Guía

DIR-G-2

Guía Metodológica para la Gestión de Riesgos de Seguridad de la Información

Instituto Caro y Cuervo

Grupo de Planeación y Relacionamiento con el Ciudadano

29/09/2025

TABLA DE INFORMACIÓN DEL DOCUMENTO

Versión	Fecha de aprobación	Elaborado	Revisado	Aprobado	Descripción del cambio
1.0	31/07/2019	Heilin Guarnizo Rodríguez Contratista- Oficial de Seguridad de la Información	Xiomara Ruiz Ballén Coordinadora del Grupo de Planeación	Comité Institucional de Gestión y Desempeño	Creación de la Guía
2.0	29/04/2021	Heilin Guarnizo Rodríguez Contratista- Oficial de Seguridad de la Información	Cristian Velandia Mora Coordinador del Grupo de planeación	Comité Institucional de Coordinación de Control Interno	Actualización del Modelo de Operación por Procesos del ICC, articulando lo desarrollado en las versiones del documento denominado: ORG-PD-01 Elaboración y Control de Documentos
3.0	29/09/2025	Alix Lorena Moreno Córdoba Contratista- Oficial de Seguridad de la Información	Cristian Velandia Mora Coordinador del Grupo de Planeación	Comité Institucional de Coordinación de Control Interno	Actualización del documento de acuerdo con la actualización del formato de gestión de riesgos: Mapa riesgos de seguridad digital. Cambio del nombre de Riesgos de Seguridad Digital a Riesgos de Seguridad de la Información.

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

INTRODUCCIÓN

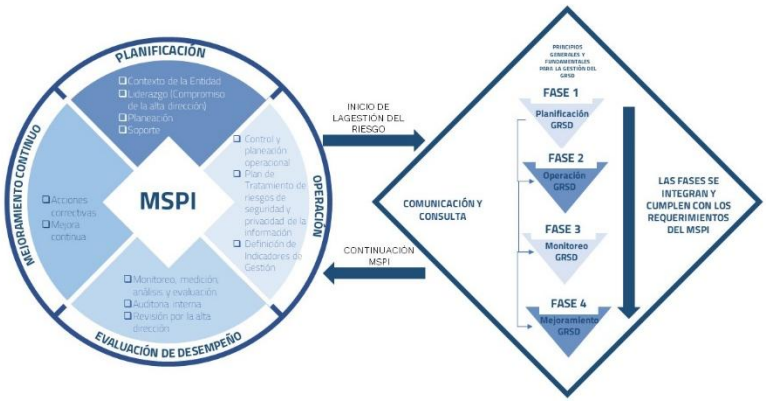
La gestión de riesgos en materia de seguridad digital constituye una estrategia clave para proteger los activos de información, garantizar la integridad de los sistemas institucionales y preservar la confianza de los usuarios. En un entorno digital en constante evolución, las entidades públicas deben adoptar enfoques integrales que permitan identificar, anticipar y mitigar amenazas a las que puede quedar expuesta al momento de llevar a cabo actividades socio económicas en el entorno digital (prestación de trámites, servicios internos y externos, transacciones en línea entre otros), así como responder de manera oportuna ante incidentes que puedan comprometer la seguridad de la información para fomentar y mantener la confianza de las múltiples partes interesadas (proveedores, ciudadanos, entidades públicas y privadas) en el uso del entorno digital en su interacción con Estado.

En este marco, el Instituto Caro y Cuervo ha avanzado en la implementación de mecanismos orientados a fortalecer su Sistema de Gestión de Seguridad de la Información (SGSI), reconociendo la importancia de incorporar la gestión de riesgos como componente transversal en todas las fases del proceso.

Dando aplicación a La Directiva Presidencial 02 de 2022 número 5: Adoptar la seguridad digital con un enfoque preventivo y proactivo basado en la gestión efectiva de riesgos en el entorno digital, priorizando la protección de datos personales e información sensible de la entidad o que goza de reserva legal, al igual que de los servicios y sistemas de información e infraestructuras críticas y de acuerdo con lo indicado en el ámbito de aplicación del Decreto 1078 de 2015, respecto a la Política de Gobierno Digital, las entidades públicas deben realizar la implementación del Modelo de Seguridad y Privacidad de la Información –MSPI– con el objetivo de conformar un Sistema de Gestión de Seguridad de la Información –SGSI– al interior de la entidad .En el MSPI se incorpora un componente de gestión de riesgos en las etapas de planificación, implementación, evaluación y mejora. Este modelo es el adoptado por el Instituto Caro y Cuervo en la ejecución del SGSI.

De acuerdo con lo anterior, la relación e interacción entre la gestión de seguridad de la información con el Modelo Nacional de Gestión de Riesgos de Seguridad de la información –MGRSD– se visualiza y se describe de la siguiente manera:

Ilustración 1 Interacción entre el MSPI y el MGRSD



En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

- Las actividades de identificación de activos, análisis, evaluación y tratamiento de los riesgos se alinean con la Fase de Planificación del MSPI.
- Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la Fase de Implementación del MSPI.
- Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la Fase de Medición del desempeño del MSPI.
- Las actividades de mejoramiento continuo en ambos modelos son similares y trabajan simultáneamente ya que dependen de las fases de Medición del desempeño para identificar aspectos a mejorar en la aplicación de ambos modelos.

1 OBJETIVO

Ofrecer una guía metodológica para la gestión de riesgos de seguridad de la información en el Instituto Caro y Cuervo en la cual se identifiquen las amenazas y vulnerabilidades a las que los activos de información pueden estar expuestos, con el fin de establecer controles, incrementar la confianza de las múltiples partes interesadas y del aseguramiento de los activos de información en la entidad.

1.1 Objetivos específicos

- Evaluar y analizar los riesgos de seguridad de la información relacionados con los activos de información, que pueden tener un impacto en el desarrollo de la misión del Instituto Caro y Cuervo.
- Identificar las amenazas y vulnerabilidades de seguridad de la información, asociadas a los activos con criticidad alta en los procesos de la entidad.
- Definir el plan de tratamiento del riesgo residual de la entidad.
- Identificar los controles aplicados para minimizar la acción del riesgo inherente en la entidad.

2 ALCANCE

Este documento se articula y complementa lo expuesto en la Política de administración del riesgo, definida y adoptada en el Instituto Caro y Cuervo; por tanto, aplica a todos los procesos de la entidad.

3 TÉRMINOS Y DEFINICIONES

Activo: Cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información, son activos los elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis del riesgo: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Apetito de riesgo: Nivel máximo de riesgo que la entidad está dispuesta a asumir.

Consecuencia: Resultado o impacto de un evento que afecta a los objetivos.

Controles: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Criterios del riesgo: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

Evaluación del riesgo: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Identificación del riesgo: Proceso para encontrar, reconocer y describir el riesgo.

Impacto: Costo para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros, por ejemplo: pérdida de reputación, implicaciones legales, etc.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad.

Política: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.

Reducción del riesgo: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.

Riesgos de seguridad de la información: posibilidad de combinación de amenazas y vulnerabilidad en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo residual: Riesgo que permanece tras el tratamiento del riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4 REFERENCIAS NORMATIVAS

- ISO 31000:2018: Norma internacional que proporciona principios y directrices para la gestión de riesgos en cualquier tipo de organización. Describe un enfoque sistemático y estructurado para identificar, analizar, evaluar, tratar, supervisar y comunicar los riesgos. Aunque no es una norma certificable, sirve como guía para implementar un sistema de gestión de riesgos efectivo, mejorando la toma de decisiones y la eficiencia operativa.

- ISO 27005: Proporciona orientación sobre la gestión de riesgos de seguridad de la información, apoyando la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001. Es una guía para identificar, analizar, evaluar y tratar los riesgos que pueden afectar la seguridad de la información de una organización.

- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6: Se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI) 12, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

- Directiva Presidencial 02 de 2022, Reiteración de la política pública en materia de seguridad digital.

5 DESCRIPCIÓN

El documento ofrece la metodología para la gestión de riesgos de seguridad de la información en el Instituto Caro y Cuervo en la cual se identifiquen las amenazas y vulnerabilidades a las que los activos de información pueden estar expuestos. Establecer controles, plantear y realizar el tratamiento de riesgos de seguridad de la información.

6 CONTEXTO ESTRATÉGICO

El Instituto Caro y Cuervo fue creado en 1942 mediante la Ley 5.a del 25 de agosto de 1942. Tiene por objeto "promover y desarrollar la investigación, la docencia y el asesoramiento y la divulgación de las lenguas del territorio nacional y de sus literaturas, con miras a fortalecer su uso y reconocimiento con base en su prestigio social y valoración estética. Con este fin, el Instituto Caro y Cuervo asesora al estado colombiano y contribuye en la elaboración de políticas para el fortalecimiento, conservación del patrimonio inmaterial de la Nación. De igual manera, preserva, compila, publica y distribuye documentos escritos y audiovisuales, así como elementos del patrimonio inmaterial, para contribuir con la conservación de la historia de la cultura colombiana." (Acuerdo 002 de 2010).

Por consiguiente, la gestión de riesgos de seguridad de la información, está orientada hacia la protección de la disponibilidad, integridad y confidencialidad de los activos de información que se generan, se producen, se almacenan y se trasmiten, , buscando prevenir la materialización de amenazas producto de vulnerabilidades que pueden afectar la información concerniente al desarrollo de la investigación, la docencia, el asesoramiento, la divulgación de las lenguas en el territorio nacional y de sus literaturas; además, el Instituto Caro y Cuervo incide en la salvaguarda del patrimonio lingüístico de la Nación principalmente, a través de una amplia oferta académica consolidada como Institución autorizada por el Ministerio de Educación Nacional para impartir programas de educación superior de posgrado a través dela Facultad Seminario Andrés Bello FSAB.

6.1 Contexto externo e interno de la entidad

Conforme lo indica el Departamento Administrativo de la Función Pública, el Instituto Caro y Cuervo debe realizar la identificación del contexto interno y externo de la entidad relacionado con seguridad de la Información, la definición de este contexto se encuentra definido en el documento denominado "Manual de Administración del Riesgo, el cual busca proteger los activos, de los potenciales riesgos asociados a la prestación del servicio, así mismo, se compromete a establecer los mecanismos necesarios para evitar, reducir, compartir y asumir los riesgos relacionados con el desarrollo de sus procesos y que pudieran afectar negativamente a las personas, las instalaciones, los bienes y los equipos; para tal efecto realiza la identificación, análisis, valoración e intervención de los riesgos inherentes al quehacer institucional, contribuyendo de esta forma al logro de los objetivos, la misión y la visión.

7 POLÍTICA DE GESTIÓN DE RIESGOS

La Política de gestión de riesgos de seguridad de la información definida para la entidad, se encuentra integrada y se desarrolla en el documento denominado "Política de administración del riesgo" contenida en el Manual administración del riesgo DIR-M-01.

8 ROLES Y RESPONSABILIDADES

Los roles y responsabilidades en materia de seguridad de la información definidos para el Instituto Caro y Cuervo se encuentran integrados en el documento denominado “Manual de políticas de seguridad y privacidad de la información” A continuación se describen los roles y responsabilidades para la gestión de Riesgos de Seguridad de la Información.

Roles	Responsabilidades
Dirección General	Asignar los recursos pertinentes para la aplicación eficaz de las Políticas de Seguridad de la Información de la institución.
Comité de Seguridad de la Información (Comité Institucional de Gestión y Desempeño)	Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
Oficial de Seguridad de la Información	Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del proyecto para darle solución oportuna y escalar al Comité de seguridad en caso de ser necesario.
Grupo de Tecnologías de la Información	Implementar los controles y planes de tratamiento de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
Demas grupos, oficinas, dependencias en el ICC	Implementar los controles y planes de tratamiento desde su función en el Instituto que ayuden a mitigar los riesgos de seguridad de la información.

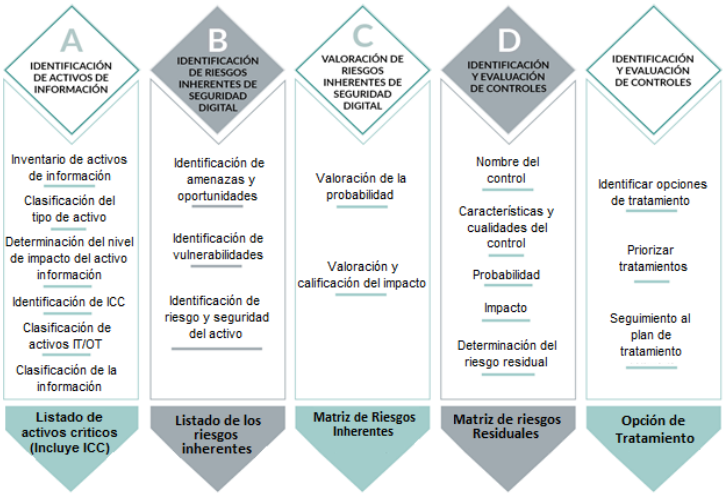
9 RECURSOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La identificación de los recursos necesarios para la gestión de riesgos de seguridad de la información debe ser realizada por los líderes de proceso, en conjunto con el oficial de cumplimiento de seguridad de la información; esta necesidad de recursos (capital, tiempo, personal, procesos, sistemas y tecnologías) deberá ser presentada a la alta dirección quien es el que define la prioridad del tratamiento, según el impacto que pueda generar en la entidad.

10 GESTIÓN DE RIESGOS

Cada una de las acciones define sus salidas, las cuales se ilustran a continuación:

Ilustración 2 Ejecución de la GRSD



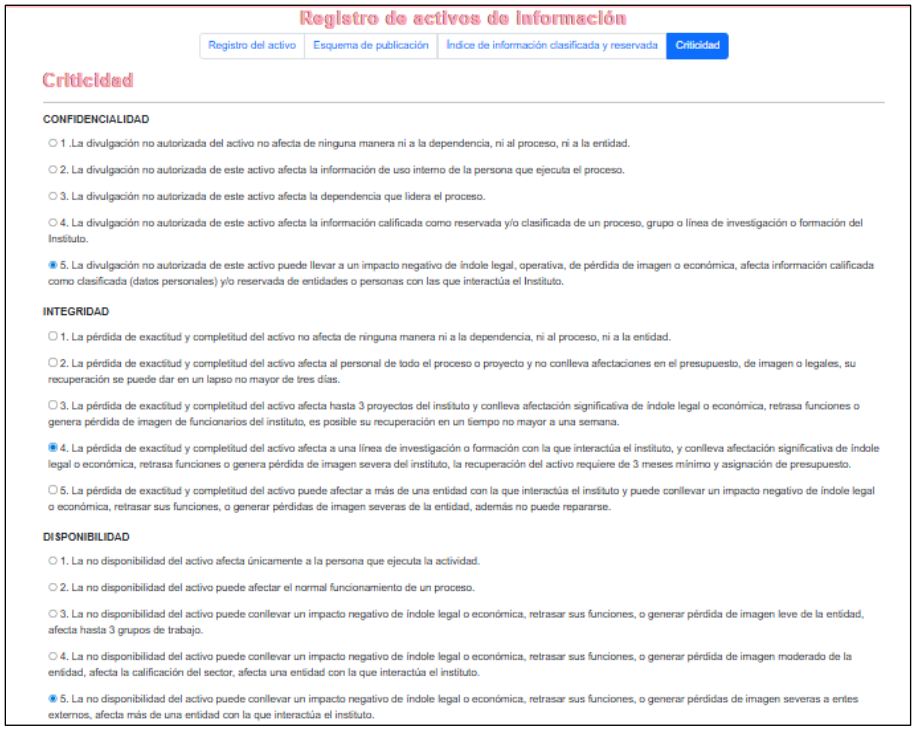
10.1 Identificación de los activos de información

El Instituto Caro y Cuervo realiza la identificación de todos los activos de información en el Sistema de información proporcionado por el grupo de las TIC; para realizar esta actividad se establece el documento denominado “Guía gestión activos de información”. La identificación y valoración de activos debe ser realizada por los líderes del proceso y/o quien delegue, –debidamente orientado por el responsable de seguridad de la información de la entidad pública.

- **Criterios de selección de los activos:** Para realizar el proceso de gestión de riesgos de seguridad digital se seleccionarán aquellos activos de información que cumplan cualquiera de estas condiciones:

    - Criticidad: Activos de información cuyo nivel de criticidad sea Alto, en el proceso de identificación y valoración de activos.

Ilustración 3 Criticidad de Activos de Información



- Calificación 1712: Activos de información que recibieron la calificación de “clasificada” y de “reservada”.

Ilustración 4 Índice de información Clasificada y Reservada

- La gestión del activo de información afecta de manera directa o importante el servicio que se presta hacia terceros.

Nota: Cuando se evidencie en el aplicativo que los procesos realizaron la identificación de sus activos por series documentales y se detallen los tipos documentales, la gestión del riesgo se realizará sobre la serie documental.

10.2 Identificación Del Riesgo

10.2.1 Cualificación del riesgo

Este primer bloque relaciona los siguientes campos:

- **ID_R:** Consecutivo para numerar el riesgo identificado
- **Proceso:** Define el proceso en el cual se identificó el activo con criticidad Alta
- **Oficina Productora:** Define el grupo u oficina que identificó el activo con criticidad Alta
- **Código Riesgo:** Nomenclatura para identificar el riesgo teniendo en cuenta el proceso, la oficina productora y vigencia de la gestión del riesgo.
- **Tipo activo de información:** Lista desplegable para escoger el tipo de activo con criticidad Alta
- **Nombre activo de información:** Identificador del activo definido con criticidad Alta y al cual se le identificará el riesgo.
- **Factor de riesgo:** Lista desplegable que indica la fuente generadora del riesgo.
- **Riesgos inherentes de seguridad digital:** Se pueden identificar los siguientes tres (3) riesgos inherentes de seguridad digital:
  - **Pérdida de la confidencialidad**: protección de la información para asegurar que solo las personas autorizadas puedan acceder a ella.
  - **Pérdida de la integridad**: garantiza la precisión, consistencia y fiabilidad de los datos, protegiéndolos contra modificaciones no autorizadas, ya sea accidental o maliciosa
  - **Pérdida de la disponibilidad**: capacidad de un sistema o información de estar accesible y utilizable para los usuarios autorizados cuando la necesitan.
- **Identificación de amenazas:** Los activos de información están expuestos a amenazas, las cuales buscan la explotación de la vulnerabilidad existente afectando los activos de información y provocando un impacto en el desarrollo normal de la entidad.

Ilustración 5 Flujo de amenazas

Dentro de las amenazas más comunes están:

- **De origen natural**: accidentes naturales (terremotos, inundaciones, ...). Ante esos cambios el sistema de información es víctima pasiva, pero de todas formas se tiene en cuenta lo que puede suceder.
- **Del entorno (de origen industrial)**: desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.
- **Defectos de las aplicaciones:** problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidad técnica o simplemente vulnerabilidad.
- **Causadas por las personas de forma accidental:** Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.
- **Causadas por las personas de forma deliberada:** Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir; es decir, las instalaciones pueden incendiarse, pero las aplicaciones no; las personas pueden ser objeto de un ataque bacteriológico, pero los servicios no; sin embargo, los virus informáticos afectan a las aplicaciones, no a las personas.

- **Vulnerabilidades:** La sola presencia de una vulnerabilidad no causa daños por sí misma, ya que representa únicamente una debilidad de un activo o un control, para que la vulnerabilidad pueda causar daño, es necesario que una amenaza pueda explotar esa debilidad. Una vulnerabilidad que no tiene una amenaza puede no requerir la implementación de un control.
- **Descripción del riesgo:** Indica la concatenación del riesgo identificado y la amenaza definida. La cualificación del riesgo, tal como lo muestra la ilustración, es el inicio del ejercicio de gestión de riesgos de Seguridad de la Información.

Ilustración 6 Cualificación del riesgo

				1.1 Cualificación del riesgo						
ID_I	Proceso	Oficina Productora	Código Ries	Tipo activo d información	Nombre activo de informació	Factor de ries	Riesgo seguri	Amenaza	Vulnerabilidades (Causa	Descripción del riesgo
1	Adquisiciones	Gestión Contractual	ADQ-GC1	Información	Actas (Comité de Defensa)	F_Talento_Humano	pérdida de confidencialidad	Fuga de información	Falla accidental de custodia de la información.	pérdida de confidencialidad debido a factores externos como: Fuga de información

10.2.2 Cuantificación del riesgo

- **Frecuencia:** Se refiere a la cantidad de veces que se realiza la actividad que origina el riesgo en un año

Tabla 1 Ejemplo de frecuencia

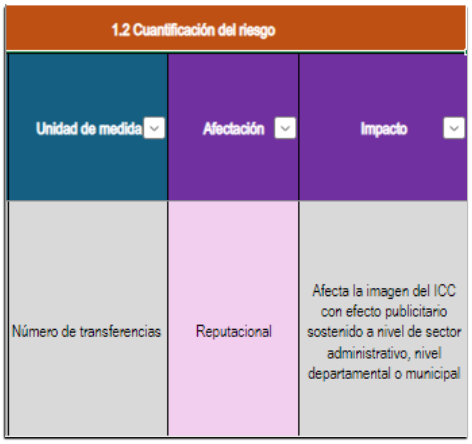
Actividad	Frecuencia de la actividad
Tecnología (incluye disponibilidad de aplicativos), tesorería. **Nota:** En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. **Ejemplo:** Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia, su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria

Tabla 2 Definición de frecuencia

Frecuencia de la Actividad (veces por año)	
La actividad que conlleva el riesgo se ejecuta…	
Mínimo	**Máximo**
0	2
3	24
25	500
501	5.000
5.001	10.000

- **Unidad de medida:** Corresponde al entregable que resulta de realizar la actividad que origina el riesgo.
- **Afectación:** Lista desplegable que indica la afectación que se genera si el riesgo se materializa, la cual puede ser: Operacional o Reputacional.
- **Impacto:** Indica el nivel de afectación del riesgo si es Operacional o Reputacional

Ilustración 7 Cuantificación del riesgo



10.3 Análisis Del Riesgo Inherente

10.3.1 Análisis probabilidad

- **Probabilidad inherente:** Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, Para determinar la probabilidad, el Instituto Caro y Cuervo define los criterios establecidos en su Política institucional de administración del riesgo definida y adoptada en la entidad así:

Tabla 3 Definición de probabilidad

Actividad	Probabilidad frente al riesgo
Tecnología (incluye disponibilidad de aplicativos), tesorería. **Nota:** En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. **Ejemplo:** Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia, su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Muy alta

Tabla 4 Definición de probabilidad

PROBABILIDAD		
Cuantitativa		Cualitativa
Mínimo	Máximo	
0,00%	20,00%	Muy Baja
20,01%	40,00%	Baja
40,01%	60,00%	Media
60,01%	80,00%	Alta
80,01%	100,00%	Muy Alta

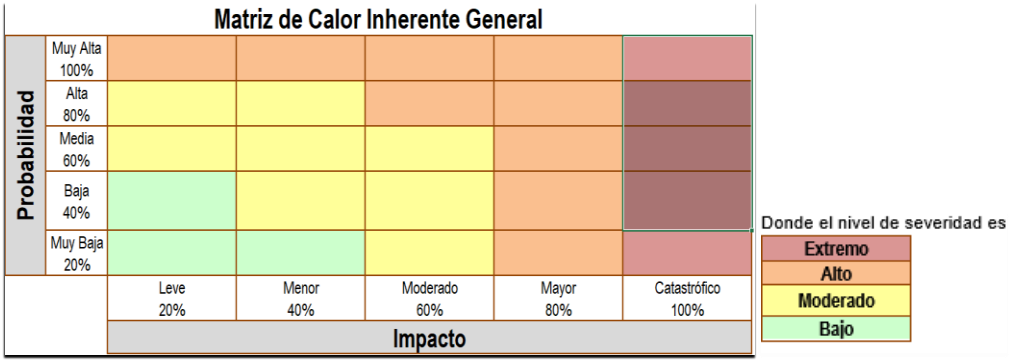
- **Impacto inherente:** El Instituto Caro y Cuervo mide el impacto en su Política institucional de administración del riesgo, por lo que define los siguientes criterios en el caso que se llegue a materializar el riesgo.

Tabla 5 Impacto del riesgo

Afectación		IMPACTO		
Económica	Reputacional	Cuantitativo		Cualitativo
Afectación en SMLMV	El riesgo afecta la imagen de…	Mínimo	Máximo	
Menor a 10 SMLMV	Alguna área de la organización	0,00%	20,00%	Leve
Entre 10 y 50 SMLMV	La entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores	20,01%	40,00%	Menor
Entre 50 y 100 SMLMV	La entidad con algunos usuarios de relevancia frente al logro de los objetivos	40,01%	60,00%	Moderado
Entre 100 y 500 SMLMV	La entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal	60,01%	80,00%	Mayor
Mayor a 500 SMLMV	La entidad a nivel nacional, con efecto publicitarios sostenible a nivel país	80,01%	100,00%	Catastrófico

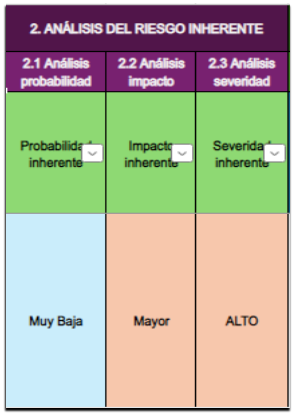
- **Severidad inherente:** Se logra a través de la determinación de la probabilidad y el impacto que puede causar la materialización del riesgo, teniendo en cuenta la siguiente tabla:

Ilustración 8 Probabilidad vs Impacto Inherente



Nota: Los criterios para la estimación del riesgo inherente se encuentran en el manual para la administración del riesgo

Ilustración 9 Cuantificación del riesgo



10.4 Diseño y Análisis De Controles

Una vez establecidos y valorados los riesgos inherentes se deben identificar los controles existentes para evitar trabajo o costos innecesarios

10.4.1 Descriptores del control

- **Responsable de ejecutar:** Se refiere al cargo o rol responsable de ejecutar el control
- **Acción de control:** Corresponde a la descripción del control existente

10.4.2 Atributos de eficiencia

- Periodicidad del control: Corresponde a la frecuencia de ejecución del control
- Momento de ejecución: Identifica si el control es preventivo, correctivo o detectivo. Se considera un control detectivo si este aporta a la efectividad si se ha materializado el riesgo.
- Forma de ejecución: Identifica como se ejecuta el control: Automático o Manual.

Ilustración 10 Diseño y Análisis de Controles

3. DISEÑO Y ANÁLISIS DE CONTROLES			
3.1 Descriptores del control		3.2 Atributos de eficiencia	
Responsable de ejecutar	Acción de control	Momento de ejecución	Forma de ejecución
1. Tecnico Administrativo Grado 13 2. Tecnico Administrativo Grado 13	1. Custodia en el repositorio de G.Contractual 2. Archivador físico con llave	Preventivo	Manual

10.5 Evaluación Del Riesgo Residual

10.5.1 Riesgo residual:

Es el resultado de aplicar la efectividad de los controles al riesgo. Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, se procede a la elaboración del mapa de riesgo residual. Debe tenerse en cuenta el manual “administración del riesgo” establecido en el Instituto Caro y Cuervo.

Ilustración 11 Probabilidad vs Impacto Residual

Matriz de Calor Residual General

Probabilidad						
	Muy Alta 100%					
	Alta 80%	Rr5 Rr55	Rr9 Rr59			
	Media 60%					
	Baja 40%					
	Muy Baja 20%	Rr15 Rr21 Rr32 Rr33 Rr40 Rr65 Rr71 Rr82 Rr83 Rr90			Rr47 Rr97	
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
		Impacto				

Donde el nivel de severidad es

Extremo
Alto
Moderado
Bajo

- **Probabilidad residual:** Resulta de correr una celda hacia abajo en la probabilidad inherente posterior a la implementación de controles
- **Impacto residual:** Resulta de correr una celda hacia la izquierda en el impacto inherente posterior a la implementación de controles
- **Severidad residual:** Se logra a través de la determinación de la probabilidad y el impacto residuales.

Ilustración 12 Evaluación Del Riesgo Residual

4. EVALUACIÓN DEL RIESGO RESIDUAL		
4.2 Riesgo residual		
Probabilidad residual	Impacto residual	Severidad residual
Muy Baja	Moderado	MODERADO

10.6 Estrategias para administración del riesgo

10.6.1 Estrategias para desarrollar con el plan de reducción

- **Tratamiento:** Una vez se han identificado los riesgos residuales, se debe reportar el plan de tratamiento. El oficial de seguridad de la información apoyará y acompañará a los diferentes procesos tanto para el reporte como para la gestión y el tratamiento de estos riesgos.

  El plan de tratamiento general será presentado y socializado al Comité Institucional de Evaluación y Desempeño, para definir y priorizar los activos que deben ser tratados inmediatamente y se lee deba realizar una asignación de recursos adicionales para la implementación de nuevos controles; esto no quiere decir que no se deben gestionar los demás riesgos.

Las opciones de tratamiento pueden ser:

  - Aceptar el riesgo: Si el resultado de Severidad residual es Muy baja - Leve
  - Evitar el riesgo: Si el resultado de Severidad residual está por encima del nivel: Muy baja – Leve y su materialización puede poner en riesgo la operación en el ICC.
  - Reducir (compartir el riesgo): Si el resultado de Severidad residual está por encima del nivel: Muy baja – Leve, y es un riesgo que el ICC no puede tratar.
  - Reducir (mitigar el riesgo): Si el resultado de Severidad residual está por encima del nivel: Muy baja – Leve, y es un riesgo que el ICC puede tratar.

- **Actividad fortalecimiento:** Describe el desarrollo de las medidas para fortalecer los controles implementados
- **Periodicidad de la actividad de fortalecimiento:** Describe la cantidad de veces en el año que se ejecutará desde el inicio hasta el fin del plan de tratamiento de riesgos de seguridad de la información.
- **Responsable estrategia:** Cargo o rol de la persona que ejecutará el plan de tratamiento de riesgos, basado en la actividad de fortalecimiento.
- **Fecha inicio:** Fecha en la cual inicia la actividad de fortalecimiento.
- **Fecha fin:** Fecha en la cual finaliza la actividad de fortalecimiento.
- **Estado de la actividad:** Estatus de ejecución de la actividad de fortalecimiento.

Ilustración 13 Estrategia de administración del riesgo

5. ESTRATEGIAS PARA ADMINISTRACIÓN DEL RIESGO					
5.1 Estrategias a desarrollar con el plan de reducción					
Tratamiento	Actividad fortalecimiento	Responsable estrate	Fecha inici	Fecha fin	Estado de la activid
Reducir (mitigar)	1. Validar y gestionar los accesos al repositorio solo al personal autorizado. (OneDrive)	1. Gestión Contractual	10/03/2025	31/07/2025	Sin iniciar

10.7 Monitoreo de la administración del riesgo

Esta actividad estará a cargo del oficial de seguridad del Instituto Caro y Cuervo, para ello se definen dos ítems para el seguimiento del plan de tratamiento de riesgos

10.7.1 Monitoreo del plan de reducción

- **Fecha de Monitoreo:** Especifica la fecha en la cual se ejecuta el monitoreo del plan
- **Evidencia de implementación de la actividad:** Se indica una breve descripción de la evidencia que garantiza el desarrollo de la actividad de fortalecimiento.
- **Estado de la actividad:** Proporciona el estatus de la actividad de fortalecimiento. Puede ser diferente del estado en el ítem: Estrategias a desarrollar con el plan de reducción a consideración del oficial de seguridad de la información.
- **Observaciones sobre el plan:** Son las consideraciones adicionales que puede determinar el oficial de seguridad de la información. Respecto al monitoreo del plan de reducción.

10.7.2 Monitoreo del control

- **Evidencia de ejecución del control:** Se indica una breve descripción de la evidencia que garantiza el desarrollo del control especificado en el ítem: Diseño y Análisis De Controles

- **Observaciones sobre el control:** Son las consideraciones adicionales que puede determinar el oficial de seguridad de la información. Respecto al Diseño y Análisis De Controles

Ilustración 14 Monitoreo de la Administración del Riesgo

6. Monitoreo de la administración del riesgo					
6.1 Monitoreo del plan de reducción				6.2 Monitoreo del control	
Fecha d Monitoreo	Evidencia de implementación d actividad	Estado de l actividad2	Observacione sobre el plan	Evidencia de ejecuci del control	Observaciones so el control
01/08/2025	Captura de pantalla de los accesos otorgados en el repositorio	Cumplido	Se ha desarrollado la actividad de fortalecimiento dentro del plazo establecido	Captura de la custodia física en archivador Correo electrónico de solicitud de accesos al repositorio	Los controles no son realizados a una periodicidad definida

10.8 Seguimiento a la administración del riesgo

Se debe diligenciar por la Primera Línea de Control del equipo MECI con el objeto de realizar seguimiento a la gestión de riesgos. Se debe dar respuesta a las siguientes preguntas con un SI o un NO. En caso del NO se debe justificar la respuesta referente a los siguientes cuestionamientos:

- ¿La identificación del riesgo es adecuada?
- ¿El diseño del control es adecuado?
- ¿Se evidencia ejecución del control?
- ¿El plan de reducción ha permitido mejorar el control?
- ¿Se presentaron eventos de materialización del riesgo?
- Observaciones del seguimiento: Son las consideraciones adicionales que puede determinar el equipo MECI referente al seguimiento.