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio estatal (efecto dañoso).
- Una adecuada gestión de riesgos fiscales exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles diseñados e implementados deben apuntarle a atacar las causas, así lograr prevenir la ocurrencia de daños fiscales.
- Al ser la causa raíz un elemento tan relevante para la eficaz gestión de riesgos fiscales, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador. Es fundamental entonces, deslindar el hecho que ocasiona el daño (evento potencial o causa raíz), del daño propiamente dicho (efecto dañoso).

e) Descripción del Riesgo Fiscal

- Se presenta la estructura de redacción de riesgos fiscales en la que se conjugan los elementos antes descritos; así mismo, se presenta un ejemplo de riesgos fiscales.
- Para redactar un riesgo fiscal, se debe tener en cuenta:
  - ✓ Iniciar con la expresión: ***Posibilidad de****,* nos referimos al evento potencial.
  - ✓ **Impacto:** Se refiere al efecto dañoso (potencial daño fiscal) sobre el área de impacto (recursos públicos, bienes o intereses patrimoniales de naturaleza pública).
  - ✓ **Circunstancia inmediata**: corresponde al cómo. Se refiere a aquella situación en la que se presenta el riesgo; pero no constituye la causa principal que lo genera.
  - ✓ **Causa Raíz:** corresponde al por qué; es el evento (acción u omisión) que de presentarse es el generador directo del potencial daño. Es la condición necesaria del riesgo, de tal forma que, si ese hecho no se produce, el daño no se genera

.

La estructura propuesta para la redacción de riesgos fiscales se desarrolla en la figura 16:

Figura 16 Descripción riesgo fiscal

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

Ejemplo: Una entidad X se atrasó en el pago del canon de arriendo de una sede, por 6 meses, generándose intereses moratorios por $30 millones. Cuando llega un nuevo director este encuentra la deuda por concepto de canon y los intereses generados y procede a gestionar los recursos para el pago de capital e intereses y al mes de su posesión efectúa el pago. A continuación, en la tabla 22 se desarrollan los pasos antes explicados:

Tabla 22 Aplicación pasos descripción riesgo fiscal Ejemplo

Paso	Identificación
Punto de Riesgo: (actividad de la gestión fiscal)	Administración de inmuebles en arrendamiento al servicio de la entidad
Circunstancia inmediata: (situación en la que se presenta el riesgo)	Pago de intereses moratorios en contrato de arrendamiento
Área de Impacto: (patrimonio público afectado)	Recursos públicos de la entidad
Efecto económico: (potencial daño al patrimonio)	Disminución de recursos disponibles equivalente al monto pagado por concepto de intereses moratorios
Causa raíz: (potencial acción u omisión)	Omisión de pago oportuno del canon de arrendamiento

Descripción del riesgo:

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efecto dañoso sobre los **recursos de la entidad**	por la generación de intereses moratorios en contrato de arrendamiento	a causa de la omisión en el pago oportuno del canon pactado.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

Conclusión: El hecho generador del daño no es el pago de la deuda ya que esta es una acción que da cumplimiento a una obligación adquirida. La causa raíz es la omisión de pago oportuno y el riesgo fiscal al potencial daño representado en intereses moratorios pagados., Activar controles correctivos para evitar que se materialice el daño patrimonial (Hallazgo fiscal), tales como el reembolso del monto correspondiente de intereses moratorios y controles preventivos para que no se vuelva a presentar la omisión (causa raíz).

A continuación, en la tabla 23 se muestran otros ejemplos de redacción de riesgos fiscales, según el objeto sobre el cual recae la posibilidad de efecto dañoso.

Tabla 23 Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por daño en equipos tecnológicos, a causa de la omisión en la implementación y operación de redes eléctricas seguras.	Posibilidad de efecto dañoso sobre los recursos públicos, por pago de multa impuesta por la autoridad ambiental, a causa de la ejecución de proyectos de infraestructura sin la aprobación de licencias ambientales requeridas.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por negación del reconocimiento de siniestros en el contrato de seguro, a causa de la omisión en la actualización del inventario de bienes amparados.

Bienes Públicos	Recursos públicos	Intereses patrimoniales de naturaleza pública
Posibilidad de efecto dañoso sobre bienes públicos, por pérdida, extravío o hurto de bienes muebles de la entidad a causa de la inexistencia de procedimientos documentados para el ingreso y salida de bienes del almacén	Posibilidad de efecto dañoso sobre recursos públicos, por sobrecostos en contratos de la entidad, a causa de la omisión del deber de elaborar estudios de mercado.	Posibilidad de efecto dañoso sobre intereses patrimoniales de naturaleza pública, por por menores ingresos percibidos sobre la explotación de marcas de propiedad comercial de la entidad a causa de errores u omisiones en el análisis técnico, jurídico y económico del mercado

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

8.6.3.2 Paso 2: Valoración del riesgo fiscal

En esta etapa se realiza la **Evaluación de riesgos** que busca establecer el nivel de riesgo inherente, entendido como la probabilidad de ocurrencia del riesgo, así como su impacto en la gestión fiscal.

- **Probabilidad:** La probabilidad es la posibilidad de ocurrencia del riesgo fiscal, se determina según al número de veces que se pasa por el punto de riesgo fiscal en el periodo de 1 año, es decir, el número de veces que se realizan las actividades que representen gestión fiscal.
- **Impacto:** la naturaleza y alcance del riesgo fiscal, siempre tendrá un impacto económico, toda vez que el efecto dañoso recae sobre un bien, recurso o interés patrimonial de naturaleza pública. Toda potencial consecuencia económica sobre el patrimonio público, es relevante, sin embargo, existen niveles para su valoración.
- **Determinación del nivel de riesgo inherente:** A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, se busca determinar la zona de riesgo inicial (riesgo inherente), se trata de determinar los niveles de severidad

Para la evaluación del riesgo fiscal, se aplicarán las tablas de frecuencia e impacto, así como la matriz de severidad 11, 12, Y 13 de este Manual.

8.6.3.3 Paso 3. Valoración de controles

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos.

Los controles pueden ser preventivos, detectivos o correctivos dependiendo el momento (antes, durante o después) en que se accionen respecto a la actividad que origina el riesgo fiscal (punto de riesgo). Los controles preventivos buscan asegurar que no se presente la causa raíz, los controles detectivos buscar tomar medidas ante la ocurrencia de la causa raíz para evitar que se produzca el efecto dañoso y los controles correctivos actúan ante el daño potencial, procurando detener su materialización o reparando el daño causado.

Para el análisis y evaluación de controles se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con eficiencia y formalización. Se aplican los lineamientos para la redacción del control establecidos en el numeral 8.7, numeral (e) y la tabla No. 23

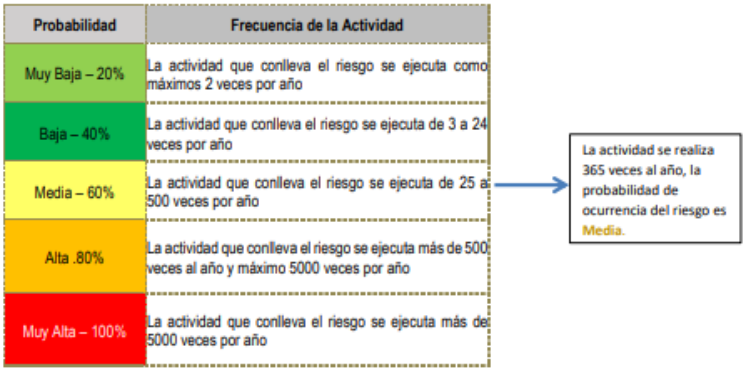
Ejemplo :

- **Proceso:** Gestión de recursos
- **Objetivo:** Gestionar los bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para el cumplimiento de la misión institucional.
- **Alcance:** Inicia con la consolidación y depuración del plan de necesidades de bienes, obras y servicios que requieran los procesos institucionales en cada vigencia fiscal y culmina con el suministro de bienes y prestación de servicios, acorde con la disponibilidad de recursos.
- **Punto de Riesgo:** Ingreso, custodia y salida de bienes muebles de la entidad
- **Riesgo Fiscal:** Posibilidad de efectos dañoso sobre bienes públicos (área de impacto), por pérdida, extravío o hurto de bienes muebles de la entidad (circunstancia inmediata), a causa de omisión en la aplicación del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de información a quien gestiona las pólizas cuando haya lugar (causa raíz).
- **Probabilidad:** Las veces que se pasa por el punto de riesgo en un año (365), puesto que todos los días del año se ejerce la custodia de los bienes muebles de la entidad. Para este ejemplo es importante tener en cuenta, la cantidad y valor de los bienes muebles en el inventario es diversa, se sugiere analizar el tipo de bien y el número de estos, a fin de acotar el nivel de probabilidad con un análisis más detallado que permita establecer controles diferenciados acorde con la naturaleza de diferentes grupos de bienes, Ejem: equipos de cómputo, muebles y enseres, entre otros.

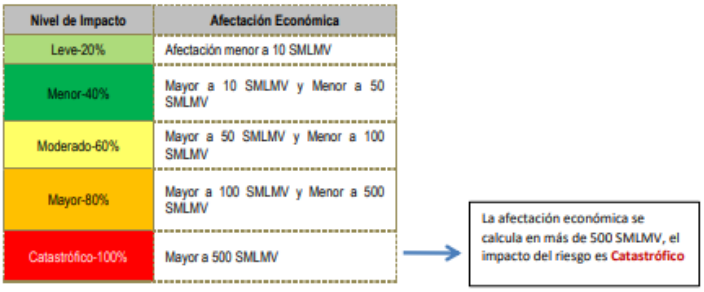
Aplicando las tablas de probabilidad e impacto tenemos:

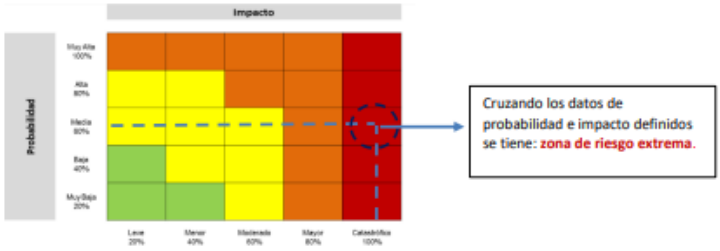
Para determinar el impacto es necesario cuantificar el potencial efecto dañoso sobre el bien, recurso o interés patrimonial de naturaleza pública.

En este ejemplo el efecto dañoso sería del valor contable del inventario de bienes muebles que se determina en 2.500 SMLMV. De acuerdo con la tabla para la definición del nivel de impacto, este riesgo tiene un nivel de impacto catastrófico.



Probabilidad inherente= moderada 60%, **Impacto inherente:** catastrófico 100% Zona de severidad o nivel de riesgo: para la definición de zona severidad, al conjugar la calificación de probabilidad con la de impacto nos resulta un nivel de riesgo extremo.





Controles Identificados:

- Control 1 Preventivo: El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.
- Control 2 Detectivo: El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.

- Control 3 Correctivo: El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador

Aplicando la tabla de valoración de controles tenemos:

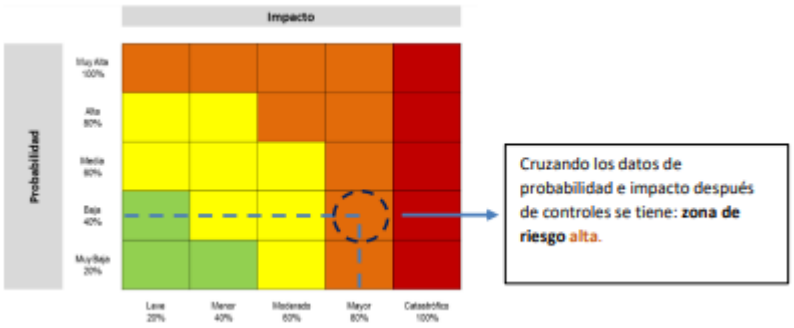
Control 1	Criterios de efectividad			Peso
El jefe de almacén valida y registra diariamente las entradas y salidas en el aplicativo dispuesto para tal fin, el cual alimenta automáticamente el inventario de bienes muebles de la entidad y su responsable.	Tipo	Preventivo	X	25%
		Detectivo		
		Correctivo		
	Implementación	Automático		
		Manual	X	15%
	Total, Valoración Control 1 =40%			
Control 2	**Criterios de efectividad**			**Peso**
El coordinador administrativo verifica mensualmente la relación de ingreso y salida de bienes muebles contra los inventarios generados por el sistema (actualización y	Tipo	Preventivo		
		Detectivo	x	15%
		Correctivo		
ubicación en el inventario), en caso de encontrar inconsistencias solicita al Jefe de Almacén ubicar el bien faltante y realizar el ajuste, teniendo en cuenta los soportes de salida e ingreso del almacén.	Implementación	Automático		
		Manual	x	15%
	Total, Valoración Control 2 = 30%			
Control 3	**Criterios de efectividad**			**Peso**
El director administrativo verifica la vigencia y actualización de la póliza de acuerdo a los bienes que ingresan a la entidad, en caso de presentarse un siniestro adelanta las reclamaciones respectivas ante el asegurador.	Tipo	Preventivo		
		Detectivo		
		Correctivo	x	10%
	Implementación	Automático		
		Manual	x	15%
	Total, Valoración Control 3 = 25%			

Es a partir de los controles que se da el movimiento, en la matriz de calor que corresponde, a continuación se muestra el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo al tipos de control y su respectiva valoración, para determinar el riesgo residual.

Nivel de riesgo (riesgo residual): Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de controles, se debe tener en cuenta que, estos mitigan el riesgo de forma acumulativa, es decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control. Siguiendo con el ejemplo propuesto, se observan los cálculos requeridos para la aplicación de los tres controles definidos así:

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de efectos dañoso sobre bienes públicos *(área de impacto)*, **por** pérdida, extravío o hurto de bienes muebles de la entidad *(circunstancia inmediata)*, **a causa de** la omisión de cumplimiento del procedimiento para el ingreso, custodia y salida de bienes e inventario del almacén y el reporte de	Probabilidad Inherente	60%	Valoración control 1 preventivo	40%	60%* 40% =24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2o control	**36%**	Valoración control 2 Detectivo	30%	36%* 30% =10.8% 36% - 10,8% = **25,2%**
	Probabilidad Residual: 25,2%				
Riesgo	**Datos relacionados con la probabilidad e impacto inherentes**		**Datos valoración de controles**		**Cálculos requeridos**
información a quien gestiona las pólizas cuando haya lugar *(causa raíz)*.	Impacto Inherente	100%	Valoración control correctivo	25%	100%* 25% =25% 100% - 25% = 75%
	Impacto Residual: 75%				

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor, a continuación, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles y cálculo final:



La anterior información puede trasladarse a la matriz mapa de riesgo que hace parte de los anexos desarrollados para el Manual.

8.7 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

El objetivo de este capítulo es orientar al área de Gestión de la Tecnología en la en la implementación de un proceso de Gestión de Riesgos de Seguridad de la información, que permita incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en la ESE.

El Modelo de Seguridad y Privacidad de la Información es un instrumento desarrollado por el Ministerio de las Tecnologías de la Información y de las Comunicaciones que imparte los lineamientos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información basado en las normas y estándares de mejores prácticas en materia de seguridad de la información.

Este capítulo aborda temas como la identificación de activos de información, riesgos, amenazas y vulnerabilidades, para llevar a cabo un análisis de los riesgos de seguridad de la información, luego, la implementación de controles diseñados para mitigar estos riesgos y el proceso de reporte de estos.

A continuación, se desarrollan los pasos necesarios para la identificación y tratamiento de los riesgos asociados a la Disponibilidad, Integridad y Confidencialidad de los activos de información que permiten cumplir con la misión y alcanzar la Visión.

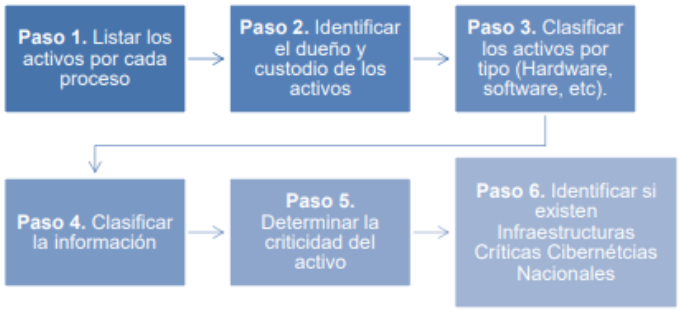
8.8.1 Paso 1: Identificación y descripción de riesgos de seguridad de la información

8.8.1.1 Identificación de los riesgos clave y asociación de estos frente a los objetivos previamente identificados:

En primer lugar, se deben identificar los activos de Información, mediante las actividades descritas en los "*Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional*" del MSPI, en esta se presenta los lineamientos básicos que debe tener en cuenta para realizar una adecuada identificación y clasificación de activos de información de cada entidad.

Para el diligenciamiento del inventario tenga en cuenta los siguientes pasos: Ver Figura 17:

Figura 17 Pasos para la identificación y valoración de activos



Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

Se deben listar cada uno de los activos de información de la entidad que corresponden al alcance del proyecto, luego, para cada activo se deben registrar los siguientes datos:

- **Macroproceso**: Macroproceso de la Entidad al que pertenece el activo de información(En caso de que existan).
- **Proceso**: Proceso de la Entidad al que pertenece el activo de información.
- **Identificador**: Se sugiere que el identificador sea una concatenación del código de la
- dependencia según la Tabla de Retención Documental (TRD) + número consecutivo.
- **Tipo**: Define el tipo de Activo de Información:
  - ✓ **Información y datos de la entidad**: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros
  - ✓ **Sistemas de información y aplicaciones de Software**: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
  - ✓ **Dispositivos de Tecnologías de información- Hardware**: Equipos de cómputo que por su criticidad son considerados activos de información, no sólo activos fijos.
  - ✓ **Soporte para almacenamiento de información**: Equipo para almacenamiento de información como USB, Discos Duros, CDs, SAN, NAS.
  - ✓ **Servicios**: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
  - ✓ Recursos Humanos
  - ✓ Instalaciones
  - ✓ Redes
- **Oficina**: Área, dependencia o proceso que está identificando el activo de información.
- **Serie documental**: Serie documental del área, dependencia o proceso que se
- encuentra identificando el Activo.
- **Subserie documental**: Subserie documental del área, dependencia o proceso que se encuentra identificando el Activo.

- **Nombre**: Nombre completo del activo de información.
- **Descripción**: Descripción resumida de manera clara para identificar el activo de
- información.
- **Nombre del responsable de la producción de la información (Propietario del**
- **activo)**: Nombre del área, dependencia, proceso responsable de producir el activo de
- información
- **Fecha de generación de la información**: Fecha en la que el activo de información fue incluido en el inventario – TRD.
- **Nombre del responsable de la información (Custodio del activo)**: Corresponde al nombre del área, proceso o dependencia encargada en la Entidad de la custodia o control de la información o implementación de controles de protección.
- **Fecha de ingreso del activo al archivo**: Fecha en la que el activo ingresa al archivo de gestión.
- **Soporte de registro**: De acuerdo con el Decreto 2609 de 2012:
  - ✓ **Físico** (análogo)
  - ✓ **Digital** (electrónico) Este campo se diligencia si el Tipo de activo es "Información"
  - ✓ **N/A:** Para el resto de los tipos de activos se debe seleccionar N/A.
- **Medio de conservación**: De acuerdo con el Decreto 2609 de 2012 Archivo Institucional Es la instancia administrativa de custodiar, organizar y proteger.
- **Formato**: Identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como: Hoja de cálculo, imagen, audio, video, documento de texto, etc.
- **Idioma**: Establece el idioma, lengua o dialecto en que se encuentra la información.

A continuación, se realiza la Clasificación de Activos de Información de acuerdo con la propiedad correspondiente: Disponibilidad, Integridad y Confidencialidad.

Para cada activo se define el nivel de criticidad de la propiedad específica, para cada propiedad "*se definieron tres (3) niveles que permiten determinar el valor general o criticidad del activo en la entidad*": Alta, Media y Baja, que corresponden con Criterios de Clasificación para cada una de las propiedades de la Información. Ver Tabla No. 24

Tabla 24 Criterios de Clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

El nivel de clasificación del activo corresponderá con el resultado de la sumatoria de la tabla de criterios de clasificación, que se muestra en la Tabla 25:

Tabla 25 Niveles de Clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

Este resultado corresponde con el nivel de Criticidad del activo.

- Es Infraestructura Critica cibernética Nacional: Se define si el activo corresponde con los criterios de Infraestructura Critica cibernética descritos en los “lineamiento para la identificación de las infraestructuras críticas cibernéticas” del MSPI.

- Información publicada: Se define si el activo está publicado en la intranet, en internet no está publicado.
  - ✓ Publicada: Si la información es publica y se puede consultar en un sitio web (interno
  - ✓ externo) o un sistema de información del Estado.
  - ✓ Publicada (Interno - Intranet)
  - ✓ Publicada (Externo - Internet)
  - ✓ No Publicada: Si la información se encuentra en la Entidad, pero no se encuentra en un sistema de información o sitio web.

- Lugar de consulta o ubicación: Indica la URL, sitio web o sistema de información donde puede ser consultada la información, si no está publicada la ubicación física.

Tabla 26 Clasificación de Activos

CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN (ISO 27001)						
Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	Es Infraestructura Critica cibernética	Información publicada	Lugar de consulta o ubicación

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

El siguiente bloque corresponde con el Índice de información clasificada y reservada:

- Objeto legítimo de la excepción: Identificación de la excepción, previsto en los Art. 18 y 19 - Ley 1712/2014, cobija la calificación de información reservada o clasificada. Si la respuesta es NO, marcar no aplica (N/A) en los demás campos sobre el índice de información clasificada y reservada.
- Fundamento constitucional o legal: Justifica la clasificación o la reserva, señalando expresamente la norma, articulo, inciso párrafo que la ampara.

- Fundamento jurídico de la excepción: Indica la norma jurídica que sirve como fundamento jurídico para la clasificación o reserva de la información.
- Excepción total o parcial: Según sea integral o parcial la calificación, las partes o secciones clasificadas o reservadas. Indicar si la totalidad del documento es clasificado reservado o si solo una parte corresponde a esta calificación
- Fecha de clasificación: Fecha de calificación como reservada o clasificada.
- Tiempo de clasificación: Tiempo que cobija la clasificación o reserva. Es limitada en años, la reserva solo puede durar como máximo por 15 años desde la creación del documento.

Tabla 27 Índice de Información Clasificada y Reservada

ÍNDICE DE INFORMACIÓN CLASIFICADA Y RESERVADA (DECRETO 103 DE 2015)					
Objeto legítimo de la excepción	Fundamento constitucional o legal	Fundamento jurídico de la excepción	Excepción total o parcial	Fecha de clasificación (DD/MM/AAAA)	Tiempo de clasificación

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

El siguiente bloque corresponde con los activos de información que contienen datos personales:

- **¿Contiene datos personales?:** ¿El activo de información contiene datos personales?: SI - NO
- **¿Contiene datos personales de niños, niñas o adolescentes?:** Su tratamiento está prohibido, salvo que se trate de datos de naturaleza pública. Ej. Registro civil.

- **Tipos de datos personales**: Si cuenta con datos personales seleccione el tipo, en caso contrario seleccione N/A:
  - ✓ **Dato personal público**: Toda información personal que es de conocimiento libre y abierto para el público en general. Ejemplo: Número de identificación apellidos.
  - ✓ **Dato personal privado**: Toda información personal que tiene un conocimiento restringido, y en principio privado para el público. Ejemplo: Dirección de residencia y Nº teléfono.
  - ✓ **Dato semiprivado**: Dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar al titular ó a cierto sector y grupo de personas. Ejemplo: Fecha y lugar de nacimiento

- **Finalidad de la recolección de los datos personales**: La finalidad de la recolección justifica por la cual el dato es capturado, almacenado y mantenido en la Entidad
- **Existe la autorización para el tratamiento de los datos personales**: Seleccionar si se cuenta o no con la autorización de la recolección y tratamiento.

Tabla 28 Datos Personales

DATOS PERSONALES (LEY 1581 DE 2012)				
¿Contiene datos personales?	¿Contiene datos personales de niños, niñas o adolescentes?	Tipos de datos personales	Finalidad de la recolección de los datos personales	Existe la autorización para el tratamiento de los datos personales

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2025

Una vez identificados, clasificados y valorados, los activos de información compilados en la Matriz de Activos, por los líderes de procesos, se envia la matriz para su consolidación y validación a la Asesora Jurídica, finalmente se presenta al Comité Institucional de Gestión y Desempeño."

Finalmente se realiza el etiquetado de la información para que los usuarios puedan establecer el nivel de confidencialidad de cada documento.

La Matriz del Inventario de Activos de Información, es el insumo principal para la Gestión de Riesgos de Seguridad de la Información (descrito en la Guía "*Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas*").

Se debe establecer según el nivel de criticidad a cuáles activos se les realizará el correspondiente análisis de riesgos. A continuación, se desarrolla un ejemplo práctico:

- Listado y registro de activos, asociando macroproceso, proceso, identificador, tipo, serie y subserie documental:

Macroproceso	Proceso	Identificador	Tipo	Oficina	Serie documental	Subserie documental
Gestión Financiera	Gestión de nomina	GF001	Software	Financiera	001	00001
Gestión Financiera	Gestión de nomina	GF001	Software	Financiera	001	00001

- Datos sobre el activo de información, sus responsables, soportes de almacenamiento de información, servicios, soporte registro, medio conservación, idioma.

Nombre	Descripción	Nombre del responsable de la producción de la información (Propietario del activo)	Fecha de generación de la información	Nombre del responsable de la información (Custodio del activo)
Software de gestión de nómina (Pagosnet)	Software de gestión de nomina	Director TI	12/03/2025	Analista nomina
Informe pagos de nómina periodo: ene-2025 a marzo-2025	Informe de los pagos de nómina realizados den el periodo: ene-2025 a marzo-2025	Director Financiero	12/03/2025	Analista nomina
Fecha de ingreso del activo al archivo	**Soporte de registro**	**Medio de conservación**	**Formato**	**Idioma**
22/11/2000	Digital	Sistemas de Información corporativos	Software de gestión de nomina	Español
22/11/2000	Digital	Sistemas de Información corporativos	Software de gestión de nomina	Español

- Clasificación de activos, de acuerdo al análisis sobre el nivel de criticidad para cada uno:

Confidencialidad	Integridad	Disponibilidad	Criticidad del activo	¿Es Infraestructura Crítica Cibernética?	Información publicada	Lugar de consulta o ubicación
Clasificada / Uso Interno = Medio	Alto	Alto	ALTA	No	Publicada (Interno - Intranet)	Intranet
Clasificada / Uso Interno = Medio	Alto	Alto	ALTA	No	Publicada (Interno - Intranet)	Sharepoint

Objeto legítimo de la excepción	Fundamento constitucional o legal	Fundamento jurídico de la excepción	Excepción total o parcial	Fecha de clasificación (DD/MM/AAAA)	Tiempo de clasificación
N/A	N/A	N/A	N/A	N/A	N/A
Si	artículo 18 de la ley 1712 de 2014	artículo 18 de la ley 1712 de 2014	Reserva parcial	15/03/2025	15 años

¿Contiene datos personales?	¿Contiene datos personales de niños, niñas o adolescentes?	Tipos de datos personales	Finalidad de la recolección de los datos personales	Existe la autorización para el tratamiento de los datos personales
N/A	N/A	N/A	N/A	N/A
Si	No	Dato semiprivado	Realizar el pago de nomina	Si

a) Matriz de Riesgos de Seguridad de la Información: Con base en la criticidad se realiza el proceso de gestión de riesgos, la cual registra en la Matriz de Riesgos de Seguridad de la Información, con respecto al activo de información se registran los siguientes datos:

Tabla 29 Matriz de Riesgos de Seguridad de la Información

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN			
Proceso	Referencia	Activo de Información	Tipo de Activo

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025.

- **Activo de Información**: Es el nombre del activo de información.
- **Tipo de Activo**: Corresponde a una de las siguientes categorías: Información, Software, Hardware, Servicios, Intangibles, Infraestructura crítica cibernética nacional, Recursos humanos e Instalaciones y Otros Servicios

b) Identificación de áreas de impacto

El área de impacto es la consecuencia negativa en los objetivos de la organización en caso de materializarse un riesgo o las que por causa de incidentes de seguridad de la información tenga consecuencias en la gestión de la entidad.

c) Identificación de áreas de factores de riesgo

Las fuentes generadoras de riesgos, la siguiente tabla define los elementos necesarios:

Tabla 30. Amenazas y Vulnerabilidades

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	
Amenazas (Causa Inmediata)	Vulnerabilidades (Causa raíz)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

- **Amenaza**: Causa potencial de un incidente no deseado, puede provocar daños a un sistema u organización. (ISO/IEC 27001:2022). Pueden ser Deliberadas (D), fortuitas (F) o ambientales (A)

Tabla 31 *Tabla de amenazas comunes*

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

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

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

Tabla 28 Tabla de Vulnerabilidades Comunes

Tipo	Vulnerabilidades
Hardware	Mantenimiento insuficiente
	Ausencia de esquemas de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoría
	Asignación errada de los derechos de acceso
	Interfaz de usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Software nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red eléctrica inestable
	Ausencia de protección en puertas o ventanas
Organización	Ausencia de procedimiento de registro/retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Ausencia de acuerdos de nivel de servicio (ANS o SLA)

Tipo	Vulnerabilidades
	Ausencia de mecanismos de monitoreo para brechas en la seguridad
	Ausencia de procedimientos y/o de políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

d) Descripción del riesgo

En este paso se identifican:

Tabla 32 Riesgos de Seguridad de la Información

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		
Tipo de riesgo	Descripción del Riesgo	Clasificación riesgo

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2025

- **Tipo de Riesgo**: Este campo solo admite uno de estos 3 valores:

✓ Pérdida de Disponibilidad
✓ Pérdida de Integridad
✓ Pérdida de Confidencialidad

- **Descripción del Riesgo**: Describe la situación específica que da como resultado el correspondiente riesgo. “Para cada tipo de activo o grupo de activos pueden existir una serie de riesgos, se deben identificar, valorar y tratar si el nivel de riesgo amerita.”

- **Clasificación del Riesgo**: Este campo corresponde al nombre que identifica a la situación que podría presentarse, es decir, el posible incidente de seguridad.

8.8.2 Paso 2: Análisis de Riesgo Inherente

A partir de este paso metodológico se incorporan la tablas y matrices establecidas en el numeral 8.6.3 que desarrolla los lineamientos para los riesgos generales de la gestión.

8.8.2.1 Determinar la probabilidad

Se debe realizar el análisis de probabilidad de la materialización de estos riesgos.

Tabla 33 Frecuencia

MATRIZ DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN		
Frecuencia	% Probabilidad Inherente	Probabilidad Inherente

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

- **Frecuencia**: Este campo corresponde al número de horas al año en el cual se realiza la actividad que conlleva al riesgo.

- **% Probabilidad Inherente**: Este campo corresponde al porcentaje anual en el cual se realiza la actividad que conlleva al riesgo medido en una escala cuantitativa.

- **Probabilidad inherente**: Corresponde al número de veces al año en el cual se realiza la actividad que conlleva al riesgo medido en una escala cualitativa. (Punto 8.6.3)

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

8.8.2.2 Determinar el impacto: En esta actividad se debe realizar el análisis del impacto de la materialización de estos riesgos.

Tabla 34 Impacto

IMPACTO	
% Impacto Inherente	Impacto Inherente

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

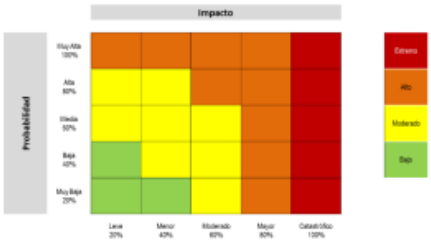
- **% Impacto Inherente**: Este campo corresponde a la medida porcentual del impacto económico o reputacional sobre la entidad de manera cuantitativa.

- **Impacto Inherente**: Este campo corresponde a la medida del impacto económico o reputacional sobre la entidad de manera cualitativa.

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

8.8.2.3 Análisis de severidad

Zona de riesgo inherente: En este campo se determina la zona de severidad de la matriz de calor en la cual se encuentra el riesgo, según su probabilidad e impacto.



8.8.3 Paso 3: Diseño y Análisis de Controles

8.8.3.1 Estructura para la Descripción del Control

Esta actividad se seleccionan los controles que se establecerán para mitigar los riesgos.

Tabla 35 Controles

No. Control	Control Anexo A	Descripción del Control

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

- **No. Control**: Este campo es un consecutivo de los controles a establecer.

- **Control Anexo A**: Este campo corresponde al control seleccionado del Anexo A de la norma 27001:2022.

- **Descripción del Control**: Este campo corresponde a una descripción de la forma en la cual el control seleccionado será implementado en la entidad.

8.8.3.2 Valoración de Controles

- **Afectación**

En esta actividad se establece la afectación que tendrá la implementación del control sobre la Probabilidad o el Impacto del riesgo.

Tabla 36 Afectación

AFECTACIÓN	
Probabilidad	Impacto

- **Probabilidad**: Especifica si el control pretende modificar la probabilidad de ocurrencia de riesgo.

- **Impacto**: Especifica si el control pretende modificar el impacto de ocurrencia de riesgo.

- **Atributos** Establece los Atributos de la implementación del control, donde se consideran atributos de eficiencia y formalización del control. Ver Tabla 37, 38 y 39

Tabla 37

Características de Eficiencia		Peso
Tipo	Preventivo	25%
	Detectivo	15%
	Correctivo	10%
*Implementación *Nota: En implementación no se tienen controles semiautomáticos.	Automático	25%
	Manual	15%

Tabla 38

Características de Eficiencia		Descripción
Documentación	Procedimientos	Basados en la estructura del Modelo de Operación por procesos, despliegue desde cada proceso, sus procedimientos y esquemas asociados, que se encuentren documentados.
	Sistemas de información	Sistemas de información de apoyo a la ejecución del control (si existen).
	Otros Esquemas	Políticas de operación, manuales o guías específicas.
Frecuencia	Siempre que se ejecuta la actividad	La oportunidad en que se ejecuta el control debe ayudar a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna.
	Periódicamente (diario, mensual, bimestral, trimestral, semestral).	
Evidencia (Trazabilidad de la ejecución)	Con registro manual	Se deja evidencia o rastro de la ejecución del control.
	Con registro electrónico	

Características de Eficiencia		Descripción
Ejecución (Fuentes de información internas o externas)	Interna	Formatos o registros internos formales.
	Externa	Registros externos confiables (extractos bancarios, confirmaciones de autenticidad de documentos, SECOP, SIIF, SIGEP, bases de datos).
	Mixta	Combinación de datos de fuentes internas y externas formales.

Tabla 39 Atributos

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

8.8.4 Paso 4: Valoración de Riesgo Residual

En esta etapa se revisa la efectividad de los controles, teniendo en cuenta la Tabla de aplicación de controles para establecer el riesgo residual del Punto 8.6.3.

Tabla 40 Valoración del Riesgo Residual

VALORACIÓN DEL RIESGO RESIDUAL				
Probabilidad Residual	% de Probabilidad Residual	Impacto Residual	% Impacto Residual	Zona de Riesgo Final

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

8.8.4.1 Plan de implementación de controles

En esta actividad se establece un plan para implementar los controles y poder realizar el correspondiente seguimiento:

Tabla 41 Plan de Implementación de Controles

PLAN DE IMPLEMENTACIÓN DE CONTROLES					
Tratamiento	Plan de Acción	Responsable	Fecha de Implementación	Seguimiento	Estado

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

- **Tratamiento**: En este campo se especifica el tipo de tratamiento que se realizará entre 4 opciones disponibles:
  - ✓ Reducir: Implementar controles para reducir la probabilidad o el impacto
  - ✓ Compartir: Compartir las consecuencias de la materialización del riesgo, por ejemplo, a través de la adquisición de una ciberpoliza
  - ✓ Aceptar: Cuando el nivel del riesgo está por debajo del apetito establecido por la alta dirección.
  - ✓ Evitar: Cuando se decide eliminar el activo que es fuente del riesgo: por ejemplo, dar de baja un servidor.
- **Plan de Acción**: En este campo se especifica la identificación del Plan de acción con el cual se realizará la implementación de dicho control.
- **Responsable**: En este campo se especifica el cargo de quien implementa el control.
- **Fecha de Implementación**: En este campo se especifica la Fecha máxima de implementación del control.

- **Seguimiento**: En este campo se especifica la periodicidad del seguimiento a la implementación del control.
- **Estado**: En este campo se especifica el estado de la implementación del control.

8.9 SISTEMA DE GESTIÓN DE RIESGOS PARA LA INTEGRIDAD PÚBLICA -SIGRIP

8.9.1 Amenazas para la integridad pública

8.9.1.2 Soborno

El Soborno puede ser entendido como “ofrecer, prometer, dar, aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar […]”.
.
Y opera en dos niveles: Soborno Entrante y Saliente.

- Se entiende como Entrante el soborno al servidor de la Entidad.
- Saliente el soborno por parte de servidores a otros en nombre de la Entidad.

Tipificación general del Soborno:

- El Código Penal Colombiano tipifica el cohecho propio, el cohecho impropio, el cohecho por dar u ofrecer

8.9.2.3 Fraude

Corresponde a errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros. Este puede ser:

- Interno, en cuyo caso el fraude involucra a colaboradores
- Externo, cuando se realizó por terceros, externos y la organización es la víctima.

El Fraude Externo es un riesgo netamente operativo, al que se expone la Entidad por conductas desplegadas por terceros por lo que este tipo de fraude es, ante todo un riesgo general de gestión.

8.9.2.4 Inadecuada gestión del conflicto de intereses:

Un conflicto de intereses surge cuando, cuando el servidor público debe decidir sobre un asunto en el que tiene interés particular y directo en su regulación, gestión, control o decisión, o lo tiene su cónyuge, compañero o compañera permanente, o sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho. Es decir, cuando el interés general, propio de la función pública, entre en conflicto con un interés particular y directo del servidor público.

8.9.2.5 Corrupción

La Corrupción es “todo acto que implique desviación de la gestión administrativa o de los recursos públicos y privados para obtener un beneficio propio o para un tercero. Igualmente, constituyen actos de corrupción las conductas punibles descritas en la Ley 599 de 2000, o en cualquier ley que la modifique, sustituya o adicione, así como lo previsto en la Ley 1474 de 2011; las faltas disciplinarias; y las conductas generadoras de responsabilidad fiscal relacionadas con los actos de corrupción y cualquier comportamiento contemplado en las convenciones o tratados contra la corrupción que Colombia haya suscrito y ratificado. Esas conductas incluyen:

- El uso del poder para obtener beneficios personales,
- Pérdida o disminución del patrimonio público,
- El perjuicio social significativo, y
- La corrupción electoral”

8.9.2.6 Lavado de Activos (LA), Financiación del Terrorismo (FT) y Financiación de la Proliferación de Armas de Destrucción Masiva (FP) -LA/FT/FP

La integridad pública también se ve afectada por el Lavado de Activos, la Financiación del Terrorismo y la Financiación de la Proliferación de Armas de Destrucción Masiva. A través de estas prácticas y conductas se compromete la capacidad del Estado para cumplir con sus fines, en la medida que las entidades pueden ser usadas para dar apariencia de legalidad a recursos obtenidos de forma ilícita o ilegal, e incluso para trasladar recursos a personas o grupos que pueden terminar atacando instituciones estatales. De esta forma, también se afecta la integridad pública, aun cuando la conducta de los funcionarios y colaboradores puede no ser es objeto de cuestionamiento.

8.9.3 Sistema de Gestión del Riesgo

Teniendo en cuenta las diferentes amenazas para la integridad pública, que pueden generar peligro o daño, es necesario que, desde un enfoque basado en riesgos, se gestionen los SIGRIP, además, permite dar cumplimiento a lineamientos establecidos para la gestión de riesgos en los Programas de Transparencia y Ética Pública, según lo dispuesto por la Secretaría de Transparencia de la Presidencia. Acreditando la gestión de riesgos para la integridad pública, de riesgos LA/FT/FP, canales de denuncia y debida diligencia.

8.9.3.1 Liderazgo del Sistema

Para SIGRIP, existen roles y responsabilidades que deben agregarse a esos niveles de responsabilidad. Se relacionan en función del esquema de líneas y los roles que existen en los Programas de Transparencia y Ética Pública, se resumen en Tabla 42:

Tabla 42 Roles y responsabilidades SIGRIP

Línea Estratégica	3ra Línea	2da Línea	1ra Línea
Supervisor del Programa	Auditor del Programa	Administrador del Programa	Ejecutores del Programa
Alta Dirección Comité Institucional de Gestión y Desempeño Comité Institucional de Coordinación de Control Interno	Oficina de Control Interno, Auditoría Interno o quien haga sus veces	Dependencia o persona designada por la Alta Dirección	Directivos, líderes de proceso, servidores y colaboradores
Son los responsables de analizar y decidir sobre el Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP	Auditoría del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP, con el propósito de asesorar y recomendar mejoras.	En el marco del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP asume la función de cumplimiento que se desarrolla en el numeral 6.3.7.3	Les corresponde la ejecución y el monitoreo de primera línea de los elementos del Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP.

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

8.9.3.2 Liderazgo del Sistema

Con el propósito de lograr una gestión integral, es que surgen los otros tres elementos del SIGRIP: la debida diligencia en el conocimiento de las contrapartes, la función de cumplimiento y las herramientas de gestión del riesgo. La estructura del SIGRIP se observa en la Figura 18 a continuación.

Figura No. 18 Sistema de Gestión de Riesgos para la Integridad Pública

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

8.9.3.4 Identificación y valoración de riesgos para la integridad pública en la Política para la Gestión Integral de Riesgos

a) Paso 1: Identificación y descripción del riesgo

- **Respecto de la "Identificación de los puntos de riesgo"**

En el marco de la gestión del riesgo de LA/FT/FP, debe tenerse en cuenta que los puntos de riesgo se refieren a operaciones que lleva a cabo la entidad. Es decir, actividades dentro del flujo de los procesos que implican un intercambio de recursos, bien sea porque la entidad recibe un bien o servicio por el cual paga un precio, o porque entrega un bien o servicio por el cual le pagan un precio. Estas operaciones son los puntos de riesgos relevantes, que deben tenerse en cuenta para la identificación del riesgo de lavado de activos, financiación del terrorismo o financiación de la proliferación de armas de destrucción masiva.

Respecto del riesgo de Corrupción y sus manifestaciones específicas como soborno, fraude e inadecuada gestión del conflicto de intereses, los puntos de riesgos pueden ser cualquier actividad dentro del flujo de proceso y no solo las operaciones.

- **Respecto de la "Identificación de áreas de impacto"**

En el marco de la gestión de los riesgos para la integridad pública, además del impacto económico y reputacional, también puede haber consecuencias legales y de contagio.

✓ La **consecuencia legal** corresponde al incumplimiento normativo o de obligaciones, que puede derivar en sanciones o indemnizaciones por daños. Así pues, el impacto legal surge desde el momento en que una contraparte es vinculada a procesos judiciales o administrativos sancionatorios o que busquen declarar un incumplimiento.

✓ El **contagio** corresponde a la posibilidad que la entidad pueda sufrir una afectación económica, reputacional o legal a causa de la acción propia de una entidad o de un individuo relacionado. El contagio se expresa cuando las partes relacionadas, pero no vinculadas, se les materializa un riesgo para la integridad pública que tiene el potencial de afectar la ESE.

Las consecuencias legales y de contagio, para efectos de determinar el impacto del riesgo, deben analizarse en términos de **afectación económica**, atendiendo a lo indicado en la Tabla 17, determinada para cálculo del impacto.

Se puede estimar que un riesgo se ha materializado cuando la situación que se había identificado como posible (riesgo) ocurre realmente y genera un impacto negativo sobre los objetivos. En el caso de los riesgos para la integridad pública, el riesgo se materializa siempre que se advierta un impacto sobre la reputación, la operación o de cumplimiento o que comprometa la ejecución del recurso.

✓ La **consecuencia reputacional**, Surge cuando la organización se ve involucrada en denuncias o reportajes que la vinculan con prácticas poco íntegras, incumplimientos normativos o corrupción en general. La consecuencia operativa corresponde a los escenarios en que la conducta contraria a la integridad termina afectando el desarrollo de los procesos. La consecuencia legal inicia desde el mismo momento en que una parte vinculada es involucrada en procesos que puedan derivar en una sanción y el contagio se da cuando la involucrada es la parte relacionada. Finalmente, la consecuencia económica puede configurarse, incluso, desde el momento en que hay retrasos en la ejecución del recurso, por conductas poco íntegras del ejecutor.

- **Respecto de la "Identificación de factores de riesgo"**

Como factores del riesgo LA/FT/FP se tiene a las contrapartes. Estos factores deben permitirle a la entidad mayor efectividad en el conocimiento de las contrapartes, el diseño y aplicación de señales de alerta, la identificación de operaciones inusuales y la determinación y el reporte de operaciones sospechosas.

Surge, entonces, la necesidad de segmentación de los factores de riesgo, a partir de la cual, se profundiza tanto en el conocimiento de las contrapartes, así como de los factores de riesgo con los que tienen relación.

- **Respecto de la "Descripción del riesgo"**

La descripción de los riesgos para la integridad pública tendrá la misma fórmula definida en la Figura 19, Todos iniciarán con la formula *"Posibilidad de"*, y deben señalar el impacto, la causa inmediata y la causa raíz.

Figura 19 Descripción del Riesgo

Fuente: Elaboración Ministerio de Tecnologías de la Información y las Comunicaciones. 2025

Las causas inmediatas de los riesgos para la integridad pública podrán ser el soborno, el fraude, la inadecuada gestión del conflicto de intereses, la corrupción y el riesgo de LA/FT/FP. De acuerdo con lo anterior, se sugiere tener en cuenta los siguientes ejemplos desplegados en la tabla 43 a continuación:

Tabla 43 Ejemplos como referente para análisis del riesgo

Impacto	Causa inmediata		Causa raíz
Afectación económica y/o reputacional	Fraude Interno	Errores, omisiones, informes inexactos o descripciones incorrectas realizados con culpa o dolo para beneficio personal o de terceros.	Descripción de la actividad en el flujo del proceso
	Soborno Entrante	Aceptar o solicitar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una persona actúe o se abstenga de actuar [...]".	
	Soborno Saliente	Ofrecer, prometer o dar una ventaja indebida de cualquier valor (que puede ser financiero o no financiero), directa o indirectamente, e independientemente de la ubicación, en violación de la ley aplicable, como incentivo o recompensa para que una	

Impacto	Causa inmediata		Causa raíz
		persona actúe o se abstenga de actuar [...]".	
	Conflicto de interés	Decidir en un asunto sobre el cual el servidor tiene un interés particular y directo en su regulación, gestión, control o decisión, o lo tuviere su cónyuge, compañero o compañera permanente, o algunos de sus parientes dentro del cuarto grado de consanguinidad, segundo de afinidad o primero civil, o su socio o socios de hecho o de derecho	
	Corrupción	Desviar la gestión administrativa o los recursos públicos y privados para obtener un beneficio propio o para un tercero	

En ese orden de ideas, para cada riesgo y su causa inmediata, atendiendo la estructura para la redacción del riesgo definida en el numeral 8.6.3 se tendría lo siguiente:

- Posibilidad de afectación económica por Corrupción en la evaluación en la evaluación de los procesos de selección para la contratación de bienes y servicios de la Entidad, a causa del direccionamiento y/o favorecimiento de la contratación hacia un proponente específico.
- Posibilidad de afectación económica por Fraude Interno en la asignación de subsidios a causa de errores, omisiones, informes inexactos o descripciones incorrectas realizados para beneficio personal o de terceros en la asignación de subsidios.
- Posibilidad de afectación reputacional por Soborno Saliente en el seguimiento a la agenda legislativa de la Entidad, a causa del ofrecimiento indebido de incentivos o recompensas para que una persona actúe o se abstenga de actuar en favor de la. entidad.
- Posibilidad de afectación reputacional por Soborno Entrante al aceptar o solicitar una ventaja indebida en la designación de citas a favor de un tercero, a causa de la manipulación indebida de sistema de información de asignación de citas.
- Posibilidad de afectación económica por conflicto de interés no declarado y/o declarado, pero no gestionado y/o declarado y no aceptado, a causa de decisiones en asuntos sobre los cuales la servidora o servidor público tiene un interés particular en desarrollo del comité de contratación.

En el caso de riesgos LA/FT/FP, debe hacerse referencia particularmente a actividades del flujo de procesos en que existe la vulnerabilidad o exposición al riesgo. Ver tabla 44.

Tabla 44 Análisis riesgos LA/FT/FP

Impacto	Causa Inmediata	Causa Raíz
Económico, Reputacional, Legal, Operativo o de Contagio	Usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas o para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva	Descripción de la Operación o Transacción

Fuente: Elaborado Secretaría de Transparencia de la Presidencia de la República, 2025.

- Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas en las operaciones de pago de subsidios.
- Posibilidad de contagio por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de contratación directa.
- Posibilidad de afectación económica por usar la entidad para dar apariencia de legalidad a los activos provenientes de actividades delictivas, para canalizar recursos hacia la realización de actividades terroristas o la proliferación de armas de destrucción masiva, a causa de fallas u omisiones en las operaciones de recaudo.

j) **Paso 2: Análisis de Riesgo Inherente**

- **Respecto del "Análisis de Riesgo Inherente"**

Por la naturaleza de los riesgos para la integridad pública, el objetivo fundamental es prevenirlos, detectarlos y reportarlos en términos de oportunidad y eficacia. Esta perspectiva debe ser transversal al análisis del riesgo y al diseño de controles.

El cálculo de probabilidad, impacto y severidad de severidad, se realiza bajo lineamientos definidos en la Tabla 11, 12 y 13, del presente Manual, la cual no es susceptible de ajustes.

c) Paso 3: Diseño y Análisis de Controles

- **Respecto del "Diseño y análisis de controles"**

En todo caso, se sugiere que el procedimiento que se establecen como controles se incorporen deberán referirse a lo definido en el Punto No. 8.6.3.4 Paso 3: Diseño y Análisis de Controles, de este Manual, que establece la estructura general, los atributos y tablas para su valoración.

d) Paso 4: Valoración de Riesgo Residual

- **Respecto de la "Valoración del riesgo residual"**

Sobre este punto referirse completamente al Punto 8.6.3.5 de este Manual.

8.9.3.5 Debida diligencia en el conocimiento de las contrapartes

Ley 2195 de 2022, que dispone: ARTÍCULO 12. PRINCIPIO DE DEBIDA DILIGENCIA. La Entidad debe llevar a cabo medidas de debida diligencia que permitan entre otras finalidades identificar el/los beneficiario(s) final(es), teniendo en cuenta como mínimo los siguientes criterios:

- Identificar la persona natural, persona jurídica, estructura sin personería jurídica o similar con la que se celebre el negocio jurídico o el contrato estatal.
- Identificar el/los beneficiario(s) final(es) y la estructura de titularidad y control de la persona jurídica, estructura sin personería jurídica o similar con la que se celebre el negocio jurídico o el contrato estatal, y tomar medidas razonables para verificar la información reportada.
- Solicitar y obtener información que permita conocer el objetivo que se pretende con el negocio jurídico o el contrato estatal. Cuando la entidad estatal sea la contratante debe obtener la información que permita entender el objeto social del contratista.
- Realizar una debida diligencia de manera continua del negocio jurídico o el contrato estatal, examinando las transacciones llevadas a cabo a lo largo de esa relación para
- asegurar que las transacciones sean consistentes con el conocimiento de la persona natural, persona jurídica, estructura sin personería jurídica o similar con la que se realiza el negocio jurídico o el contrato estatal, su actividad comercial, perfil de riesgo y fuente de los fondos.
- El obligado a cumplir con el principio de debida diligencia del presente artículo, debe mantener actualizada la información suministrada por la otra parte.

El conocimiento de las contrapartes consiste en la obtención de información de la contraparte, de las operaciones y de los productos involucrados en la relación que le permitan a la entidad gestionar adecuadamente los riesgos.

El resultado de estos mecanismos tiene como único propósito generar insumos para la toma de decisiones, la entidad sí podrá atribuir consecuencias a partir del conocimiento que alcance de sus contrapartes, entre ellos:

- La identificación de señales de alerta que deben ser atendidas por la organización.
- La necesidad de implementar controles adicionales, especiales o revisar los existentes para ajustarlos a los resultados de la aplicación del mecanismo de conocimiento de la contraparte.
- La necesidad de hacer ajustes en los equipos a cargo del relacionamiento con la contraparte o que se requieran aprobaciones adicionales, de instancias superiores o plurales, para continuar la relación.
- En circunstancias excepcionales, podrá evaluarse la necesidad de terminar con la relación o abstenerse de iniciarla, en cuyo caso tendrá que aplicarse la normativa especial que aplique.
- Un monitoreo especial a las operaciones que se realicen en el marco del relacionamiento para generar los reportes cuando estas sean inusuales o sospechosas, ante las autoridades correspondientes.

La entidad garantizara que los resultados de la aplicación de los mecanismos para conocimiento de las contrapartes queden documentados dentro de la organización adecuadamente y asegura la confidencialidad de la información clasificada y reservada, el correcto tratamiento de los datos personales y su archivo y custodia, según la normativa aplicable.

- Para ello se establecen lineamientos de debida diligencia:

a) **Preparación:** (1) definir los objetivos de la debida diligencia; (2) determinar los procesos clave en los que se aplicará; (3) identificar dentro de los equipos de trabajo que la llevaran a cabo.
b) **Recolección de información:** (1) determinar las fuentes de información, como estados financieros, contratos, informes legales, listas restrictivas y vinculantes, etc., que se consultaran.
c) **Análisis:** (1) establecer los criterios para determinar los casos en que hay lugar a un problema, inconsistencia o riesgo; (2) establecer el procedimiento de evaluación de la información obtenida antes de la vinculación o relación; (3) establecer los estándares normales de funcionamiento de la organización, según el análisis de contexto realizado, y del sector, industria o mercado en que se dará la vinculación o relacionamiento, para determinar los patrones normales.
d) **Informe de resultados:** (1) indicar el contenido detallado de los informes que se generaran como resultado de la aplicación de los mecanismos de conocimiento con hallazgos clave y riesgos identificados; (2) el informe debe contener una evaluación sobre la viabilidad de la vinculación o relación con base en los hallazgos; (3) el informe debe incluir recomendaciones para mitigar o gestionar los riesgos encontrados.

Toda la documentación relacionada en los anteriores puntos será parte del presente Manual como anexo.

- Establecer un procedimiento y lista de verificación, para la consulta en los siguientes listados:
  - ✓ Sistema de Información del Boletín de Responsables Fiscales – SIBOR, de la Contraloría General de la República.
  - ✓ Sistema de Información de Registro de Sanciones e Inhabilidades – SIRI, de la Procuraduría General de la Nación.
  - ✓ Antecedentes Penales y Requerimientos Judiciales, de la Policía Nacional de Colombia.
  - ✓ Sistema Registro Nacional de Medidas Correctivas – RNMC, de la Policía Nacional de Colombia.
  - ✓ Registro de Deudores Alimentarios Morosos – REDAM, del Ministerio de Tecnologías de la Información y las Comunicaciones.
  - ✓ Lista consolidada del Consejo de Seguridad de las Naciones Unidas, que incluye, pero sin limitarse, las Resoluciones 1267 de 1999, 1988 de 2011, 1373 de 2001, 1718 y 1737 de 2006 y 2178 de 2014 del Consejo de Seguridad de las Naciones Unidas, y todas aquellas que le sucedan, relacionen y complementen, y cualquiera otra lista que se adopte formalmente por el país.
  - ✓ Lista vigente de terroristas de Estados Unidos de América. Lista vigente de la Unión Europea de Organizaciones Terroristas.
  - ✓ Lista vigente de la Unión Europea de Personas Catalogadas como Terroristas.

La consulta deberá hacerse respecto de las contrapartes que sean personas naturales y del representante legal y suplente, revisor fiscal y beneficiarios finales de las contrapartes que sean personas jurídicas u otras estructuras.

- Se Establece un procedimiento para la verificación de la identidad de las contrapartes y evaluación de su historial, lo cual es fundamental para detectar cualquier vinculación con actividades sospechosas. Para lo cual se deberá:

  - ✓ Identificar el nombre o razón social la contraparte.
  - ✓ Determinar la existencia y representación legal. Las personas naturales lo acreditan con su cédula; las personas jurídicas con los certificados expedidos por las cámaras de comercio; otras estructuras con su acto de creación y Registro Único Tributario, si aplica.
  - ✓ En el caso de personas jurídicas u otras estructuras, identificar la estructura de propiedad y existencia de situaciones de control.
  - ✓ En el caso de personas jurídicas u otras estructuras, identificar los beneficiarios finales
  - ✓ Evaluar las relaciones que ha tenido la contraparte con entidades similares en un período de dos (2) años anteriores al relacionamiento, siempre y cuando la contraparte tenga dos o más años de existencia. Para estos efectos, la entidad podrá solicitar referencias de, al menos, dos entidades similares con que la contraparte haya estado relacionada.
  - ✓ Determinar si la contraparte cuenta con un Programa de Transparencia y Ética Pública o Empresarial, o con políticas Antilavado de Activos, Antisoborno o Anticorrupción.
  - ✓ Verificar la documentación aportada para acreditar cualquier hecho en el marco de la relación, como formación, experiencia, capacidad financiera y organizacional, etc.
  - ✓ Verificar, por los medios disponibles, la reputación de la contraparte. Para esto, la entidad podrá revisar noticias e información pública que esté disponible en internet y hacer uso de herramientas de inteligencia artificial.
  - ✓ Requerir declaraciones sobre la fuente de los recursos que utilizará en el marco de la relación que mantenga con la entidad, con sus debidos soportes.
  - ✓ Verificar si la contraparte tiene procesos administrativos sancionatorios, disciplinarios, de responsabilidad fiscal, penales o judiciales, que estén activos o en curso ante las autoridades colombianas.

Toda esta información busca asegurar que la entidad entienda claramente el propósito y el carácter que se pretende dar a la interacción o relación establecida.

Sin embargo, atendiendo al principio de proporcionalidad, y desde un enfoque basado en riesgos, es posible que no se requiera en todos los casos conocer toda la información.

- **Establecer un lineamiento respecto de los casos en que se identifique que una de las contrapartes es una Persona Expuesta Políticamente, según la definición del artículo 2.1.4.2.3 del Decreto 1081 de 2015. Sobre este punto se debe resaltar que**

la calidad de Persona Expuesta Políticamente (PEP) se mantendrá en el tiempo durante el ejercicio del cargo y por dos (2) años más desde la dejación, renuncia, despido o declaración de insubsistencia del nombramiento, o de cualquier otra forma de desvinculación, o terminación del contrato.

La debida diligencia debe incluir una investigación más profunda sobre estas contrapartes, ya que pueden estar expuestos a mayores riesgos para la integridad pública.

- Establecer lineamientos para la toma de decisiones basada en los resultados de la debida diligencia:

  - ✓ El Manual debe identificar los **procesos** en que se deben aplicar los mecanismos de conocimiento de la contraparte. Deben incluirse todos aquellos en que se ha identificado riesgos para la integridad pública.

  - ✓ En cada proceso, se deben identificar, además, las operaciones, vinculaciones o relaciones que tienen exposición a riesgos para la integridad pública.

  - ✓ El Manual debe establecer como una política institucional incluir en todos los procesos donde se identifiquen operaciones, vinculaciones o relaciones expuestas a riesgos, la adopción de un punto de control relacionado con la aplicación de mecanismos de conocimiento de las contrapartes.
  - ✓ La política, además, debe indicar cómo se realizará la discusión de los hallazgos, y cómo se tomarán decisiones sobre si proceder, modificar o cancelar la operación, vinculación o relación.

- Establecer un lineamiento para el tratamiento de los hallazgos y las “posdebida diligencia”
  - ✓ En el Manual la entidad debe incluir una política que establezca el margen de acción posible ante eventuales hallazgos, contemplando los ajustes que puede realizar la entidad en los términos del acuerdo para mitigar riesgos.
  - ✓ Es fundamental resaltar que no en todos los casos la debida diligencia deriva en una inhabilidad, sin embargo, los hallazgos deben ser objeto de tratamiento.
  - ✓ El tratamiento de los hallazgos puede ir desde cambios en los términos del acuerdo; supervisión especial a la operación, vinculación o relacionamiento; la transferencia del riesgo; solicitar garantías adicionales de cumplimiento o requisitos complementarios; el reporte a autoridades; etc. Los posibles tratamientos los define cada entidad y se pueden ir ajustando conforme la experiencia institucional en gestión del riesgo se haga más compleja.
  - ✓ En la política debe quedar contemplada la obligación de la entidad de examinar continuamente, a lo largo de la vinculación o relación, las operaciones llevadas a cabo por la contraparte relacionada con los hallazgos, para asegurar que sean consistentes con el conocimiento que se tiene de la contraparte, su actividad económica y su perfil de riesgo.

- ✓ Se consideran como alertas que pueden derivar en potenciales hallazgos que requieren tratamiento:
  - No haber identificado plenamente a la contraparte, incluyendo, no conocer sus beneficiarios finales.
  - La existencia de procesos activos o en curso que involucren a la contraparte, haber obtenido referencias negativas o malos antecedentes en la revisión de la reputación. En el caso de las personas jurídicas u otras estructuras, aplicará respecto del representante legal principal y suplente, el revisor fiscal y los miembros de junta directiva, los controlantes y el beneficiario final.
  - Los precios son considerablemente distintos a los normales del mercado, aun cuando no fueron considerados artificiales.
  - La contraparte se financia con recursos internacionales que se originan en países no cooperantes o jurisdicciones de riesgo, según lo defina la normativa nacional.
  - La relación implica que la contraparte deberá contar con subcontratistas.
  - La contraparte está registrada en los listados internacionales vinculantes para el país de personas y entidades asociadas con organizaciones terroristas. En el caso de las personas jurídicas u otras estructuras, aplicará respecto del representante legal principal y suplente, el revisor fiscal y los miembros de junta directiva, los controlantes y el beneficiario final.

- Establece un lineamiento para informar a las autoridades de los hallazgos.

  - ✓ Si se detecta alguna actividad intentada o sospechosa de lavado de activos, financiación del terrorismo y financiación de la proliferación de armas de destrucción masiva, la entidad está obligada a informar a las autoridades competentes, como la Unidad de Información y Análisis Financiero (UIAF) o Fiscalía General de la Nación. Esto es parte del cumplimiento con las leyes.

8.9.3.6 Función de cumplimiento

La función de cumplimiento implica, entre otros aspectos:

- ✓ Velar por el efectivo, eficiente y oportuno funcionamiento del SIGRIP en su conjunto, y cada uno de sus elementos, promoviendo el cumplimiento de sus disposiciones y apoyando a los líderes de procesos y gestores de riesgo, en la gestión de los riesgos identificados. Para estos efectos, se podrán generar políticas o procedimientos internos, vinculantes para la organización.
- ✓ Evaluar el SIGRIP y presentar, en la periodicidad que se establezca, los resultados de la evaluación a la Alta Dirección. Las evaluaciones deberán contemplar, además: o Los resultados de la gestión desarrollada en el marco de la función de cumplimiento.
  - Los reportes de operaciones generados en el marco de la gestión del riesgo.
  - Los planes de mejoramiento del SIGRIP implementados, en el marco del proceso de mejora continua.
- ✓ Revisar y recomendar la implementación de los lineamientos que el Departamento Administrativo de la Función Pública, la Secretaría de Transparencia de la Presidencia

de la República, la Unidad de Información y Análisis Financiero, y las entidades de control, expidan en temas relacionados con la gestión del riesgo.

- ✓ Promover la adopción de correctivos del SIGRIP y adoptar aquellos que estén dentro de su competencia.
- ✓ Articular con las dependencias correspondientes las gestiones pertinentes para la operatividad del SIGRIP, así como el desarrollo de programas internos de capacitación en materia de cumplimiento y gestión del riesgo.
- ✓ Proponer a la Alta Dirección la actualización de los elementos del SIGRIP y velar por su comunicación oportuna a todas las partes interesadas.
- ✓ Colaborar con el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos que requiera el SIGRIP y aplicarlos según corresponda.
- ✓ Establecer los lineamientos institucionales para la aplicación proporcional basada en riesgos de los mecanismos de debida diligencia en el conocimiento de las contrapartes.
- ✓ Elaborar y someter a aprobación de la Alta Dirección, los criterios objetivos para la determinación de las operaciones inusuales y sospechosas.
- ✓ Reportar a la Unidad de Información y Análisis Financiero, a la Fiscalía General de la Nación o a la autoridad que corresponda, las operaciones intentadas o sospechosas que se hayan identificado conforme a los criterios definidos y el procedimiento institucional adoptado.

Para efectos de lo anterior se informa a la Secretaría de Transparencia de la Presidencia de la República el nombre, teléfono de contacto y correo electrónico de la persona quien asuma la función o que lidere el grupo o dependencia.

8.9.3.7 Herramientas de gestión del riesgo

Como herramientas de Gestión del Riesgo la ESE ha definido las siguientes acciones:

- Política para la Gestión Integral de Riesgos,
- Mapa de Riesgos,
- Manual de Debida Diligencia en el Conocimiento de las Contrapartes y una
- Función de cumplimiento distribuida dentro de la organización,
- Códigos de conducta
- Políticas que se requiera como:
  - ✓ Política Antilavado de Activos, Contra la Financiación del Terrorismo y Contra la Financiación de la Proliferación de Armas de Destrucción Masiva (ALA/CFT/CFP).
  - ✓ Política Antisoborno.
  - ✓ Política Antifraude.
- Procedimientos como:
  - ✓ Procedimiento para la gestión de los conflictos de intereses.
  - ✓ Procedimiento para el reporte de operaciones sospechosas.
  - ✓ Procedimiento para la operación del canal institucional de denuncias por Corrupción y buzón ético.

.

8.9.3 Monitoreo, evaluación, auditoría y mejora

El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP debe ser objeto permanente de monitoreo, evaluación, auditoría y mejora. Para este propósito, tendremos en cuenta las siguientes consideraciones:

- En la Política para la Gestión Integral de Riesgos queda establecido la periodicidad y el contenido del monitoreo a los riesgos que gestiona el SIGRIP. En esa medida, los líderes, junto con sus equipos, son los responsables de generar los reportes que la organización determine sobre el estado de la gestión de riesgos en el marco del SIGRIP, y remitirlos al Administrador.
- El Administrador del Programa, desde su rol como segunda línea de defensa, la evaluación de la gestión del riesgo. Se determino el cumplimiento de los objetivos definidos para el Sistema y de cada uno de sus elementos. En la Política para la Gestión Integral de Riesgos se define la periodicidad y los contenidos de la evaluación al SIGRIP.
- El Sistema de Gestión de Riesgos para la Integridad Pública – SIGRIP debe ser objeto de auditoría, la cual estará a cargo de la unidad de control interno o quien ejerza la tercera línea de defensa.

La auditoría se realizará con una evaluación independencia del Sistema para determinar su conformidad y eficacia, tanto del conjunto como de los controles individualmente vistos. La auditoría se realizará bajos las técnicas vigentes, al plan de auditoría de la entidad y desde un enfoque basado en riesgos.

En la Política para la Gestión Integral de Riesgos se establece los criterios de auditoría que aplicaran al SIGRIP.

9. BIBLIOGRAFIA

- Departamento Administrativo de la Función Pública DAFP, establecidos mediante la Guía para la Gestión Integral del Riesgo en Entidades Públicas. Versión 7. 2025

10. CONTROLES

Versión	Descripción del cambio	Fecha Vigencia
01	Creación del Código	Diciembre de 2025.
02	Actualización del Código	Mayo de 2026

Elaborado Por	**Revisado por**	**Aprobado por**
		La Junta Directiva de la E.S.E. Quilisalud.
Nombre: MARTHA LUCIA DIAZ CASTRO	**Nombre:** IVAN ANTONIO LEDEZMA GOMEZ	
Proceso: Planeación y calidad.	**Proceso:** Gerencia.	
Fecha: Mayo 2026	**Fecha:** Mayo 2026.	**Fecha:** Mayo 2025.