2021

Guía

DIR-G-2

Guía Metodológica para la Gestión de Riesgos de Seguridad Digital

Pertenece al procedimiento
MEJ-P-02 Administración del riesgo

Instituto Caro y Cuervo
Grupo de Planeación
29/04/2021

INFORMACIÓN DEL DOCUMENTO

Versión	Fecha de aprobación	Elaborado por:	Revisado por:	Aprobado por:	Descripción del Cambio
1.0	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	Se crea la guía de acuerdo con la actualización del Modelo de Operación por Procesos del ICC, articulando lo desarrollado en las versiones del documento denominado: TIC-G-03 GUÍA METODOLÓGICA PARA LA DE RIESGOS DE SEGURIDAD DIGITAL

TABLA DE CONTENIDO

1. INTRODUCCIÓN 4
2. OBJETIVO 5
2.1. OBJETIVOS ESPECÍFICOS 5
3. ALCANCE 5
4. TERMINOS Y DEFINICIONES 5
5. DESCRIPCIÓN DEL DOCUMENTO 7
6. CONTEXTO ESTRATEGICO 7
6.1. CONTEXTO EXTERNO E INTERNO DE LA ENTIDAD 7
6.2. CONTEXTO DEL PROCESO 8
7. POLÍTICA DE GESTIÓN DE RIESGOS 8
8. ROLES Y RESPONSABILIDADES 8
9. RECURSOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL 8
10. GESTIÓN DE RIESGOS 8

A. Identificación de los activos de información 9

B. Identificación de riesgos inherentes de seguridad digital 10

C. Valoración de riesgos inherentes de seguridad digital 15

D. Identificación y evaluación de controles 17

TABLAS

Tabla 1. Impacto social, económico y ambiental 10
Tabla 2. identificación y análisis del riesgo inherente 14
Tabla 3. Criterios de actividad 15
Tabla 4. Frecuencia de la actividad 15
Tabla 5. Criterios de riesgo. 16
Tabla 6. Diseño, análisis y evaluación de controles. 18
Tabla 7. Evaluación del riesgo residual 19
Tabla 8. Plan de tratamiento de riesgos de seguridad digital 20
Tabla 9. Monitoreo de la administración del riesgo 21

TABLAS DE FIGURAS

Figura 1.Interacción entre el MSPI y el MGRSD 4
Figura 2. Ejecución de la GRSD 9
Figura 3. identificación de amenazas 11

TABLA DE GRAFICAS

Grafica 1. Matriz de Calor Inherente General 17
Grafica 2. Matriz de Calor Residual General. 19

1. INTRODUCCIÓN

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 Digital –MGRSD– se visualiza y se describe de la siguiente manera:

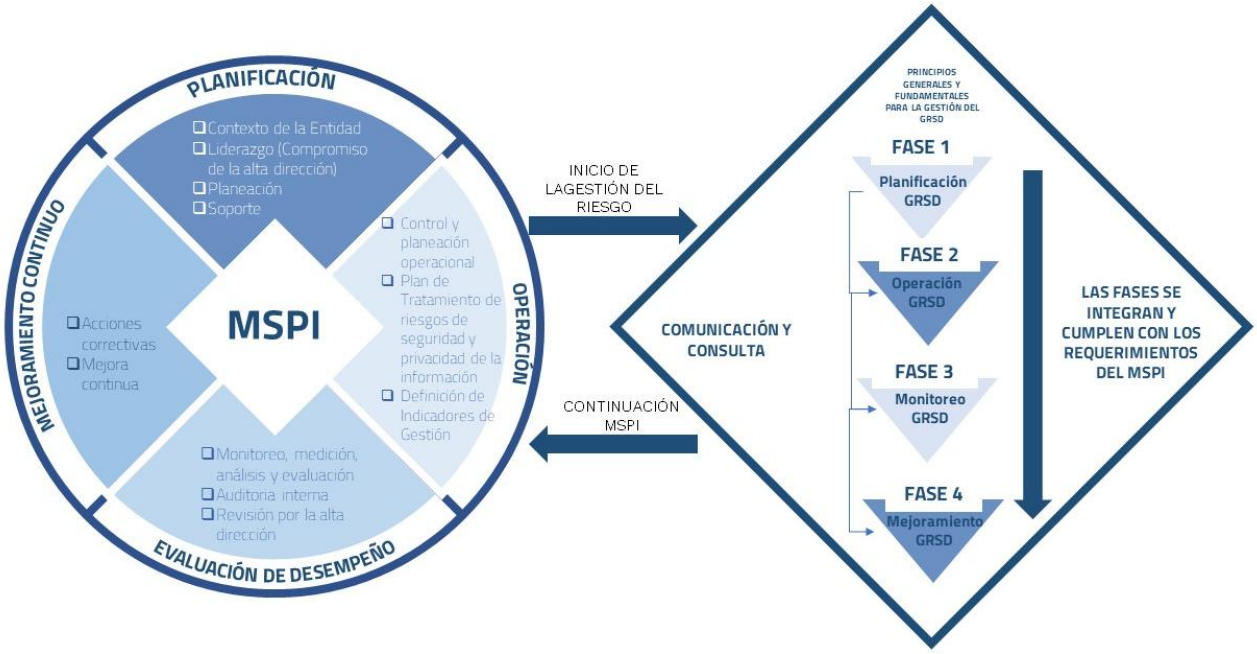

Figura 1.Interacción entre el MSPI y el MGRSD

Fuente: Ministerio de Tecnologías de la información y las Comunicaciones - MinTIC.

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.

2. OBJETIVO

Ofrecer una guía metodológica para la gestión de riesgos de seguridad digital 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 desde el ambiente cibernético, con el fin de establecer controles, incrementar la confianza de las múltiples partes interesadas en el medio digital y del aseguramiento de los activos de información en la entidad.

2.1. OBJETIVOS ESPECÍFICOS

a) Evaluar y analizar los riesgos de seguridad digital y 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.

b) Identificar las amenazas y vulnerabilidades de seguridad digital y de la información, asociadas a los activos de mayor impacto en los procesos de la entidad.

c) Definir el plan de tratamiento del riesgo residual de la entidad.

3. 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.

4. TERMINOS Y DEFINICIONES

Activo: Cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, 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.

CSIRT: Equipo de respuesta a incidentes de seguridad informática.

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.

Perfil del riesgo: Descripción de cualquier conjunto de riesgos.

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 digital: 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.

5. DESCRIPCIÓN DEL DOCUMENTO

Documento que tiene por objetivo ofrecer la metodología para la gestión de riesgos de seguridad digital 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 desde el ambiente cibernético, con el fin de establecer controles, incrementar la confianza de las múltiples partes interesadas en el medio digital y del aseguramiento de los activos de información en la entidad.

6. CONTEXTO ESTRATEGICO

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 digital, 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, teniendo en cuenta aquellos activos digitales que apoyan la gestión de los procesos, por medio del uso de las tecnologías de la información, buscando prevenir la materialización de amenazas 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 de Educación Superior –IES– por su Facultad Seminario Andrés Bello –FSAB–.

6.1. CONTEXTO EXTERNO E INTERNO DE LA ENTIDAD

Conforme lo indica el Función Pública, el Instituto Caro y Cuervo debe realizar la identificación del contexto interno y externo de la entidad relacionado con seguridad digital, la definición de este contexto se encuentra definido en documento denominado "Manual del sistema de gestión de seguridad de la información".

6.2. CONTEXTO DEL PROCESO

La Gestión de riesgos de seguridad digital se encuentra alineada con el SGSI y se encuentra como parte de las actividades relacionadas en el Plan de seguridad y privacidad de la información definido por la entidad, cabe precisar que dicho sistema de información es liderado por el proceso estratégico denominado "Direccionamiento estratégico".

Teniendo en cuenta que el Grupo de Tecnologías de la Información y las Comunicaciones –TIC– tiene dentro de sus funciones *"Definir estrategias y procesos que garanticen, la disponibilidad, confiabilidad, confidencialidad, integridad eficiencia y eficacia de los productos que maneja el Instituto"* los procedimientos, políticas, guías, manuales y formatos que hacen parte de la gestión de riesgos de **seguridad digital** se encuentran ubicados en el proceso de apoyo denominado "Mejoramiento Continuo".

7. POLÍTICA DE GESTIÓN DE RIESGOS

La Política de gestión de riesgos de seguridad digital definida para la entidad, se encuentra integrada en el documento denominado "Política de administración del riesgo".

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 del sistema de gestión de seguridad de la información". Cabe aclarar que el profesional responsable de la seguridad de la información es el mismo para seguridad digital y pertenece al grupo de Planeación.

9. RECURSOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL

La identificación de los recursos necesarios para la gestión de riesgos de seguridad digital debe ser realizada por los líderes de proceso, en conjunto con el profesional de seguridad digital; 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:

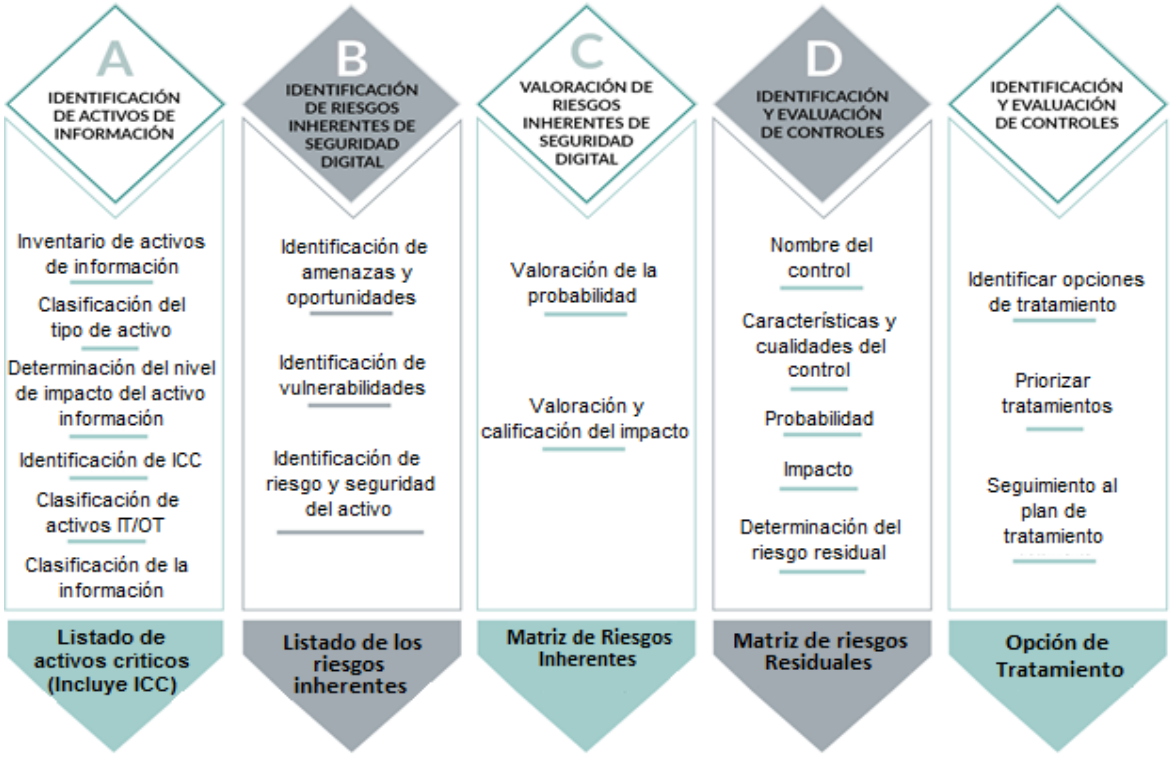

Figura 2. Ejecución de la GRSD

Fuente: MinTIC.

A. 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 la Primera línea de defensa –Líderes de proceso–, en cada proceso donde aplique la gestión del riesgo de seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o 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 igual o superior a 4, en el proceso de identificación y valoración de activos.
  - **Calificación 1712:** Activos de información que recibieron la calificación de "**clasificada**" y de "**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.

A.1 Identificar si existen infraestructuras críticas: Culminado el paso anterior, la entidad determina si los procesos en los cuales identificó los activos de información son servicios esenciales y si estos hacen parte de la infraestructura crítica cibernética (ICC) del país. De acuerdo con los lineamientos de la función pública, un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios:

IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	**$464.619.736**	**3 años en recuperación**

Tabla 1. Impacto social, económico y ambiental

Fuente: Tomado de Comando Conjunto Cibernético (CCOC), Comando General Fuerzas Militares de Colombia. Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia Primera Edición.

El Instituto Caro y Cuervo determina si los activos identificados en cada uno de sus procesos proveen servicios esenciales, entendidos estos como "los necesarios para el mantenimiento de las funciones sociales básicas, salud, seguridad, bienestar social y económico de los ciudadanos o el funcionamiento de las instituciones del Estado y de las administraciones públicas", en el caso de que si se determine que tiene Infraestructuras Críticas Cibernéticas, es importante que se identifiquen los componentes que conforman dicha infraestructura. Por ejemplo, dicha ICC puede tener componentes de TI (como servidores) o de TO (como sistemas de control industrial o sensores).

B. Identificación de riesgos inherentes de seguridad digital

Se pueden identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

La variación es amenazas y vulnerabilidades que pueda causar que dichos riesgos se materialicen. Para cada riesgo, se deben asociar el grupo de activos específicos del proceso y, conjuntamente, analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización.

✓ 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.

Figura 3. identificación 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[1].

[1] Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT.

La siguiente tabla es un ejemplo de cómo realizar la identificación de riesgos inherentes de seguridad digital:

Identificación y análisis del riesgo inherente											
REFERENCIA	**Tipo de activo**	**Nombre del activo**	**Riesgo**	**Amenaza**	**Vulnerabilidades (causas)**	**Descripción del riesgo**	**categoría del riesgo**	**Frecuencia de la actividad que origina el riesgo (# de horas en el año)**	**Unidad de medida de la actividad de origina el riesgo**	**Afectación**	**Criterios de impacto** a) Económico: SMLMV b) Reputacional: El riesgo afecta la imagen de...
1	Información	Expedientes de convenios	pérdida de disponibilidad	extravió de convenios	• No existe la serie documental CONVENIOS • Cada profesor cuenta con la autonomía de suscribir convenios y no se cuenta con unos tipos documentales específicos mínimos para convenios del área misional obligatorios para la suscripción de este	Las vulnerabilidades de la columna anterior pueden facilitar extravío de convenios generando pérdida de disponibilidad de expedientes de convenios	Ejecución y administración de procesos	50	Número de veces que se prestan los convenios	Reputacional	La entidad con algunos usuarios de relevancia frente al logro de los objetivos

31	Software	Diccionario Sáliba	Pérdida de integridad	manipulación intencional o accidental de la información	El aplicativo no cuenta con ambiente de pruebas, por lo que se debe trabajar directamente en producción	Las vulnerabilidades anteriores pueden facilitar manipulación intencional o accidental de la información generando pérdida de integridad de DICCIONARIO SÁLIBA	Ejecución y administración de procesos	9000	Número de horas de servicio	Económica	Entre 100 y 500 SMLMV

Tabla 2. identificación y análisis del riesgo inherente

Nota: 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

C. Valoración de riesgos inherentes de seguridad digital

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE), para la realización de esta valoración debe tenerse en cuenta:

- 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:

Actividad	Frecuencia de la 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.	Diaria	Muy alta

Tabla 3. Criterios de actividad

Frecuencia de la Actividad (veces por año)		PROBABILIDAD		
La actividad que conlleva el riesgo se ejecuta…		Cuantitativa		Cualitativa
Mínimo	Máximo	Mínimo	Máximo	
0	2	**0,00%**	**20,00%**	**Muy Baja**
3	24	**20,01%**	**40,00%**	**Baja**
25	500	**40,01%**	**60,00%**	**Media**
501	5.000	**60,01%**	**80,00%**	**Alta**
5.001	10.000	**80,01%**	**100,00%**	**Muy Alta**

Tabla 4. Frecuencia de la actividad

- 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.

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**

Tabla 5. Criterios de riesgo.

Estimar el nivel de riesgo inicial – 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:

Matriz de Calor Inherente General

Probabilidad					
Muy Alta 100%					
Alta 80%					
Media 60%					
Baja 40%					
Muy Baja 20%					
	Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%
	Impacto				

Donde el nivel de severidad es

Extremo
Alto
Moderado
Bajo

Grafica 1. Matriz de Calor Inherente General

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

D. Identificación y evaluación de controles

- Una vez establecidos y valorados los riesgos inherentes se deben identificar los controles existentes para evitar trabajo o costos innecesarios, la valoración de controles la ejerce la Unidad de control interno.

IMPORTANTE

* Para cada causa debe existir un control.
* Las causas se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón).
* Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

3. Diseño, análisis y evaluación de controles							
3.1 Descriptores del control				3.2 Atributos de eficiencia			
# de control	Responsable de ejecutar el control	Acción	Complemento	Momento de ejecución	Forma de ejecución	Calificación	Efecto
1	Coordinadora grupo alianzas	revisar la completitud y exactitud de la información de los convenios que ha firmado el instituto	se está revisando cada una de las carpetas y se organizan por vigencia, recursos y procedencia (nacional e internacional)	preventivo	Manual	50%	Probabilidad
2	Coordinadora grupo alianzas	centralizar y revisar los requisitos para la suscripción de los convenios	Mediante el memorando firmado por la decana y por el subdirector académico	preventivo	Manual	70%	Probabilidad

3.3 Eficiencia del control		3.4 Atributos informativos		
Eficiencia en probabilidad	Eficiencia en impacto	Documentación	Frecuencia	Evidencia
30%	21%	Documentado	Aleatoria	Con registro

Tabla 6. Diseño, análisis y evaluación de controles.

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 (después de los controles), debe tenerse en cuenta el manual "administración del riesgo" establecido en el Instituto Caro y Cuervo.

- **Estimar el nivel de riesgo residual:** es el resultado de aplicar la efectividad de los controles al riesgo inherente y se mide a través de la siguiente tabla:

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

Grafica 2. Matriz de Calor Residual General.

Resultados del riesgo residual:

4. Evaluación del riesgo residual										
Reducción probabilidad	**%**	**Reducción impacto**	**%**	**Reducción severidad**	**Probabilidad residual**	**Pr %**	**Impacto residual**	**Ir%**	**Nivel de severidad residual**	**Posición severidad**
Baja	30%	Moderado	60%	Moderado	Baja	30%	Menor	39%	Moderado	5
Media	48%	Moderado	45%	Moderado	Media	48%	Menor	29,3%	Moderado	6

Tabla 7. Evaluación del riesgo residual

Tratamiento de riesgos de seguridad digital

Una vez se han identificado los riesgos residuales, se debe reportar en el mapa y planes de tratamiento. El oficial de seguridad digital apoyará y acompañará a las diferentes líneas de defensa tanto para el reporte como para la gestión y el tratamiento de estos riesgos.

Plan de tratamiento de riesgos de seguridad digital				
5.1 Estrategias		5.2 Plan de reducción		
Vulnerabilidades	Tratamiento	Actividad	Responsable	Fecha final
No existe la serie documental CONVENIOS	Reducir (mitigar)	Validar en el Instituto cual es el área responsable de la custodia de los CONVENIOS.	Coordinadora de alianzas	31/12/2021
Cada profesor cuenta con la autonomía de suscribir convenios y no se cuenta con unos tipos documentales específicos mínimos para convenios.	Reducir (mitigar)	*Realizar el acompañamiento a la supervisión del convenio	Coordinadora de alianzas	31/12/2021
El aplicativo no cuenta con ambiente de pruebas, por lo que se debe trabajar directamente en producción	Reducir (mitigar)	*Solicitar al grupo TIC un ambiente de pruebas para el sistema	Coordinador de Investigación	31/12/2021

Tabla 8. Plan de tratamiento de riesgos de seguridad digital

El plan de tratamiento general será presentado y socializado a la dirección general para definir y priorizar los activos que deban tratados inmediatamente sobre los cuales se deba realizar una asignación de recursos adicionales para la implementación de controles, esto no quiere decir que no se deben gestionar los demás riesgos.

Monitoreo y revisión

Esta actividad estará a cargo de la primera línea de defensa y será apoyada por el oficial de seguridad del Instituto Caro y Cuervo, para ello se definen dos indicadores para el seguimiento del plan de tratamiento de riesgos:

- **EFICACIA:** Índice de cumplimiento actividades = (# de actividades cumplidas / # de actividades programadas) x 100
- **EFECTIVIDAD:** Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)

6. Monitoreo de la administración del riesgo					
6.1 Monitoreo del plan de reducción				6.2 Monitoreo del control	
Fecha de Monitoreo	**Evidencia de implementación de la actividad**	**Estado de la actividad**	**Observaciones sobre el plan**	**Evidencia de ejecución del control**	**Observaciones sobre el control**
14/03/2022	Serie documental convenios suscrito con gestión documental	Finalizada	Se realizó la entrega al área competente	FUID y TRD	Eficiente
15/04/2022	Convenios acordes a lineamientos del instituto	Vencida	Se realizó el 50% del trabajo a la fecha	Convenios firmados	Se requiere más recursos
17/07/2022	No existe	Vencida	No hay recursos	Correos de solicitud	Se debe adquirir más almacenamiento

Tabla 9. Monitoreo de la administración del riesgo