




## CONTENIDO

INTRODUCCIÓN.....	3
<b>1. OBJETIVOS .....</b>	<b>5</b>
<b>2. ALCANCE .....</b>	<b>5</b>
<b>3. ESQUEMA DE ASIGNACIÓN DE RESPONSABILIDADES (Roles y Responsabilidades).....</b>	<b>6</b>
3.1 LÍNEA ESTRATÉGICA: .....	6
3.1.1. El Director y la alta dirección:.....	6
3.1.2 Comité Institucional de Coordinación de Control Interno. CICCI.....	6
3.1.3 Comité Institucional de Gestión y Desempeño – CIGD.....	7
3.2 PRIMERA LÍNEA DE DEFENSA – Director, líderes de proceso y sus equipos de trabajo .....	7
3.3 SEGUNDA LÍNEA DE DEFENSA .....	8
3.4 TERCERA LÍNEA DE DEFENSA- Oficina de Control Interno.....	9
<b>4. METODOLOGÍA GENERAL PARA LA ADMINISTRACION DE LOS RIESGOS DE CORRUPCION, GESTION Y SEGURIDAD DIGITAL.....</b>	<b>11</b>
4.1 Identificación de Riesgos .....	11
4.2 Valoración de Riesgos .....	12
4.2.1 Controles .....	12
4.3 Tratamiento obligatorio a los riesgos .....	17
4.4 Estrategia para combatir el riesgo .....	17
<b>5. MONITOREO Y SEGUIMIENTO A LA GESTIÓN DE LOS RIESGOS Y ACCIONES DE NTRATAMIENTO .....</b>	<b>19</b>
<b>6. HERRAMIENTA PARA LA GESTIÓN DEL RIESGO .....</b>	<b>21</b>
<b>7. GENERALIDADES ACERCA DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL .....</b>	<b>22</b>
<b>8. DESARROLLO METODOLÓGICO PARA LA FASE DE IDENTIFICACIÓN Y VALORACIÓN DE LOS RIEGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL .....</b>	<b>24</b>
8.1 RIESGOS DE GESTIÓN .....	24
8.1.1 Metodología para la Administración de los Riesgos de Gestión.....	24
8.1.1.1 Análisis de objetivos estratégicos y de procesos .....	24



8.1.1.2	Identificación de los puntos de riesgo o actividades claves de éxito del proceso. ....	25
8.1.1.3	Identificación del impacto.....	25
8.1.1.4	Descripción del riesgo .....	27
8.1.1.5	Identificación de factores de riesgo.....	28
8.1.1.6	Valoración del Riesgo de Gestión.....	29
8.1.1.7	Valoración de controles.....	31
<b>8.2</b>	<b>RIESGOS DE CORRUPCION.....</b>	<b>37</b>
8.2.1	METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE CORRUPCIÓN....	37
8.2.1.2	Lineamientos sobre los riesgos relacionados con posibles actos de corrupción.....	37
8.2.2	Definición de Riesgo de Corrupción: .....	38
8.2.3	Identificación de Riesgo de Corrupción: .....	39
8.2.4	Valoración de Riesgos de Corrupción.....	40
8.2.6	Seguimiento de riesgos de corrupción - OFICINA DE CONTROL INTERNO .....	46
8.2.7	Herramienta para la gestión de los riesgos de corrupción:.....	47
<b>8.3</b>	<b>RIESGOS DE SEGURIDAD DIGITAL.....</b>	<b>49</b>
8.3.1	METODOLOGIA PARA LA ADMINISTRACION DE RIEGOS DE GESTION DIGITAL ..	49
8.3.2	Identificación del riesgo de seguridad digital:.....	51
8.3.3	Valoración del Riesgo .....	55
8.3.3.1	Determina la Probabilidad.....	55
8.3.3.2	Determinar el impacto.....	56
8.3.3	Determinar el nivel de severidad en el mapa de calor.....	59
8.3.4	Controles asociados a la seguridad de la información .....	60
<b>9.</b>	<b>DEFINICIONES.....</b>	<b>63</b>

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

## INTRODUCCIÓN

La administración del riesgo en el INDERHUILA, mediante el desarrollo y aplicación de la metodología para la administración del riesgo, establece los lineamientos para la identificación, valoración y seguimiento a los riesgos de gestión, corrupción y seguridad digital, entendidos como el efecto que se causa sobre los objetivos estratégicos o de procesos, debido a eventos potenciales que pueden llevar a la entidad a la posibilidad de incurrir en pérdidas o afectaciones a nivel económico o reputacional por deficiencias, fallas o inadecuaciones, en el recurso humano, procesos, tecnología, infraestructura o por la ocurrencia de acontecimientos externos, fraudes internos o externos.

El INDERHUILA, está comprometido con la política de operación para la administración de riesgos que pudieran afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos, planes institucionales, la satisfacción de los usuarios y el manejo transparente de los recursos públicos, a partir de la elaboración y adopción de la presente política de operación y la herramienta de trabajo, documentos técnicos que facilitan la buena “Gestión y Administración de los riesgos de gestión, corrupción y seguridad digital”, a través de los cuales se establecieron los lineamientos para la identificación, valoración, diseño y ejecución de controles, tratamiento y seguimiento de dichos riesgos, tomando como referentes las directrices establecidas por el Departamento Administrativo de la Función Pública -DAFP y del Modelo Integrado de Planeación y Gestión - MIPG, conforme a la política de “Direccionamiento estratégico y planeación”, de “Definir la política de administración de riesgos, identificar y valorar riesgos (gestión, corrupción y seguridad digital), de acuerdo con la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno - MECI, la Guía para la Administración del riesgo del DAFP, el Modelo de Seguridad y Privacidad de la información de la estrategia de Gobierno Digital y la Secretaría de Transparencia de la Presidencia de la República desde su estrategia Plan Anticorrupción y de Atención al Ciudadano.

**EI INDERHUILA**, actualizará anualmente sus mapas de Riesgos de gestión, corrupción y seguridad digital, con el fin de ajustar controles y mitigar los riesgos en el marco de la viabilidad jurídica, técnica, financiera y económica. Los responsables de cada proceso, junto con sus equipos de trabajo, serán quienes adelanten la ejecución de los controles y las acciones preventivas y realicen el seguimiento a su cumplimiento como primera línea de defensa y mecanismo de autocontrol, conforme lo establece el Esquema de asignación de responsabilidades establecido.


*Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila*



Estos lineamientos, deben ser acatados por todos los servidores públicos y contratistas de la entidad en el desarrollo de sus funciones, compromisos y obligaciones, buscando que éstos conduzcan a disminuir la vulnerabilidad frente a las diferentes situaciones que puedan interferir en el logro de la misionalidad y objetivos institucionales y preparar la respuesta oportuna a amenazas externas que puedan generar eventos de riesgo, para lo cual se establecen las siguientes etapas:

1. Objetivos
2. Alcance
3. Esquema de asignación de responsabilidades
4. Metodología General para la administración de los riesgos de corrupción, gestión y seguridad digital.
5. Monitoreo y seguimiento a la Gestión de los Riesgos y acciones de tratamiento.
6. Herramienta para la Gestión del Riesgo.
7. Generalidades acerca de los Riesgos de Gestión, Corrupción y Seguridad Digital.
8. Desarrollo Metodológico para la fase de identificación y valoración de los Riesgos de Gestión, Corrupción y Seguridad Digital.

HUILA  
CRECE

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

## 1. OBJETIVOS

Los objetivos establecidos en la gestión integral del riesgo involucran de forma específica, los aspectos relacionados con el funcionamiento institucional, definiéndolos de la siguiente manera:


- Identificar los riesgos asociados a la implementación y ejecución de los “procesos”, “procedimientos” y “actividades” críticas o complejas que no permitan alcanzar los objetivos institucionales.
- Identificar las causas y situaciones expresas asociadas al riesgo de corrupción, su valoración y tratamiento, a partir de la implementación de las directrices emitidas por la Secretaría de Transparencia de la Presidencia de la República, mediante el documento “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano”.
- Identificar los riesgos asociados a la implementación de un Sistema de Gestión de Seguridad de la Información, al igual que la identificación y valoración de “Activos de Información”.

## 2. ALCANCE.

La Política de Operación para la Administración de Riesgos es aplicable a todos los procesos del modelo de operación por procesos, a los planes institucionales, a los programas, a los proyectos y a las acciones ejecutadas por los servidores públicos y contratistas de prestación de servicios del INDERHUILA, durante el ejercicio de sus funciones y obligaciones, respectivamente.

Incluye lineamientos para el tratamiento, manejo y seguimiento a los riesgos de:

- Riesgos de *gestión*
- *Riesgos de corrupción*
- *Riesgos del Sistema de Gestión de la Información – Seguridad de Información (SGSI)*, en todos los procesos del INDERHUILA.

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

### 3. ESQUEMA DE ASIGNACIÓN DE RESPONSABILIDADES (Roles y Responsabilidades)

Gráfico 19. Interacción de las Líneas de Defensa en el Modelo Estándar de Control Interno



Gráfica. Función Pública

#### 3.1 LÍNEA ESTRATÉGICA:


##### 3.1.1. El Director y la alta dirección:

Definirán los lineamientos para la administración del riesgo de la entidad; el equipo directivo determinará el apetito, tolerancia y capacidad de los riesgos, identificará aquellos riesgos que impidan el logro de su propósito fundamental y las metas estratégicas.

##### 3.1.2 Comité Institucional de Coordinación de Control Interno. CICC.

Analizará los cambios en el entorno (contexto interno y externo), que puedan tener un impacto significativo en la operación de la entidad y generen cambios en la estructura de riesgos y controles. Para ello, durante la formulación del Plan Estratégico Institucional (o antes, cuando las circunstancias lo ameriten) la Oficina de Planeación o quien haga sus veces, coordinará la revisión de la Plataforma Estratégica y la elaboración del Diagnóstico de Capacidades y del Entorno bajo la metodología DOFA, con el fin de documentar el



 <b>INDERHUILA</b>	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

contexto general de la entidad y asesorar a la línea estratégica en la decisión y/o actualización de la Política Institucional de Administración del Riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.


### 3.1.3 Comité Institucional de Gestión y Desempeño – CIGD.

- Asegurará la permeabilización en todos los niveles de la organización pública de la presente política institucional, de tal forma que cada una de las tres líneas de defensa conozcan claramente los niveles de responsabilidad y autoridad que posee frente a la gestión del riesgo.
- Evaluará y dará línea sobre la administración de los riesgos en la Entidad.
- Aprobará el Mapa de riesgos de corrupción que hace parte del Plan Anticorrupción y de Atención al Ciudadano y las actualizaciones del mismo.
- Analizará gestión del riesgo y aplicará mejoras.

### 3.2 PRIMERA LÍNEA DE DEFENSA – Director, líderes de proceso y sus equipos de trabajo

- Liderar la identificación de los riesgos del proceso a cargo, acorde a los lineamientos establecidos por la metodología. Guía para la administración del riesgo Versión 5.0 Identificarán y valorarán los riesgos, que pueden afectar los procesos a su cargo y los actualizarán cuando se requiera, bajo la metodología vigente, informando de la novedad a la Oficina Asesora de Planeación o quien haga sus veces.
- Definirán, diseñarán, aplicarán y realizarán seguimiento a los controles para mitigar los riesgos y propondrán mejoras a la gestión del riesgo en su proceso.
- Supervisarán la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectando las deficiencias de los controles y determinando las acciones de mejora a que haya lugar.
- Revisarán el cumplimiento de los objetivos de sus procesos e identificarán en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.

*Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa*  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila

 <b>INDERHUILA</b>	<b>POLITICA</b>	<b>CODIGO</b>	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	<b>VERSIÓN</b>	01
		<b>VIGENCIA</b>	OCTUBRE 2020

- Revisará y realizará seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.
- Revisarán los planes de acción o de contingencia establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.

### **3.3 SEGUNDA LÍNEA DE DEFENSA**


La Oficina de Planeación o quien haga sus veces, pertenece a la segunda línea de defensa, no obstante, esto no quiere decir que sea la única que pertenezca a dicha línea, ya que todos los líderes de proceso tienen la responsabilidad de realizar seguimiento a los Riesgos, sin embargo, establece el control, de los Riesgos de Corrupción.

Revisará los cambios en el Direccionamiento Estratégico o en el entorno y cómo éstos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de apoyar a sus líderes de proceso en la actualización del mapa de riesgos.

La Oficina de Planeación o quien haga sus veces se encargará de asistir y guiar a la línea estratégica y la primera línea de defensa en la gestión adecuada de los Riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos (a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos) y monitoreará la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo de la siguiente forma:

- Diseñará y pondrá en marcha mecanismos para que los funcionarios, contratistas de prestación de servicios, la ciudadanía y los interesados externos (Interventores, Contratistas de obra, entre otros) conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del Mapa de Riesgos de Corrupción.
- Consolidará el Mapa de riesgos de Corrupción y lo presentará para revisión y aprobación del Comité Institucional de Gestión y Desempeño. Una vez sea aprobado,




	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

lo publicará en la página web de la entidad, como anexo al Plan Anticorrupción y de Atención al Ciudadano, a más tardar el 31 de enero de cada vigencia.


- Consolidará el Mapa de riesgos institucional y lo presentará para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno.
- Supervisará en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, evalúe y gestione los riesgos y controles para que se generen acciones de mejora continua.
- Evaluará que los riesgos sean consistentes con la presente política y que sean monitoreados por la primera línea de defensa.
- Identificará cambios en el apetito del riesgo en la Entidad, especialmente en aquellos riesgos ubicados en zona baja y los presentará para aprobación del Comité Institucional de Coordinación de Control Interno.
- Asegurará que los controles y procesos de gestión del riesgo de la 1ª línea de Defensa sean apropiados y funcionen correctamente (supervisión de la implementación de prácticas de gestión de riesgo eficaces).

### **3.4 TERCERA LÍNEA DE DEFENSA- Oficina de Control Interno**

- Proporcionará un aseguramiento, a través de la auditoría interna, sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno (SCI), para lo cual:

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

- Identificará y evaluará cambios que podrían tener un impacto significativo en el Sistema de Control Interno (SCI) y/o evaluación de los riesgos, durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna y lo reportará al Comité de Coordinación del Sistema de Control Interno.
- Revisará la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad.
- Alertará a la línea estratégica sobre la probabilidad de riesgo de corrupción en las áreas auditadas.
- Asesorará de forma coordinada con la Oficina de Planeación o quien haga sus veces, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles.
- Recomendará mejoras a la política de administración del riesgo.
- Revisará la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad.
- Adelantará seguimiento a la gestión de riesgos de corrupción, verificando la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad y la efectividad de los controles y publicará los resultados en la página web de la Entidad dentro de los diez (10) primeros días de los meses de mayo (con corte a 30 de abril), septiembre (corte 31 de agosto) y enero (corte 31 de diciembre).
- Proporcionará un aseguramiento objetivo e independiente sobre la eficacia de gobierno, gestión de riesgos y control interno a la Alta Dirección de la entidad, incluidas las maneras en que funciona la primera y segunda línea de defensa.

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

#### 4. METODOLOGÍA GENERAL PARA LA ADMINISTRACION DE LOS RIESGOS DE CORRUPCION, GESTION Y SEGURIDAD DIGITAL.

La metodología aplicada para la administración del riesgo será la contemplada en:

“Guía para la administración del riesgo y el diseño de controles en entidades públicas”, versión 4 de octubre de 2019, expedida por La Vicepresidencia, Función Pública y Min-Tic, para los riesgos de corrupción y Seguridad Digital.

“Guía para la administración del Riesgo y el Diseño de Controles en Entidades Públicas”, versión 5 de diciembre de 2020, expedida por El Departamento Administrativo de la Función Pública, para los riesgos de Gestión.

El paso a paso para la identificación y valoración de los riesgos variará teniendo en cuenta las particularidades de los riesgos de gestión, corrupción y seguridad digital.


##### 4.1 Identificación de Riesgos

Esta etapa tiene como objetivo identificar los riesgos que estén o no bajo el control de la entidad, teniendo en cuenta el contexto estratégico en el que éste opera, la caracterización de cada proceso que contempla su objetivo y alcance, y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

La entidad debe analizar los objetivos estratégicos y de procesos e identificar los posibles riesgos que afectan su cumplimiento y que pueden ocasionar el éxito o fracaso, para ello, es necesario revisar que estos objetivos se encuentren alineados con la Misión y la Visión Institucional y asegurar que los objetivos de procesos contribuyan a los objetivos estratégicos, así como, analizar su adecuada formulación (para formular objetivos es importante cumplir características de SMART: Sencillos y específicos, Medibles, Ambicioso pero alcanzables, Relevante y Tiempo), así:

- Específico (que esté bien definido y que apunte a lo que se pretende lograr con las salidas de ese proceso).
- Medible (que se puede parametrizar para medirlo de forma cuantitativa o cualitativa).
- Realista (que es ambicioso pero alcanzable, no una ilusión).
- Relevante (que esté alineado con el propósito institucional).

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila

 <b>INDERHUILA</b>	<b>POLITICA</b>	<b>CODIGO</b>	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	<b>VERSIÓN</b>	01
		<b>VIGENCIA</b>	OCTUBRE 2020

Para el Inderhuila se identificarán los riesgos a los objetivos estratégicos y a todos los procesos de la entidad, como mínimo un riesgo por proceso u objetivo con el respectivo análisis e identificación de los factores generadores de riesgos y el impacto o consecuencia en caso de materialización del mismo, según sea; Riesgo de Gestión, Riesgo de Corrupción o Riesgo de seguridad digital.

## **4.2 Valoración de Riesgos**

Esta etapa tiene como objetivo establecer la probabilidad de ocurrencia del riesgo, es decir la exposición que tiene la entidad frente al riesgo y el impacto o consecuencias que se pueden generar, con el fin de determinar la zona de severidad del riesgo inherente, así mismo se diseñarán y analizarán la efectividad de los controles existentes, a fin de determinar, la probabilidad de ocurrencia, estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año, es decir, el número de veces que se ejecuta la acción.


Lo anterior, permite determinar con total claridad la frecuencia con la cual se lleva a cabo una actividad y no los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión de la entidad.

Para todos los riesgos identificados se debe realizar el análisis de probabilidad e impacto para determinar el nivel de severidad del riesgo inherente, a través de la combinación de probabilidad e impacto en el mapa de calor establecido.

### **4.2.1 Controles**

Un control se define como la medida que permite reducir o mitigar el riesgo, por lo tanto, es necesario identificar controles a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto. Adicional los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

La estructura para descripción de un control como mínimo debe llevar lo siguiente:

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

- **Acción de control:** Se determina mediante verbos en los cuales se identifica la acción a realizar como parte del control.  
*Ej. Verificar, comparar, concatenar, chequear, conciliar, etc.*
- **Complemento:** Corresponde a los detalles que permiten identificar claramente el objeto del control.
- **Responsable de ejecutar el control:** Identifica el cargo del servidor que ejecuta el control, en caso de ser controles automáticos se identificará el sistema que realiza la actividad.


De igual manera, se tendrá una tipología de controles a través del ciclo de procesos que permitirá saber cuándo se debe activar el control. Los controles pueden ser preventivos, detectivos o correctivos

- **Control preventivo:** Acción y/o mecanismo ejecutado antes que se realice la actividad Originadora del riesgo, se busca establecer condiciones que aseguren el resultado final esperado. En general estos controles actúan sobre las causas del riesgo.
- **Control detectivo:** Acción y/o mecanismo ejecutado que permite detectar el riesgo durante la ejecución del proceso y puede disminuir la materialización de dicho riesgo.  
Estos controles detectan el riesgo, pero genera reprocesos.
- **Control correctivo:** Acción que se ejecutan después de que se materializa el riesgo y en la mayoría de las ocasiones permiten reducir el impacto de dicho riesgo.

Así mismo, de acuerdo a la forma como se ejecutan se tiene:

**Control manual:** Controles que son ejecutados por una persona.

**Control automático:** Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.

	POLITICA		CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>		VERSIÓN	01
			VIGENCIA	OCTUBRE 2020

El INDERHUILA define los controles teniendo en cuenta la estructura para su descripción, la tipología y la manera como se implementa, se debe tener en cuenta que los controles de tipo preventivo y detectivo mitigan la probabilidad de ocurrencia y los controles correctivos el impacto del riesgo, por lo tanto, es necesario revisar qué tipo de controles se deben definir para mitigar los riesgos identificados en la entidad.

Es de aclarar, que según el tipo de control (preventivo, detectivo o correctivo) y su implementación (automático o manual) tienen un peso porcentual que se debe determinar para realizar la correspondiente valoración del riesgo inherente y servirá para realizar el respectivo desplazamiento en el mapa de calor y conocer el riesgo residual.

Criterios para el diseño del control, es de aclarar que mínimo se debe garantizar la tipología y la implementación del control para conocer la eficiencia de este y los otros atributos se determinan bajo el criterio del líder del proceso de manera informativa.

Características		Descripción	
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, Aseguran el resultado
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles Preventivos. Se pueden genera reprocesos.
		Correctivo	Dado que permiten reducir el impacto de la caracterización del riesgo, tienen un costo en su Implementación.
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.
Atributos de Formalización	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales procedimientos, flujogramas o cualquier otro documento propio del proceso.

Gráfica. Función Pública

El peso porcentual de los atributos de los controles, dependen del tipo de riesgo.





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, lo cual llevará a determinar el riesgo inherente una vez aplicados los controles y establecido su nivel de efectividad.

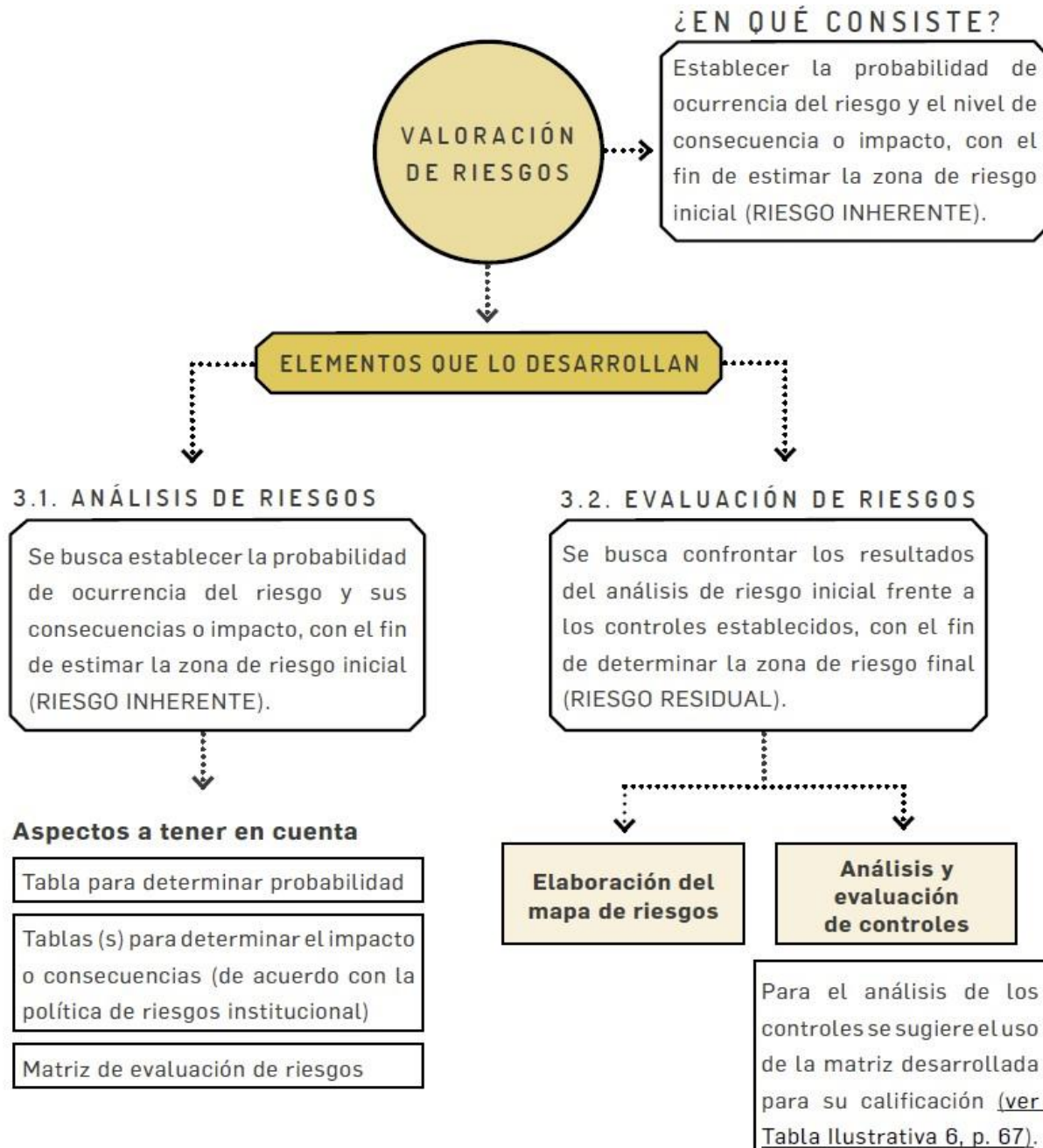
De acuerdo con lo anterior, el resultado de aplicar la efectividad de los controles al riesgo inherente determina el riesgo residual, así:




Gráfica Función Pública

Dependiendo del nivel de severidad en que se ubique el riesgo residual, el INDERHUILA priorizará la atención en aquellos riesgos residuales que todavía se encuentren en un nivel de severidad moderado, alto y extremo y se define su tratamiento y posibles acciones a seguir.

### Resumen de la valoración de riesgos



Gráfica. Función Pública

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

### 4.3 Tratamiento obligatorio a los riesgos


El tratamiento a un determinado nivel de riesgo se analiza frente al riesgo residual, sin embargo, para procesos nuevos se realizará sobre el riesgo inherente.

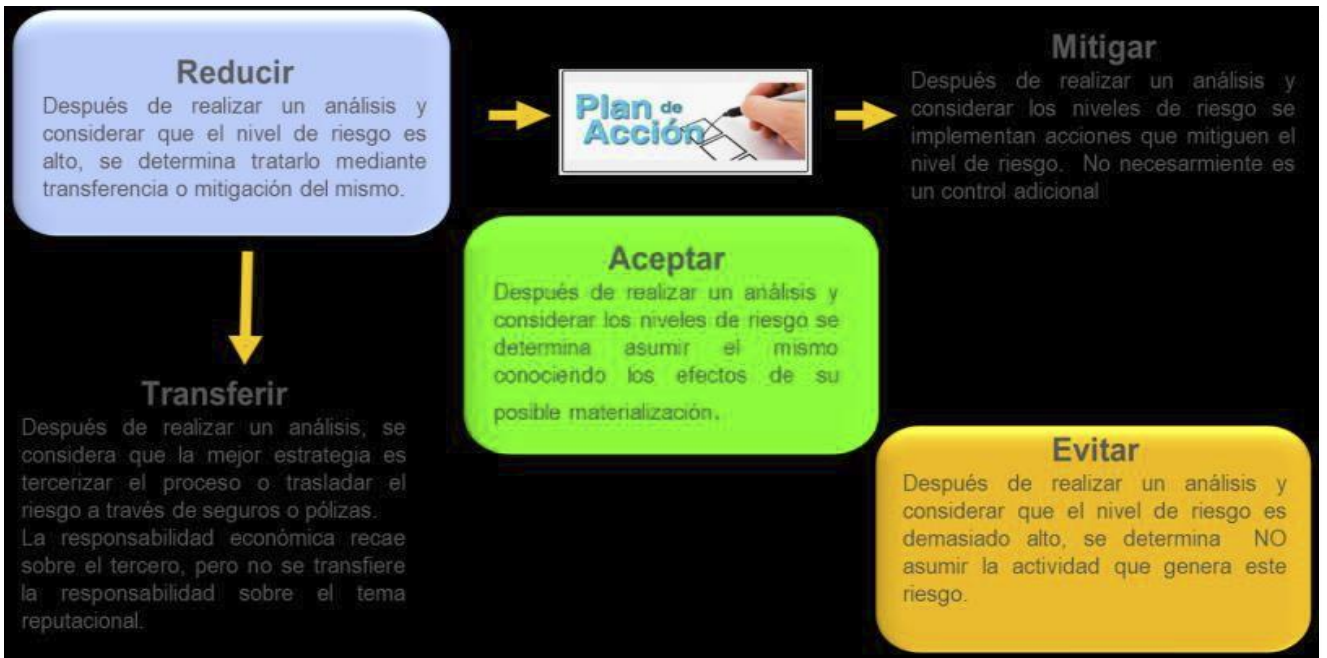
Zona Severidad	Estrategia de tratamiento / Periodicidad de Seguimiento
<b>BAJO</b>	<p><b>ACEPTAR</b> el riesgo y se determina <b>ASUMIR</b> el mismo conociendo los efectos de su posible materialización. El seguimiento a sus controles es <b>SEMESTRAL</b> a través de la Oficina de Control Interno de Gestión.</p> <p><b>NO APLICA PARA LOS RIESGOS DE CORRUPCIÓN.</b></p> <p><b>NOTA:</b> NINGÚN riesgo de corrupción podrá ser ACEPTADO. En razón a que estos riesgos no pueden ubicarse en los niveles de impacto INSIGNIFICANTE y MENOR</p>
<b>MODERADO</b>	<p><b>REDUCIR</b> el riesgo y se determina <b>MITIGAR</b> a través de un plan de acción y el seguimiento es de manera <b>TRIMESTRAL</b> a través de la Oficina de Control Interno de Gestión</p>
<b>ALTO</b>	<p><b>REDUCIR</b> el riesgo y se determina <b>MITIGAR</b> a través de un plan de acción y el seguimiento es de manera <b>BIMENSUAL</b> a través de la Oficina de Control Interno de Gestión</p>
<b>EXTREMO</b>	<p><b>REDUCIR</b> el riesgo y se determina <b>MITIGAR</b> a través de un plan de acción y el seguimiento es de manera <b>MENSUAL</b> a través de la Oficina de Control Interno de Gestión</p>

Para los casos que requiere establecer un plan de acción para reducir o mitigar al máximo el nivel de riesgos no controlados es necesario que el líder del proceso determine las actividades, responsables, fechas de implementación y seguimiento, conforme al plan de tratamiento establecido.

### 4.4 Estrategia para combatir el riesgo

De acuerdo con la valoración de cada riesgo residual y su ubicación en la zona de riesgo (extremo, alto, moderado, bajo) se establece su opción de manejo. Esto se define a partir del nivel del riesgo residual (con controles), de la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020



Gráfica. Función Pública


Para los casos que requiere establecer un plan de acción para reducir o mitigar al máximo el nivel de riesgos no controlados es necesario que el líder del proceso determine las actividades, responsables, fechas de implementación y seguimiento, conforme al plan de tratamiento establecido.

Decisión que se toma frente a un determinado nivel de riesgo, pueden ser, aceptar, reducir y evitar. Se analiza frente al Riesgo Residual, esto para proceso en funcionamiento, cuando se trate de procesos nuevos se procede a partir del riesgo inherente.

Dependiendo del valor del riesgo residual, este se puede:

- **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.

Fuente Función Pública

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

Frente al plan de acción referido para la opción de reducir, es importante mencionar que conceptualmente y de manera general se trata de herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos cuando se define la opción de reducir, se requerirá la definición de un plan de acción que requerirá: i) responsable, ii) fecha de implementación y iii) fecha de seguimiento.

## 5. MONITOREO Y SEGUIMIENTO A LA GESTIÓN DE LOS RIESGOS Y ACCIONES DE TRATAMIENTO

- Los riesgos operativos se revisan y validan cada vez que el líder y dueño de proceso lo considere necesario y como mínimo 1 vez al año, atendiendo la metodología vigente, según sea el tipo de riesgo.
- La periodicidad de seguimiento a los controles y plan de acción de cada riesgo está definida de acuerdo a la zona de severidad donde se encuentre cada riesgo y su tratamiento establecido en la tabla correspondiente.
- El líder o delegado de riesgos en cada proceso analiza los resultados del seguimiento y pueden determinar establecer un plan de mejoramiento ante cualquier desviación y socializa al interior de su dependencia las acciones a seguir, solicitando de ser necesario el apoyo a la segunda línea de defensa según corresponda, así:
  - Riesgos de Gestión, Acompaña y apoya el líder de MIPG y Calidad.
  - Riesgos de Corrupción, Acompaña y apoya el líder de Planeación o quien haga sus veces.
  - Riesgos de Seguridad digital, Acompaña y apoya el líder de TIC.

Zona Severidad	Periodicidad de Seguimiento a los riesgos
<b>BAJO</b> (N.A. para riesgos de corrupción)	El seguimiento a sus controles es <b>SEMESTRAL</b> a través de la Oficina de Control Interno de Gestión.
<b>MODERADO</b>	El seguimiento es de manera <b>TRIMESTRAL</b> a través de la Oficina de Control Interno de Gestión
<b>ALTO</b>	El seguimiento es de manera <b>MESUAL</b> a través de la Oficina de Control Interno de Gestión
<b>EXTREMO</b>	El seguimiento es de manera <b>MENSUAL</b> a través de la Oficina de Control Interno de Gestión

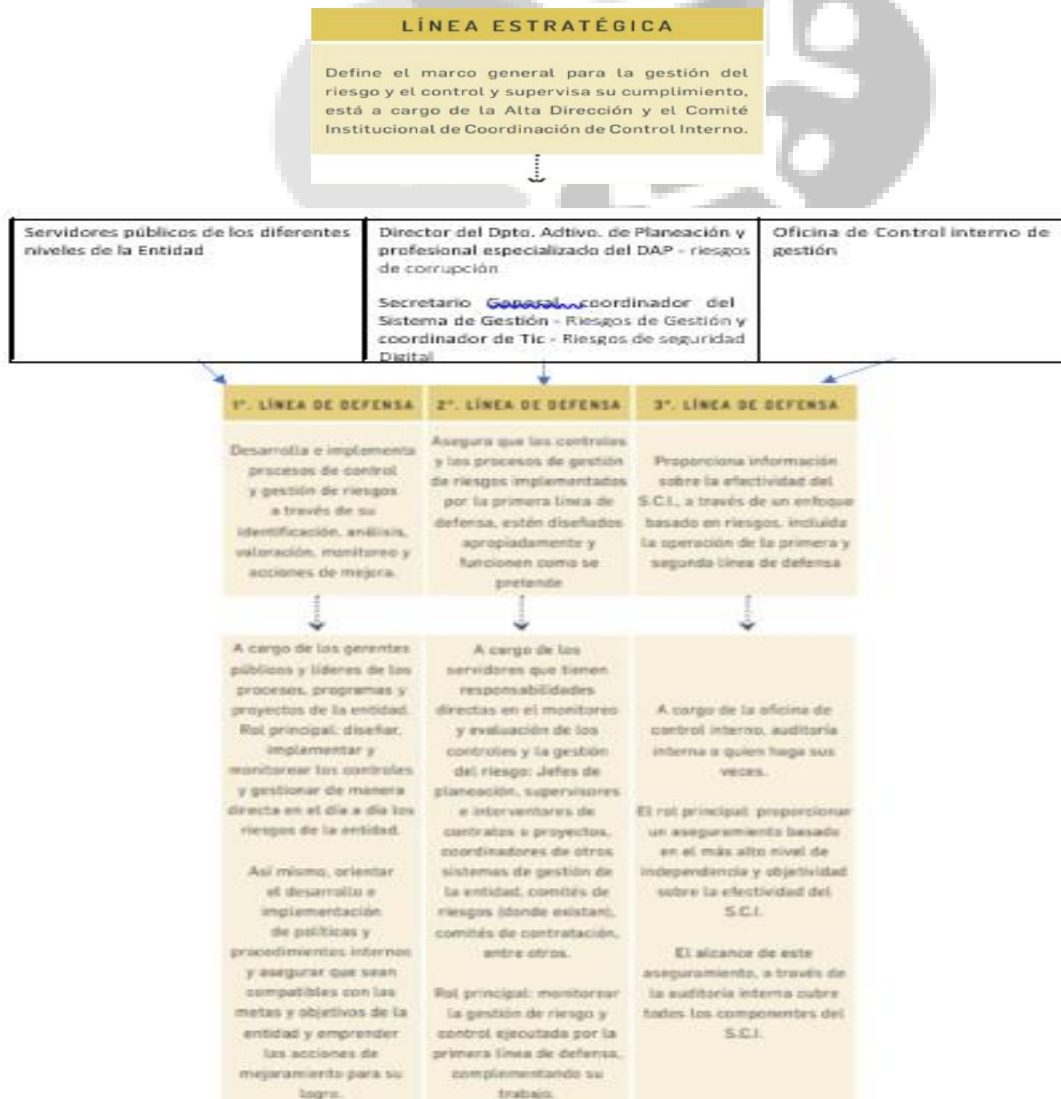
Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila






Para identificar la responsabilidad de la gestión del riesgo y control que está distribuida en diversos servidores y dependencias de la entidad, conforme a la Línea estratégica y 3 líneas de defensa, en coherencia con el ítems “**3 ESQUEMA DE ASIGNACIÓN DE RESPONSABILIDADES**” de este documento, tal como se muestra en la figura siguiente;

**Alta dirección y (Comité institucional de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno)**



Gráfica. Función Pública




	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

## 6. HERRAMIENTA PARA LA GESTIÓN DEL RIESGO

El INDERHUILA determina que el mapa de riesgos es la herramienta establecida para la identificación, valoración, tratamiento y seguimiento a los riesgos, para lo cual tendrá en cuenta conforme a los roles definidos para las 3 líneas de defensa, que:


La oficina de Planeación o quien haga sus veces	Asesora y socializa la metodología descrita para los Riesgos de Corrupción
La líder de MIPG y la líder de Gestión de la calidad	Asesora y socializa la metodología descrita para los Riesgos de Gestión
El líder de las TIC	Asesora y socializa la metodología descrita para los Riesgos de Seguridad Digital
La Oficina de Control interno de Gestión (tercer línea de defensa).	Realiza seguimiento al cumplimiento de los lineamientos establecidos en esta política y revisa la eficacia y efectividad de los controles y las acciones de tratamiento de los 3 tipos de riesgos, de acuerdo a la periodicidad definida para el nivel de severidad de dichos riesgos de gestión, corrupción y seguridad digital (ver ítems 4.3 las frecuencias de seguimiento para el tratamiento: semestral, trimestral y mensual respectivamente).

HUILA  
CRECE

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

## 7. GENERALIDADES ACERCA DE LOS RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL

- Elaboración y/o revisión anual por parte de cada responsable de los procesos al interior del INDERHUILA, junto con su equipo de trabajo y bajo el acompañamiento de la segunda línea de defensa así: Riesgos de corrupción: oficina de Planeación o quien haga sus veces, Riesgos de Gestión: Líder de MIPG y Líder de Calidad, Riesgos de seguridad digital: Líder de las Tic.
- Consolidación: La dependencia con rol de segunda línea de defensa (Planeación o quien haga sus veces), le corresponde liderar el proceso de administración de los 3 tipos de riesgos según el caso.
- Adicionalmente, esta misma dependencia será la encargada de consolidar el mapa de riesgos de corrupción, gestión y seguridad digital y realizar los respectivos análisis.
- Publicación del mapa de riesgos de corrupción: Para el caso de los riesgos de corrupción, éstos se deben publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año, en coherencia con el PAAC.
- Ajustes y modificaciones: se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos (de corrupción, gestión y seguridad digital), después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas, conforme al control de cambios establecido por la INDERHUILA.
- La publicación será parcial y fundamentada en la elaboración del índice de información clasificada y reservada. En dicho instrumento del INDERHUILA debe establecer las condiciones de reserva y clasificación de algunos de los elementos constitutivos del mapa de riesgos en los términos dados en los artículos 18 y 19 de la Ley 1712 de 2014. En este caso se deberá anonimizar esa información. Es decir, la parte clasificada o reservada, aunque se elabora, no se hace visible en la publicación.


	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

Las excepciones solo pueden estar establecidas en la ley, un decreto con fuerza de ley o un tratado internacional ratificado por el Congreso o en la Constitución.

- **Socialización:** Los servidores públicos y contratistas del INDERHUILA deben conocer el mapa de riesgos de corrupción, gestión y seguridad digital antes de su publicación. Para lograr este propósito la dependencia que ejerce la segunda línea de defensa, deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos.
- **Monitoreo:** en concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizarán monitoreo y evaluación permanente a la gestión de riesgos de corrupción, gestión y seguridad digital, conforme a la primera línea de defensa establecida.
- **Seguimiento:** el jefe de control interno, o quien haga sus veces debe adelantar seguimiento a la gestión de riesgos de corrupción, gestión y seguridad digital. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en cada mapa de riesgos.

De acuerdo a los tres tipos de riesgos que se administran en la entidad, éstos se implementarán con base en la herramienta aprobada, conforme a:

- Riesgos de Gestión, bajo la coordinación del Sistema de la Líder de calidad y MIPG.
- Riesgos de Corrupción, bajo la coordinación de Planeación o quien haga sus veces
- Riesgos de Seguridad digital, bajo la coordinación del líder de las TIC.

 <b>INDERHUILA</b>	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

## 8. DESARROLLO METODOLÓGICO PARA LA FASE DE IDENTIFICACIÓN Y VALORACIÓN DE LOS RIEGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL

### 8.1 RIESGOS DE GESTIÓN

#### 8.1.1 Metodología para la Administración de los Riesgos de Gestión

##### 8.1.1.1 Análisis de objetivos estratégicos y de procesos


Antes de empezar el diseño e implementación del marco de referencia para la gestión integral del riesgo, es importante evaluar y entender el contexto tanto externo como interno de la organización, dado que este puede tener influencia significativa en el resultado final.

De acuerdo al artículo 52. de la constitución política de Colombia. “Se reconoce el derecho de todas las personas a la recreación, a la práctica del deporte y al aprovechamiento del tiempo libre. El Estado fomentará estas actividades e inspeccionará las organizaciones deportivas cuya estructura y propiedad deberán ser democráticas”, para lo cual el IINDERHUILA, tiene identificado procesos misionales como: deporte asociado, deporte formativo, infraestructura deportiva y recreación y aprovechamiento del tiempo libre y de apoyo, garantizando el cumplimiento de la misión y la visión institucional.

Adicionalmente, cuenta con personal profesional de planta y por prestación de servicios ubicados en las distintas áreas o dependencias de la Entidad, logrando un cubrimiento total para la prestación de un servicio de calidad adecuado y pertinente, pensando en la satisfacción de las necesidades y expectativas del ciudadano.

La entidad debe analizar los objetivos estratégicos y de procesos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso, es necesario revisar que se encuentren alineados con la Misión y la Visión Institucional y asegurar que los objetivos de procesos contribuyan a los objetivos estratégicos, así como, analizar su adecuada formulación.

Para la formulación o revisión de dichos objetivos, se tendrá en cuenta características de SMART (Sencillo, medible, ambicioso, relevante y tiempo).

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

### 8.1.1.2 Identificación de los puntos de riesgo o actividades claves de éxito del proceso.

Son actividades claves dentro del flujo del proceso donde existe evidencia o se tienen indicios que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control y monitoreo para asegurar que el proceso cumpla con su objetivo.

### 8.1.1.3 Identificación del impacto

Los Riesgos se identifican a partir del Marco Estratégico del INDERHUILA, o el documento que establezca el direccionamiento estratégico, que estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los **objetivos estratégicos o del proceso**.

Es la consecuencia “económica” o “reputacional” o “económica y reputacional” a la cual se ve expuesta la organización en caso de materializarse un riesgo.

Los impactos que aplican son de tipo económico y reputacional.

El **impacto / consecuencia** se establece, de acuerdo con los siguientes criterios:


RIESGOS DE GESTION		
NIVEL	CUANTITATIVAS - ECONOMICA	CUALITATIVAS - REPUTACIONAL
<b>CATASTROFICO 100%</b>	<ul style="list-style-type: none"> <li>-Impacto que afecte la ejecución presupuestal en un valor <math>\geq 50\%</math>.</li> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 50\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 50\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 50\%</math> del presupuesto general de la entidad.</li> </ul>	<ul style="list-style-type: none"> <li>-Interrupción de las operaciones de la entidad por más de cinco (5) días.</li> <li>- Intervención por parte de un ente de control u otro ente regulador.</li> <li>- Pérdida de información crítica para la entidad que no se puede recuperar.</li> <li>- Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal.</li> <li>- Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.</li> </ul>
<b>MAYOR 80%</b>	<ul style="list-style-type: none"> <li>-Impacto que afecte la ejecución presupuestal en un valor <math>\geq 20\%</math>.</li> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 20\%</math>.</li> </ul>	<ul style="list-style-type: none"> <li>-Interrupción de las operaciones de la entidad por más de dos (2) días.</li> <li>- Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.</li> </ul>



RIESGOS DE GESTION		
NIVEL	CUANTITATIVAS - ECONOMICA	CUALITATIVAS - REPUTACIONAL
	<ul style="list-style-type: none"> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 20\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 20\%</math> del presupuesto general de la entidad.</li> </ul>	<ul style="list-style-type: none"> <li>- Sanción por parte del ente de control u otro ente regulador.</li> <li>- Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.</li> <li>- Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.</li> </ul>
<b>MODERADO</b> <b>60%</b>	<ul style="list-style-type: none"> <li>- Impacto que afecte la ejecución presupuestal en un valor <math>\geq 5\%</math>.</li> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 10\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre-supuesto total de la entidad en un valor <math>\geq 5\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 5\%</math> del presupuesto general de la entidad.</li> </ul>	<ul style="list-style-type: none"> <li>- Interrupción de las operaciones de la entidad por un (1) día.</li> <li>- Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.</li> <li>- Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios.</li> <li>- Reproceso de actividades y aumento de carga operativa.</li> <li>- Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.</li> <li>- Investigaciones penales, fiscales o disciplinarias.</li> </ul>
<b>MENOR</b> <b>40%</b>	<ul style="list-style-type: none"> <li>- Impacto que afecte la ejecución presupuestal en un valor <math>\geq 1\%</math>.</li> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 5\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el pre-supuesto total de la entidad en un valor <math>\geq 1\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor <math>\geq 1\%</math> del presupuesto general de la entidad.</li> </ul>	<ul style="list-style-type: none"> <li>- Interrupción de las operaciones de la entidad por algunas horas.</li> <li>- Quejas de los usuarios relacionadas con la indebida aplicación de la Ley disciplinaria vigente, dentro de las actuaciones disciplinarias.</li> <li>- Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.</li> </ul>
<b>LEVE</b> <b>%</b>	<ul style="list-style-type: none"> <li>- Impacto que afecte la ejecución presupuestal en un valor <math>\geq 0,5\%</math>.</li> <li>- Pérdida de cobertura en la prestación de los servicios de la entidad <math>\geq 1\%</math>.</li> <li>- Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor <math>\geq 0,5\%</math>.</li> <li>- Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador.</li> </ul>	<ul style="list-style-type: none"> <li>- No hay interrupción de las operaciones de la entidad.</li> <li>- No se generan sanciones económicas o administrativas.</li> <li>- No se afecta la imagen institucional de forma significativa.</li> </ul>

Fuente. Función Pública



	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

#### 8.1.1.4 Descripción del riesgo

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para las personas ajenas a él. A continuación, se relaciona la estructura que facilita su redacción y claridad. Se inicia con la frase “POSIBILIDAD DE”.

Desglosando la estructura tenemos:

**Impacto:** Aquí definimos el ¿Qué puede pasar?, los factores de impacto a los que puede estar expuesta la entidad son:

**Afectación Económica:** afectación presupuestal de la entidad

**Afectación Reputacional:** afectación de la imagen de la entidad.

**Causa inmediata:** nos responde al ¿Cómo puede pasar?, son las situaciones más evidentes por las cuales se puede materializar el riesgo.

**Causa raíz:** nos da respuesta al ¿Por qué puede pasar?, se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o su causa pueden ser analizadas. Esta es la base para la definición de los controles.

El esquema para la redacción del riesgo es:

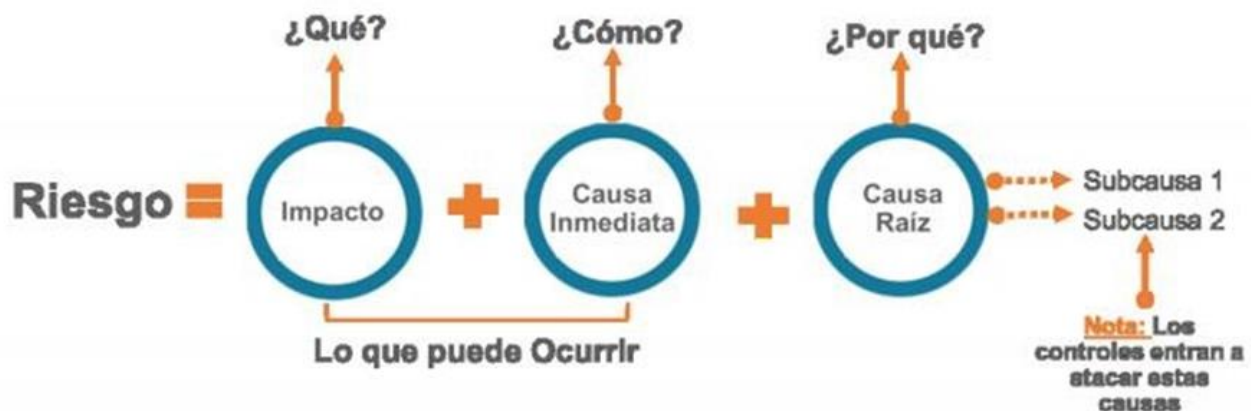



Gráfico. Función Pública

Figura Estructura propuesta para la redacción del riesgo y ejemplo

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa

Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)

Neiva-Huila

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

## Recomendaciones:

- **No describir como omisiones ni desviaciones de control.**

**Ejemplo:** errores en la liquidación de la nómina por fallas en los procedimientos existentes.

- **No describir causas como riesgos.**

**Ejemplo:** inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.

- **No describir riesgos como la negación de un control.**

**Ejemplo:** retrasos en la prestación del servicio por no contar con digiturno para la atención.


- **No existen riesgos transversales**, lo que pueden existir son causas transversales.

**Ejemplo:** pérdida de expedientes.

- **Evitar iniciar con palabras negativas como:** “No...”, “Que no...”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en...”
- Generar en el lector o escucha la imagen del evento como si ya estuviera sucediendo.
- Pregúntese si el riesgo identificado está relacionado directamente con las características del objetivo. Si la respuesta es “no”, lo descrito puede ser la causa o la consecuencia del riesgo

### 8.1.1.5. Identificación de factores de riesgo

FACTOR	DEFINICION	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.	grabación, autorización, errores en cálculos para pagos internos y externos, falta de capacitación, temas relacionados con el personal
Talento Humano	Incluye Seguridad y Salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto de activos, posibles comportamientos no éticos de los empleados, fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes, incendios, inundaciones, daño a activos fijos
Infraestructura	Eventos relacionados con la infraestructura física de la entidad.	Derrumbes, incendios, inundaciones, daños a activos fijos
Evento externo	Situaciones externas que afectan la entidad.	Suplantación de identidad, asalto a la oficina, atentados, vandalismo, orden público

 <b>INDERHUILA</b>	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

### 8.1.1.6 Valoración del Riesgo de Gestión

La valoración del Riesgo consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto del riesgo, con el fin de estimar la zona de Riesgo inicial o propia de la actividad también llamada RIESGO INHERENTE.

#### 8.1.1.6.1 Determinar la Probabilidad:


Consiste en establecer la probabilidad de ocurrencia y el nivel de consecuencia o impacto del riesgo, con el fin de estimar su **probabilidad** de ocurrencia e **impacto/ consecuencia** si no se controla (RIESGO INHERENTE).

El nivel de probabilidad estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando, es decir el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. Es decir, el número de veces que se ejecuta la acción.

A continuación, se establecen los criterios para definir el nivel de probabilidad:

NIVEL	FRECUENCIA DE LA ACTIVIDAD	FRECUENCIA DE EVENTOS	PROBABILIDAD
<b>MUY BAJA</b>	La actividad que conlleva el riesgo se ejecuta como máximo 4 veces por año.	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	20%
<b>BAJA</b>	La actividad que conlleva el riesgo se ejecuta de 5 veces al año máximo 12 veces al año.	El evento puede ocurrir en algún momento.	40%
<b>MODERAD A</b>	La actividad que conlleva el riesgo se ejecuta de mínimo 13 veces al año y máximo 365 veces al año.	El evento podrá ocurrir en algún momento.	60%
<b>ALTA</b>	La actividad que conlleva el riesgo se ejecuta de 500 veces al año y máximo 5.000 veces por año.	Es viable que el evento ocurra en la mayoría de las circunstancias.	80%
<b>MUY ALTA</b>	La actividad que conlleva el riesgo se ejecuta más de 5.000 veces por año.	Se espera que el evento ocurra en la mayoría de las circunstancias.	100%

Criterios para definir el nivel de PROBABILIDAD de ocurrencia de los riesgos

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

### 8.1.1.6.2 Determinar el Impacto:

Se contemplan afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, temas todos que se agrupan en impacto económico y reputacional.


Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, los cuales tienen diferentes niveles, se debe tomar el más alto, bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando a subjetividad que usualmente puede darse en este tipo de análisis.

Ilustración Función Pública

	Afectación Económica (o presupuestal)	Pérdida Reputacional
Insignificante 20%	Afectación menor a 10 SMLMV	Solo de conocimiento de algunos funcionarios.
Menor-40%	Mayores o iguales a 10 SMLMV y menores a 21 SMLMV	De conocimiento general de la entidad a nivel interno, de junta directiva y accionistas y/o de proveedores
Moderado 60%	Mayores o iguales a 21 SMLMV y menores a 318 SMLMV	Afecta imagen con algunos usuarios que impacten significativamente los objetivos.
Mayor 80%	Mayores o iguales a 318 SMLMV y menores a 2120 SMLMV	Deterioro de imagen con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayores a 2120 SMLMV	Deterioro de imagen a nivel nacional, con efecto publicitario sostenido a nivel país

### 8.1.1.6.3 Determinar el nivel de severidad en el mapa de calor:

Se trata de 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 (extremo, alto, moderado, bajo).

	POLITICA			CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>			VERSIÓN	01
				VIGENCIA	OCTUBRE 2020

Cruzando los datos de probabilidad e impacto definidos se tiene el nivel de severidad del riesgo.

### 8.1.1.7 Valoración de controles

Los controles o actividades de control son medidas que permiten reducir o mitigar las causas que hacen que el riesgo se materialice, por eso la importancia en su diseño y evaluación, se debe tener en cuenta:

- La identificación de los controles se realiza a cada riesgo a través de entrevistas con los líderes de procesos o servidores expertos en su quehacer, de igual forma son los responsables de implementar y monitorear dichos controles con el apoyo de su equipo de trabajo.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

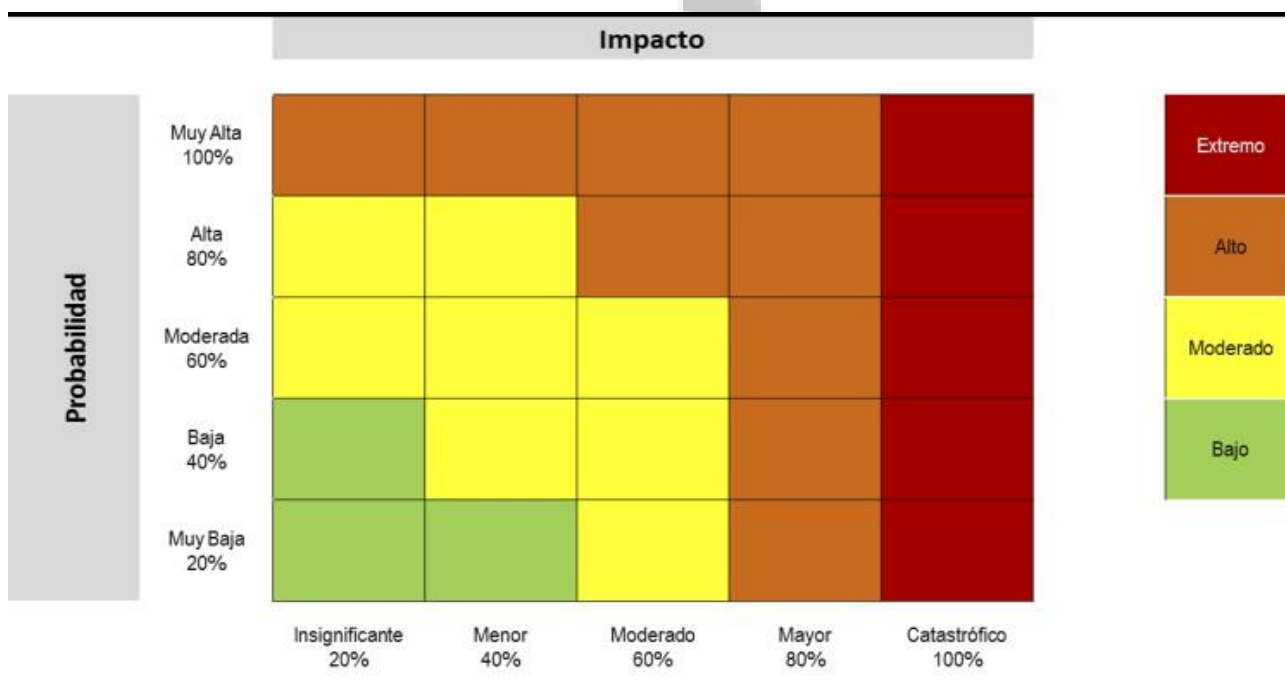


Ilustración Función Pública



CRITERIO DE EVALUACIÓN	DESCRIPCION	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	PESO
1. Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
	Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
3. Tipo	Prevenir	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
	Detectar	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
	Corregir	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
3. Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
	Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
4. Estado de la documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
	Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
5. Evidencia de la ejecución del control	Con registro	El control deja un registro, permite evidenciar la ejecución del control.	-
	Sin registro	El control no deja registro de la ejecución del control.	-
<b>TOTAL VALORACION CONTROL # _____ Máximo 50%, mínimo 25%</b>			


Ilustración Función Pública

### 8.1.1.6.5 Estructura para la descripción del control

Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
Neiva-Huila



	<b>POLITICA</b>		<b>CODIGO</b>	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>		<b>VERSIÓN</b>	01
			<b>VIGENCIA</b>	OCTUBRE 2020

- Responsable de ejecutar el control: Identifica el cargo del servidor que ejecuta el control, en caso de ser controles automáticos se identificará el sistema que realiza la actividad.
- Acción: Se determina mediante verbos en los cuales se identifica la acción a realizar como parte del control.
- Complemento: Corresponde a los detalles que permiten identificar claramente el objeto del control.

En la redacción del control tener en cuenta la siguiente estructura:

**Acción de control + Periodicidad+ Evidencia + Complemento + Responsable de ejecutar el control**

Ej. Comparar semestralmente el listado maestro de documentos generado de la base de datos con los documentos físicos de los documentos del sistema de gestión por parte del líder de calidad.

### 8.1.1.6.6 Tipología de controles

A través del ciclo de los procesos es posible establecer cuándo se activa un control y por lo tanto establecer su tipología con mayor precisión, para comprender esta estructura conceptual se consideran 3 fases globales del ciclo de un proceso.

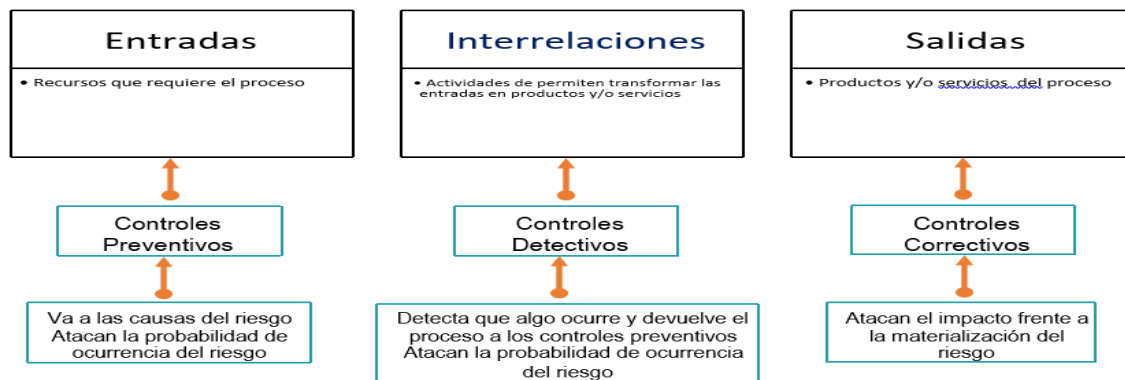


Ilustración Función Pública

- Control preventivo: Acción y/o mecanismo ejecutado antes que se realice la actividad originadora del riesgo, se busca establecer condiciones que aseguren el resultado final esperado. En general estos controles actúan sobre las causas del riesgo.
- Control detectivo: Acción y/o mecanismo ejecutado que permite detectar el riesgo durante la ejecución del proceso y puede disminuir la materialización de dicho riesgo. Estos controles detectan el riesgo, pero genera reprocesos.
- Control correctivo: Acción que se ejecutan después de que se materializa el riesgo y en la mayoría de las ocasiones permiten reducir el impacto de dicho riesgo.

**De acuerdo** con la forma como se ejecutan los controles tenemos:

**Control manual:** controles que son ejecutados por personas.

**Control automático:** son ejecutados por un sistema.

### 8.1.1.6.7 Determinar la eficiencia de los controles

Características		Descripción	Peso	
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	49%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	33%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	16%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	49%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	25%

Ilustración Función Pública

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila



Una vez identificado el tipo de control se revisa si su implementación es manual o automático y se establece el peso porcentual.

La entidad deberá implementar una política de reducción del control máximo del 50%, con el fin de evitar que un solo control genere movimientos exagerados dentro de la matriz. (Ejemplo: Control = preventivo (49%) + automático (49%) = 98%, este valor puede generar movimientos de zonas altas o extremas a zonas bajas que distorsionan el análisis).

Teniendo en cuenta que es a partir de los controles que se dará el movimiento en la matriz de calor a continuación, se muestra en la matriz o mapa de calor cual es el movimiento en el eje de probabilidad e impacto según el tipo de control.

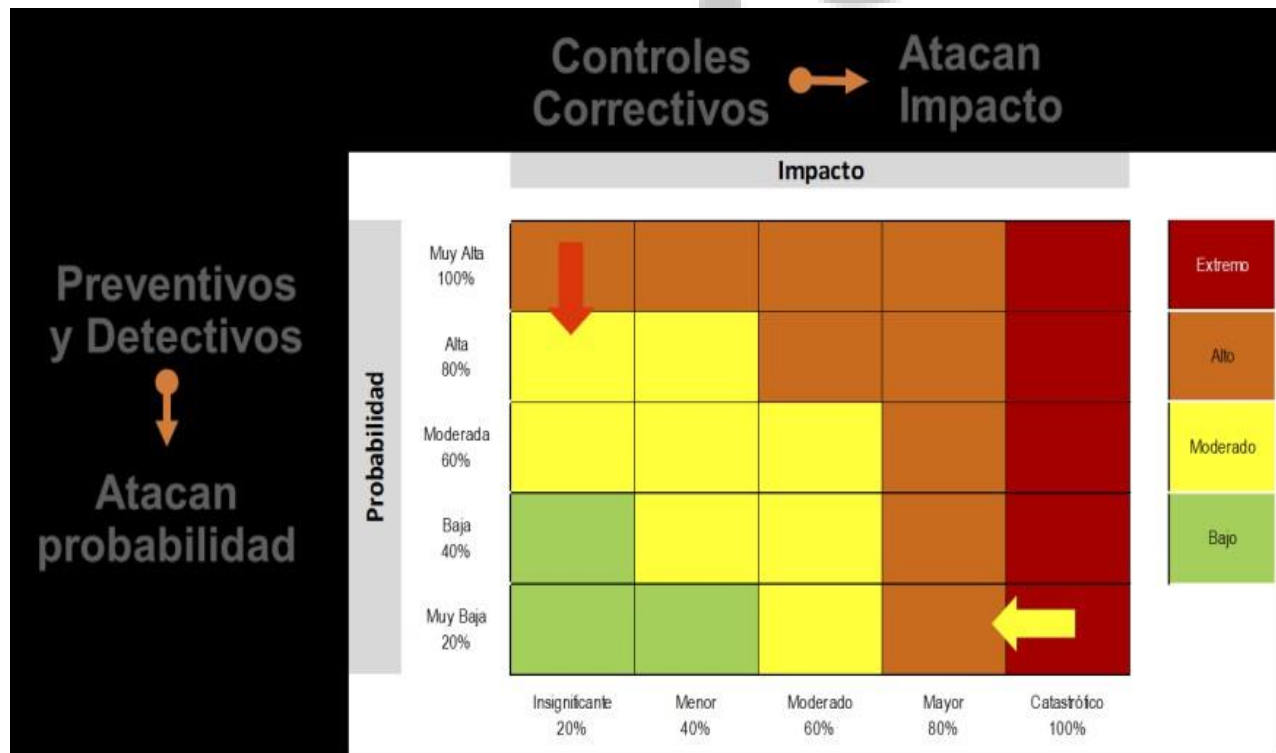



Ilustración Función Pública

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020


### 8.1.1.6.8 Determinar Riesgo Residual:

Dependiendo del nivel de severidad en que se ubique el riesgo residual una vez aplicados los controles y determinada su efectividad, el INDERHUILA priorizará la atención en aquellos niveles de severidad Extrema, Alta y Moderada, a los cuales se les debe realizar acciones de tratamiento.



Ilustración Función Pública

HUILA  
CRECE

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

## 8.2 RIESGOS DE CORRUPCION

### 8.2.1 METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE CORRUPCIÓN

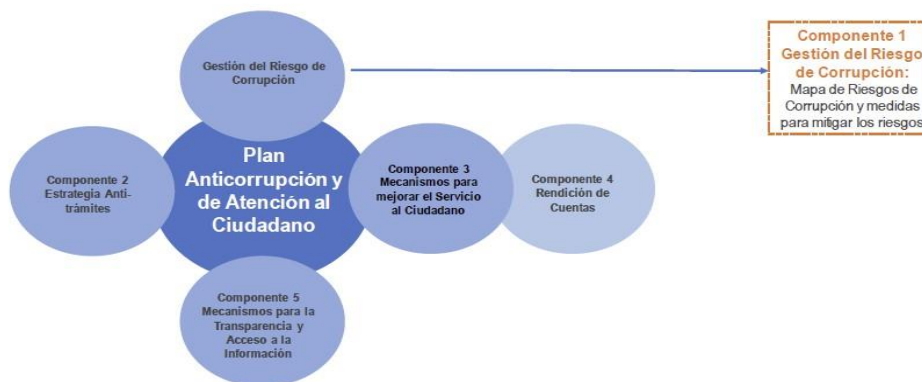
Para la gestión de riesgos de corrupción, continúa vigente los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018.

#### 8.2.1.2 Lineamientos sobre los riesgos relacionados con posibles actos de corrupción.

En el marco del Plan Anticorrupción y de Atención al Ciudadano establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1.) que define las estrategias de lucha contra la corrupción y de atención al ciudadano se definen los lineamientos para la identificación y valoración de riesgos de corrupción que hacen parte del componente 1: gestión del riesgo de corrupción. Esta se articula con los demás componente del PAAC, ya que se trata de una acción integral en la lucha contra la corrupción.

Dependiendo del nivel de severidad en que se ubique el riesgo residual una vez aplicados los controles y determinada su efectividad, el INDERHUILA priorizará la atención en aquellos niveles de severidad Extrema, Alta y Moderada, a los cuales se les debe realizar acciones de tratamiento.


Figura 20 Componentes plan anticorrupción y de atención al ciudadano



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y la Secretaría de Transparencia, 2020.

Ilustración Función Pública

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila

 <b>INDERHUILA</b>	<b>POLITICA</b>	<b>CODIGO</b>	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	<b>VERSIÓN</b>	01
		<b>VIGENCIA</b>	OCTUBRE 2020

### 8.2.2 Definición de Riesgo de Corrupción:

Es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

“Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos” (Conpes N° 167 de 2013).

Es necesario que en la descripción del riesgo concurren los componentes de su definición, así:


**ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.**

Los riesgos de corrupción se establecen sobre procesos. El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos. Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la siguiente matriz de definición de riesgo de corrupción, que incorpora cada uno de los componentes de su definición. Si se marca con una X en la descripción del riesgo que aparece en cada casilla quiere decir que se trata de un riesgo de corrupción (si no cumple las 4 condiciones no es riesgo de corrupción, así:

<b>MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN</b>				
<b>Descripción del riesgo</b>	<b>Acción u omisión</b>	<b>Uso del poder</b>	<b>Desviar la gestión de lo público</b>	<b>Beneficio privado</b>
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República.



	<b>POLITICA</b>	<b>CODIGO</b>	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	<b>VERSIÓN</b>	01
		<b>VIGENCIA</b>	OCTUBRE 2020


### 8.2.3 Identificación de Riesgo de Corrupción:

Análisis de Contexto de Riesgos. Procesos, procedimientos o actividades susceptibles de riesgos de corrupción, a partir de los cuales se podrá adelantar el análisis de contexto interno para la correspondiente identificación de los riesgos.

Algunos de los procesos, procedimientos o actividades susceptibles de actos de corrupción:

Direccionamiento estratégico (alta dirección)	<ul style="list-style-type: none"> <li>• Concentración de autoridad o exceso de poder.</li> <li>• Extralimitación de funciones.</li> <li>• Ausencia de canales de comunicación.</li> <li>• Amiguismo y clientelismo.</li> </ul>
Financiero (está relacionado con áreas)	<ul style="list-style-type: none"> <li>• Inclusión de gastos no autorizados. de planeación y presupuesto) Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración.</li> <li>• Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión.</li> <li>• Inexistencia de archivos contables.</li> <li>• Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.</li> </ul>
De contratación (como proceso o bien los procedimientos ligados a este)	<ul style="list-style-type: none"> <li>• Estudios previos o de factibilidad deficientes.</li> <li>• Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular).</li> <li>• Pliegos de condiciones hechos a la medida de una firma en particular.</li> <li>• Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica).</li> <li>• Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación.</li> <li>• Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados.</li> <li>• Urgencia manifiesta inexistente. • Concentrar las labores de supervisión en poco personal.</li> </ul>
De información y documentación	<ul style="list-style-type: none"> <li>• Ausencia o debilidad de medidas y/o políticas de conflictos de interés.</li> <li>• Concentraciyn de información de determinadas actividades o procesos en una persona.</li> <li>• Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración.</li> <li>• Ocultar la informaciyn considerada pública para los usuarios.</li> <li>• Ausencia o debilidad de canales de comunicación de investigación y Sanción.</li> </ul>
De investigación y Sanción	<ul style="list-style-type: none"> <li>• Inexistencia de canales de denuncia interna o externa.</li> <li>• Dilatar el proceso para lograr el vencimiento de términos o la prescripción de este.</li> <li>• Desconocimiento de la ley mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación.</li> <li>• Exceder las facultades legales en los fallos. De trámites y/o servicios internos y externos</li> </ul>
De trámites y/o servicios internos y externos	<ul style="list-style-type: none"> <li>• Cobros asociados al trámite.</li> <li>• Influencia de tramitadores.</li> <li>• Tráfico de influencias: (amiguismo, persona influyente). De reconocimiento de un derecho (expedición de licencias y/o permisos)</li> </ul>
De reconocimiento de un derecho (expedición de licencias y/o permisos)	<ul style="list-style-type: none"> <li>• Falta de procedimientos claros para el trámite</li> <li>• Imposibilitar el otorgamiento de una licencia o permiso.</li> <li>• Tráfico de influencias: (amiguismo, persona influyente).</li> </ul>

Fuente: Secretaría de Transparencia, 2018

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

## 8.2.4. Valoración de Riesgos de Corrupción

### Cálculo de la probabilidad e impacto

#### Análisis de la probabilidad.

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde, frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

Criterios para calificar: Probabilidad e Impacto

	Descriptor	Descripción	Frecuencia
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los 2 últimos años
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años
1	Rara vez	circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años

Para determinar el **IMPACTO/CONSECUENCIA**: este se determina para establecer las consecuencias o efectos del riesgo, con el fin de estimar la zona de riesgo en caso de no controlarse (RIESGO INHERENTE). Para definir la tabla de criterios, las variables principales que se tienen en cuenta son impactos económicos y reputaciones.

Cuando se presente más de un impacto en un solo riesgo con diferentes niveles, se debe tomar el nivel más alto.

Para el Riesgos de **Corrupción y Fraude** se tiene en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos. En este orden de ideas, no se contemplan los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.


	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

Tabla Función Pública

NIVEL	VALOR IMPACTO / CONSECUENCIA RIESGOS	
	Riesgos de Gestión y de Seguridad de la Información	Riesgos de Corrupción y Fraude
LEVE	20%	N/A
MENOR	40%	
MODERADO	60%	60%
MAYOR	80%	80%
CATASTRÓFICO	100%	100%

Criterios para definir el nivel de impacto/consecuencia riesgos de la entidad vs riesgos de corrupción

Para calificar el impacto / consecuencia del riesgo de corrupción y fraude se debe responder el siguiente cuestionario

No.	PREGUNTA: Si el Riesgo de Corrupción o Fraude se materializa podría:	RESPUESTA	
		SI	NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila



Medición de Impacto Riesgo de Corrupción			
Descriptor	Descripción	Nivel	Respuestas Afirmativas
Moderado	Afectación parcial al proceso y a la dependencia Genera medianas consecuencias para la entidad.	5	1 – 5
Mayor	Impacto negativo de la Entidad Genera altas consecuencias para la entidad.	10	6 - 11
Catastrófico	Consecuencias desastrosas sobre el sector Genera consecuencias desastrosas para la entidad.	20	12 - 19

Ilustración Función Pública

### Análisis del impacto en riesgos de corrupción

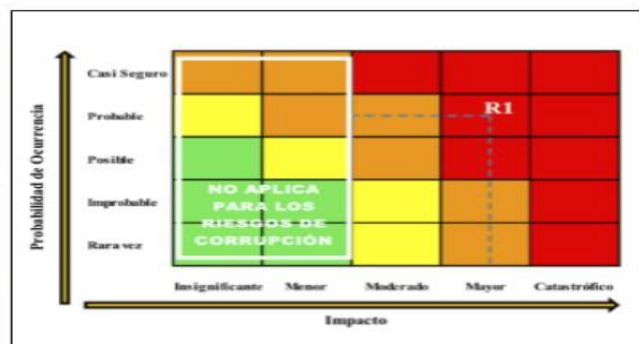
Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos.


Por último ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.

Ilustración Función Pública

Extremo	■
Alto	■
Moderado	■
Bajo	■

**IMPORTANTE**  
Aunque se utilice el mismo mapa de calor, para los riesgos de gestión y de corrupción, a estos últimos solo les aplican las columnas de impacto Moderado, Mayor y Catastrófico.



	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

Criterios para Análisis y evaluación de controles, según 6 variables:

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	No asignado
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	Inadecuado
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	Inoportuna
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, ejemplo Verificar, Validar Cotejar, Comparar, Revisar, etc.?	Prevenir o detectar	No es un control
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?.	Confiable	No confiable
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	No se investigan y resuelven oportunamente.
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control, que permita a cualquier tercero con la evidencia, llegar a la misma conclusión?.	Completa	Incompleta / no existe

Tabla. Función Pública

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila





**Criterios para evaluar controles**

**Solidez del Control Integralmente (Diseño y Ejecución)**

Peso del diseño individual o promedio de los Controles. (DISEÑO)	El Control se ejecuta de manera consistente por los responsables. (EJECUCION)	Solidez individual de cada control Fuerte:100 Moderado:50 Débil:0	Aplica acciones para fortalecer el Control Si / NO	
Fuerte Calificación Entre 96 y 100	Fuerte (Siempre se ejecuta)	Fuerte + Fuerte = Fuerte	NO	
	Moderado ( Algunas veces)	Fuerte + Moderado = Moderado	SI	
	Débil (No se ejecuta)	Fuerte + Débil = Débil	SI	
Moderado Calificación Entre 86 y 95	Fuerte (Siempre se ejecuta)	Moderado + Fuerte = Moderado	SI	
	Moderado (Algunas veces)	Moderado + Moderado = Moderado	SI	
	Débil (No se ejecuta)	Moderado + Débil = Débil	SI	
Débil Entre 0 y 85	Fuerte (Siempre se ejecuta)	Débil + Fuerte = Débil	SI	
	Moderado (Algunas veces)	Débil + Moderado = Débil	SI	
	Débil (No se ejecuta)	Débil + Débil = Débil	SI	
Moderado	No disminuye	Directamente	0	1



Si la solidez del conjunto de los controles es Débil, este no disminuirá ningún cuadrante de impacto o probabilidad


**Solidez del Control Integralmente (Diseño y Ejecución)**



Calificación de la Solidez del Conjunto de Controles	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación está entre 50 y 99
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos la calificación es menor a 50.

Ilustración Función Pública



	POLITICA		CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>		VERSIÓN	01
			VIGENCIA	OCTUBRE 2020

## 8.2.5 Tratamiento de Riesgos de Corrupción

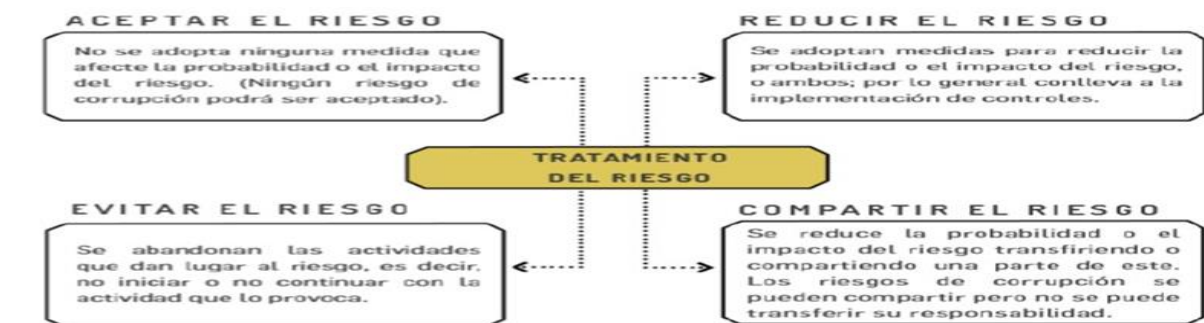
El formato general para el Plan de Tratamiento de los Riesgos de Corrupción es:

PLAN DE TRATAMIENTO OBLIGATORIO PARA LOS RIESGOS NO CONTROLADOS							
ACCIÓN A IMPLEMENTAR	F - INICIO	F - FIN	RESPONSABLE DE LA ACCIÓN	F- SEGUIMIENTO	EVIDENCIA O SOPORTE	SEGUIMIENTO DESCRIPCIÓN	PORCENTAJE DE AVANCE

En la actividad de control deberá registrar el tiempo con el cual aplica el control. En el porcentaje de avance, podrá hacer énfasis también al indicador que le permite determinar el % de avance.

*Tener en cuenta que, de acuerdo a la política, se establecerán las acciones de tratamiento correspondientes, según política, así;*

Ilustración Función Pública




Fuente: DAFP

ACEPTAR EL RIESGO

**IMPORTANTE**  
En el caso de riesgos de corrupción, estos no pueden ser aceptados.

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila

 <b>INDERHUILA</b>	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

### 8.2.6 Seguimiento de riesgos de corrupción - OFICINA DE CONTROL INTERNO

**SEGUIMIENTO:** El Jefe de Control Interno, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.

**Primer seguimiento:** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

**Segundo seguimiento:** Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

**Tercer seguimiento:** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.


El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

En especial deberá adelantar las siguientes actividades:

- Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
- Seguimiento a la gestión del riesgo.
- Revisión de los riesgos y su evolución.
- Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.
- Acciones a seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

- 1) Informar a las autoridades de la ocurrencia del hecho de corrupción.
- 2) Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- 3) Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- 4) Llevar a cabo un monitoreo permanente.

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

### 8.2.7 Herramienta para la gestión de los riesgos de corrupción:


Herramienta en Excel, que incluye 9 hojas, así:

Hoja # 1: CRITERIOS PARA IDENTIFICAR/REDACTAR RIESGOS DE CORRUPCIÓN Y METODOLOGÍA ESTABLECIDA, no se diligencia, solo para tener en cuenta para la identificación de Riesgos de Corrupción”, considerando el concepto de Riesgo de Corrupción, con las 4 condiciones que debe cumplir para ser un riesgo de corrupción (ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO), conforme a la “Matriz definición del Riesgo de Corrupción”, teniendo presente el ejemplo de descripción de riesgo de corrupción establecido en este formato.

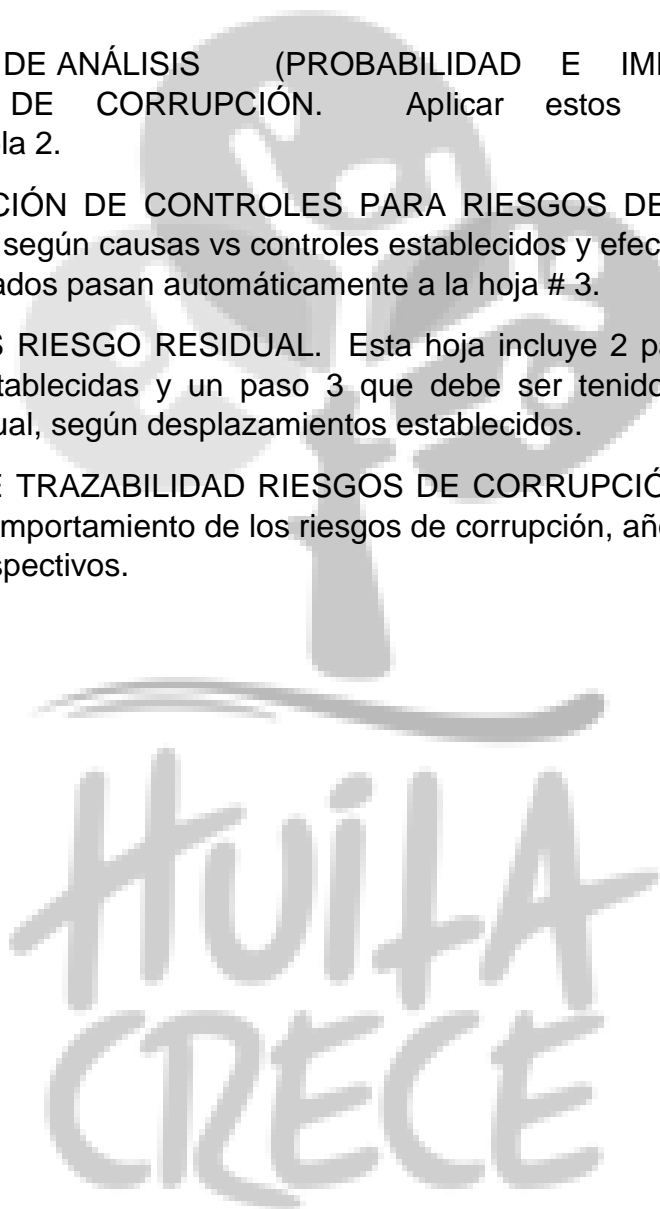
2. Hoja # 2: Mapa de Riesgos de Corrupción. No requiere diligenciamiento, porque ésta se genera automáticamente de la Hoja # 3, mientras no se dañen los link automáticos.


3. Hoja # 3: MATRIZ DE IDENTIFICACIÓN, VALORACIÓN, TRATAMIENTO Y SEGUIMIENTO DE RIESGOS CORRUPCIÓN. Es la hoja de trabajo, que enlaza las otras hojas.

4. Hoja # 4. ANÁLISIS DEL CONTEXTO PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE CORRUPCIÓN. Permite realizar el análisis de contexto interno, externo y de proceso. Así mismo identificar OPORTUNIDADES asociadas a riesgos de corrupción.

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

5. Hoja # 5: CRITERIOS PARA VALORAR RIESGOS DE CORRUPCIÓN. Tenerlos en cuenta.
6. Hoja # 6: CRITERIOS DE ANÁLISIS (PROBABILIDAD E IMPACTO), PARA VALORAR RIESGOS DE CORRUPCIÓN. Aplicar estos criterios, según corresponda Tabla 1 y tabla 2.
7. Hoja # 7: EVALUACIÓN DE CONTROLES PARA RIESGOS DE CORRUPCIÓN. Diligencia esta hoja, según causas vs controles establecidos y efectuar la evaluación según tabla. Estos resultados pasan automáticamente a la hoja # 3.
8. Hoja # 8. CRITERIOS RIESGO RESIDUAL. Esta hoja incluye 2 pasos automáticos con fórmulas preestablecidas y un paso 3 que debe ser tenido en cuenta para determinar el riesgo residual, según desplazamientos establecidos.
9. Hoja # 9. MATRIZ DE TRAZABILIDAD RIESGOS DE CORRUPCIÓN. Permite llevar la trazabilidad del comportamiento de los riesgos de corrupción, año a año, con el fin de generar los análisis respectivos.



	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

## 8.3 RIESGOS DE SEGURIDAD DIGITAL

### 8.3.1 METODOLOGIA PARA LA ADMINISTRACION DE RIESGOS DE GESTION DIGITAL

Tener en cuenta que la política de seguridad digital, se vincula al modelo de seguridad y privacidad de la información (MSPI)<sup>3</sup>, 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

Identificación de los activos de seguridad de la información: como primer paso para la identificación de riesgos de seguridad de la información es necesario identificar los activos de información del proceso.

#### 8.3.1.1. Conceptualización de Activos:

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: -Aplicaciones de la organización	Permite determinar <b>qué es lo más importante que cada entidad y sus procesos poseen</b> (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios).
-Servicios web -Redes -Información física o digital -Tecnologías de información TI -Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	La entidad puede saber <b>qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano</b> , aumentando así su confianza en el uso del entorno digital.

Fuente: Actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública y Ministerio TIC, 2020





**Pasos para identificación de activos:**



Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

**Nota:** para realizar la identificación de activos deberá remitirse a la sección 3.1.6 del anexo 4 “Modelo nacional de gestión de riesgo de seguridad de la información en entidades públicas” que hace parte de los anexos de la presente guía.

# ¿Cómo identificar los activos?

## Ejemplo

ACTIVO	TIPO DE ACTIVO	CRITICIDAD CON RESPECTO A SU CONFIDENCIALIDAD	CRITICIDAD CON RESPECTO A SU COMPLETITUD	CRITICIDAD CON RESPECTO A SU COMPLETITUD	NIVEL DE CRITICIDAD
BASES DE DATOS DE NÓMINA	Información	Alta	Alta	Alta	Alta
APLICATIVO DE FINANCIERO	Software	Alta	Media	Media	Media
SERVIDOR INTERNO	Hardware	Baja	Baja	Baja	Baja

Ilustración Función Pública




	<b>POLITICA</b>					<b>CODIGO</b>	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>					<b>VERSIÓN</b>	01
						<b>VIGENCIA</b>	OCTUBRE 2020

Tabla 12 Ejemplo identificación activos del proceso

Proceso	Activo	Descripción	Dueño del activo	Tipo del activo	Ley 1712 de 2014	Ley 1581 de 2012	Criticidad respecto a su confidencialidad	Criticidad respecto a completitud o integridad	Criticidad respecto a su disponibilidad	Nivel de criticidad
Gestión financiera	Base de datos de nómina	Base de datos con información de nómina de la entidad	Jefe de oficina financiera	Información	Información reservada	No contiene datos personales	ALTA	ALTA	ALTA	ALTA
Gestión financiera	Aplicativo de nómina	Servidor web que contiene el <i>front office</i> de la entidad	Jefe de oficina financiera	Software	N/A	N/A	BAJA	MEDIA	BAJA	MEDIA
Gestión financiera	Cuentas de cobro	Formatos de cobro diligenciados	Jefe de oficina financiera	Información	Información pública	No contiene datos personales	BAJA	BAJA	BAJA	BAJA

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

Corresponde al líder del Sistema de Gestión de Seguridad y Privacidad de la Información y al líder del proceso o proyecto la identificación de los riesgos de la Información. Estos se basan en la afectación de tres criterios en un activo de información o un grupo de activos de información dentro del proceso “Integridad, confidencialidad o disponibilidad”.

### 8.3.2 Identificación del riesgo de seguridad digital:

Se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

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

Para cada riesgo se deben asociar el grupo de activos, o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el Anexo 4

Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas donde se encuentran las siguientes tablas necesarias para este análisis:

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila


	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

Tabla 5. Tabla de amenazas comunes

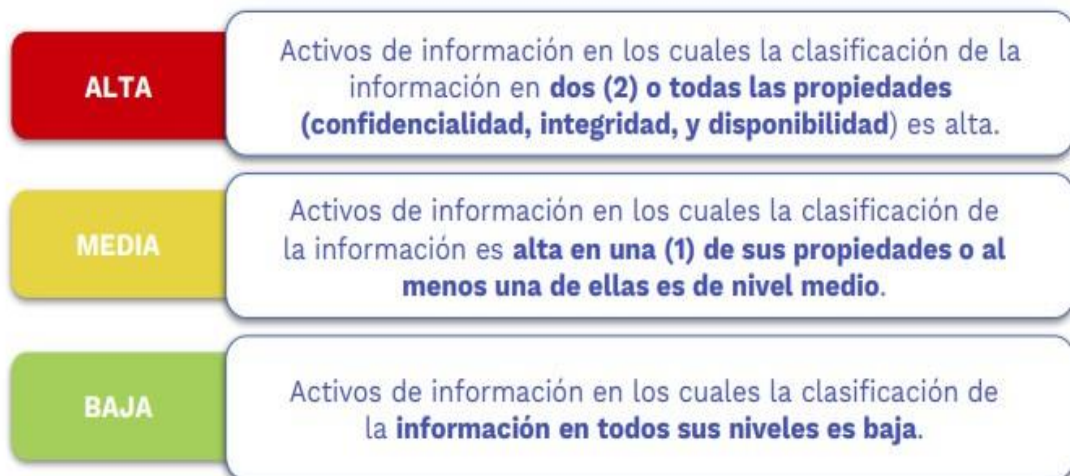
Tabla 6. Tabla de amenazas dirigida por el hombre

Tabla 7. Tabla de vulnerabilidades comunes


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.

## Niveles de criticidad de los activos



*Ilustración Función Pública*

	<b>POLITICA</b>			<b>CODIGO</b>	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>			<b>VERSIÓN</b>	01
				<b>VIGENCIA</b>	OCTUBRE 2020

**10 pasos para establecer los CRITERIOS PARA IDENTIFICAR LA CRITICIDAD DE LOS ACTIVOS DE SEGURIDAD DIGITAL. Para un proceso x:**

1 Activos de Seguridad digital asociados al proceso	2 Tipo de Activo	3 Dueño del Activo	4 Custodia del Activo	5 Clasificación de los activos			6 Criticidad del activo
				Confidencialidad	Integridad	Disponibilidad	
Informacion del SIG	Información	Gerente SIG	Gerente SIG	3	1	1	Alta
Aplicativo extranet	Software	Lider Atencion al ciudadano	Coordinador TIC	3	1	1	Alta
Funcionarios de apoyo al proceso	Personas	Secretaria General	Gerente SIG	3	1	1	Alta
Acompañamiento a la implementacion y mejora continua del SIG	Servicios	Secretaria General	Gerente SIG	3	1	1	Alta
Herramientas tecnologicas para seguimiento del SIG	Software	Secretaria General	Gerente SIG	2	1	1	Alta
Equipos de computo	Hardware	Secretaria General	Gerente SIG	3	2	2	Media
							Baja

Ilustración Función Pública

7 Amenazas por activo				8 Causas / Vulnerabilidades			9 Infraestructura Crítica Cibernética	10 Observaciones
Naturales	Industriales	Errores	Ataques					
N.A.	N.A.	Destrucción de la información	Destrucción de la información	Fallas en conectividad a internet	Falta de backup de la información	Falta de políticas de seguridad de la información	N.A.	N.A.
N.A.	Avería de origen físico o lógico	Alteración accidental de la información	Modificación deliberada de la información	Fallas en servidor de app extranet	Falta de backup de la información	Falta de políticas de seguridad de la información	N.A.	N.A.
N.A.	N.A.	Indisponibilidad del personal	Indisponibilidad del personal	Ausencia del personal			N.A.	N.A.
N.A.	N.A.	Alteración accidental de la información	Destrucción de la información	Falta de backup de la información	Falta de políticas de seguridad de la información		N.A.	N.A.
Avería de origen físico o lógico	N.A.	Errores de los usuarios	Manipulación de programas	Fallas en conectividad a internet			N.A.	N.A.
Daños por desastres naturales	Daños debido a actividad humana	Errores de mantenimiento o actualización de hardware	Uso no previsto	Mantenimiento insuficiente	Falta de políticas de seguridad de la información		N.A.	N.A.



**POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL**

Personal	Falta de capacitación en las herramientas	Error en el uso
Organización	Ausencia de políticas de seguridad	Abuso de los derechos

Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC, 2018.

	protección	documentos
Software	Ausencia de parches de seguridad	Abuso de los derechos
Red	Líneas de comunicación sin protección	Escucha encubierta
Información	Falta de controles de acceso físico	Hurto de información


Tabla de amenazas y vulnerabilidades – Función Pública

**Riesgo de seguridad digital:** combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como 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.

Ejemplo Riesgo de seguridad digital de un proceso de nómina:

Ilustración Función Pública

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/VULNERABILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo (legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

 <b>INDERHUILA</b>	<b>POLITICA</b>	<b>CODIGO</b>	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	<b>VERSIÓN</b>	01
		<b>VIGENCIA</b>	OCTUBRE 2020

### 8.3.3. Valoración del Riesgo

Esta etapa tiene como objetivo establecer la probabilidad de ocurrencia del riesgo, es decir la exposición que tiene la entidad frente al riesgo y el impacto o consecuencias que se pueden generar, con el fin de determinar la zona de severidad del riesgo inherente, así mismo se diseñarán y analizarán la efectividad de los controles existentes.

La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año, es decir el número de veces que se ejecuta la acción.

Lo anterior, permite determinar con total claridad la frecuencia con la cual se lleva a cabo una actividad y no los posibles eventos que pudiesen haberse dado en el pasado, ya que, bajo esta óptica, si nunca se han presentado eventos, todos los riesgos tendrán la tendencia a quedar ubicados en niveles bajos, situación que no es real frente a la gestión.

#### 8.3.3.1 Determina la Probabilidad

Criterios para definir el nivel de **PROBABILIDAD** de ocurrencia de los riesgos.


**Nota:** En materia de tecnología (incluye disponibilidad de aplicativos) se tiene en cuenta 1 hora de funcionamiento = 1 vez

Se analiza a partir de la pregunta ¿qué tan posible es que ocurra el riesgo? Está asociada a la exposición al riesgo del proceso o actividad que se está analizando, se trata en este caso de un hecho que no se ha presentado, pero es posible, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año, o tratándose de hechos que se han materializado o frente a los cuales se cuenta con un historial de situaciones o eventos asociados al riesgo.

A continuación, se establecen los criterios para definir el nivel de probabilidad:

El nivel de probabilidad estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando, es decir el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. Es decir, el número de veces que se ejecuta la acción.



	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

### Criterios para definir la probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad se realiza máximo 4 veces por año.	20%
Baja	La actividad se realiza mínimo 5 veces al año y máximo 12 veces al año.	40%
Moderada	La actividad se realiza mínimo 13 veces al año y máximo 365 veces al año.	60%
Alta	La actividad se realiza mínimo 365 veces al año y máximo 3660 veces al año.	80%
Muy Alta	La actividad se realiza 3661 veces o más al año	100%

*Ilustración Función Pública*

#### 8.3.3.2 Determinar el impacto

El impacto se entiende como la consecuencia económica y reputacional que se genera por la materialización del riesgo.

Se contemplan afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, temas todos que se agrupan en impacto económico y reputacional.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, los cuales tienen diferentes niveles, se debe tomar el más alto

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento eliminando la subjetividad que usualmente puede darse en este tipo de análisis:





**Criterios para definir el impacto**

	Afectación Económica (o Pérdida Reputacional presupuestal)	
Insignificante 20%	Afectación menor a 10 SMLMV	Sólo de conocimiento de algunos funcionarios.
Menor 40%	Mayores o iguales a 10 SMLMV y menores a 21 SMLMV	De conocimiento general de la entidad a nivel interno, de junta directiva y accionistas y/o de proveedores
Moderado 60%	Mayores o iguales a 21 SMLMV y menores a 318 SMLMV	Afecta imagen con algunos usuarios que impacten significativamente los objetivos.
Mayor 80%	Mayores o iguales a 318 SMLMV y menores a 2120 SMLMV	Deterioro de imagen con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayores a 2120 SMLMV	Deterioro de imagen a nivel nacional, con efecto publicitario sostenido a nivel país

Ilustración Función Pública

NIVEL	VALOR	
	Riesgos de Gestión y de Seguridad de la Información	Riesgos de Corrupción y Fraude
LEVE	20%	N/A
MENOR	40%	N/A
MODERADO	60%	60%
MAYOR	80%	80%
CATASTRÓFICO	100%	100%

El **impacto / consecuencia** se establece, de acuerdo con los siguientes criterios

De acuerdo con el resultado anterior, el número de preguntas contestadas afirmativamente permitirá ubicar el riesgo según la siguiente tabla y determinar el impacto / consecuencias del riesgo de corrupción y fraude:

DESCRIPTOR	CANTIDAD DE PREGUNTAS AFIRMATIVAS	IMPACTO / CONSECUENCIAS CUALITATIVO
<b>CATASTRÓFICO 100%</b>	DOCE a DIECINUEVE preguntas	Genera consecuencias desastrosas para la entidad
<b>MAYOR 80%</b>	SEIS a ONCE preguntas	Genera altas consecuencias sobre
<b>MODERADO 60%</b>	UNA a CINCO pregunta(s)	Genera medianas consecuencias sobre la

Calificación impacto / consecuencia  
– RIESGO CORRUPCION



RIESGO DE SEGURIDAD DE LA INFORMACION		
NIVEL	CUANTITATIVAS - ECONOMICA	CUALITATIVAS - REPUTACIONAL
<b>CATASTROFICO 100%</b>	<ul style="list-style-type: none"> <li>-Afectación mayor o igual al 50% de la población.</li> <li>-Afectación mayor o igual al 50% del presupuesto anual de seguridad digital.</li> <li>-Afectación muy grave del medio ambiente que requiere de mayor o igual a 3 años de recuperación.</li> </ul>	<ul style="list-style-type: none"> <li>-Afectación muy grave de la integridad de la información debido al interés particular de los empleados y terceros.</li> <li>- Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.</li> <li>- Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.</li> </ul>
<b>MAYOR 80%</b>	<ul style="list-style-type: none"> <li>-Afectación en un valor igual o mayor al 20% e inferior al 50% de la población.</li> <li>-Afectación en un valor igual o mayor al 20% e inferior al 50% del presupuesto anual de seguridad digital.</li> <li>-Afectación importante del medio ambiente que requiere de 1 a 3 años de recuperación.</li> </ul>	<ul style="list-style-type: none"> <li>-Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros.</li> <li>-Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.</li> <li>-Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.</li> </ul>
<b>MODERADO 60%</b>	<ul style="list-style-type: none"> <li>-Afectación en un valor igual o mayor al 10% y menor al 20% de la población.</li> <li>-Afectación en un valor igual o mayor al 10% y menor al 20% del presupuesto anual de seguridad digital.</li> <li>- Afectación leve del medio ambiente requiere de 3 meses a 1 año de recuperación.</li> </ul>	<ul style="list-style-type: none"> <li>-Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros.</li> <li>-Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros.</li> <li>-Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.</li> </ul>
<b>MENOR 40%</b>	<ul style="list-style-type: none"> <li>-Afectación en un valor igual o mayor al 1% y menor al 10% de la población.</li> <li>-Afectación en un valor igual o mayor al 1% y menor al 10% del presupuesto anual de seguridad digital.</li> <li>-Afectación leve del medio ambiente requiere de Afectación leve del medio ambiente requiere de 1 a 3 meses de recuperación.</li> </ul>	<ul style="list-style-type: none"> <li>-Afectación leve de la integridad.</li> <li>-Afectación leve de la disponibilidad.</li> <li>-Afectación leve de la confidencialidad.</li> </ul>
<b>LEVE 20%</b>	<ul style="list-style-type: none"> <li>-Afectación en un valor menor al 1% de la población.</li> <li>-Afectación en un valor menor al 1% del presupuesto anual de seguridad digital.</li> <li>-No hay afectación medio ambiental.</li> </ul>	<ul style="list-style-type: none"> <li>-Sin afectación de la integridad.</li> <li>-Sin afectación de la disponibilidad.</li> <li>-Sin afectación de la confidencialidad.</li> </ul>

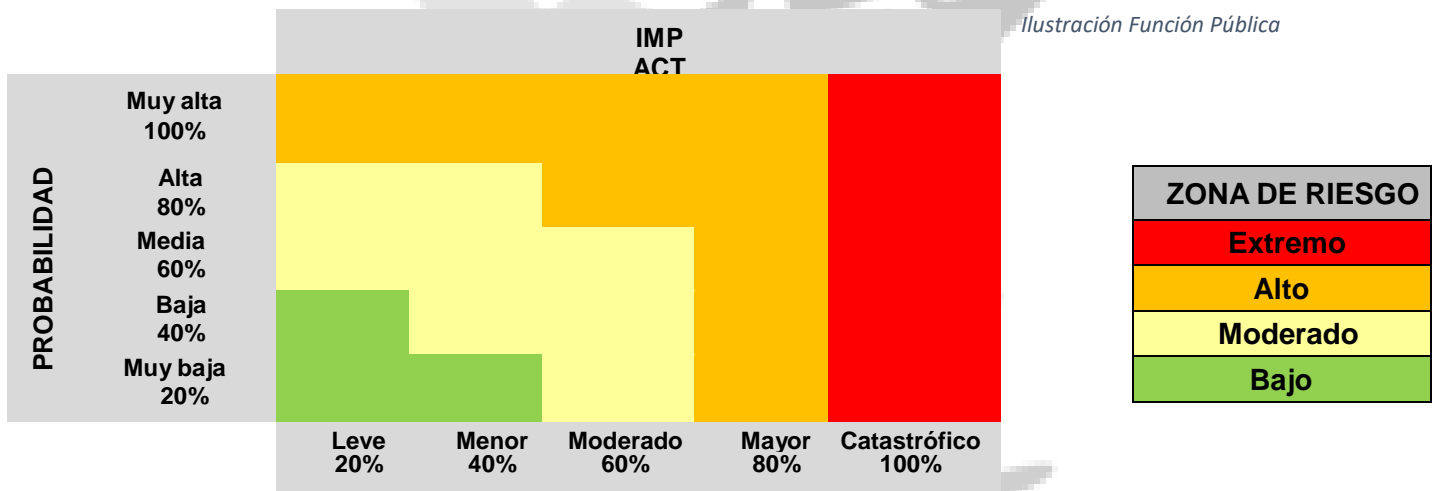
Tabla 9. Criterios para calificar el impacto / consecuencia – RIESGO DE SEGURIDAD DE LA INFORMACION



### 8.3.3 Determinar el nivel de severidad en el mapa de calor

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE). Para establecer el nivel de riesgo inherente (sin aplicación de controles) y residual (con aplicación de controles) se utilizan los Mapas de Calor, que permiten ubicar el riesgo en la zona de acuerdo con la calificación de la probabilidad y el impacto / consecuencia.

Para todos los riesgos de gestión y de seguridad de la información, se definen cuatro zonas de severidad en el mapa de calor como se menciona a continuación;




RIESGO	ACTIVO	AMENAZA	VULNERABILIDAD	PROBABILIDAD	IMPACTO	ZONA DE RIESGO
Pérdida de la Confidencialidad	Base de datos de nómina	Modificación no autorizada	Ausencia de políticas de control de acceso	4-Probable	4- Mayor	Extrema
			Contraseñas sin protección			
			Ausencia de mecanismos de identificación y autenticación de usuarios			
			Ausencia de bloqueo de sesión			

Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. Agosto 2004.

Desp

Extremo	<span style="display:inline-block; width:15px; height:15px; background-color:red;"></span>
Alto	<span style="display:inline-block; width:15px; height:15px; background-color:orange;"></span>
Moderado	<span style="display:inline-block; width:15px; height:15px; background-color:yellow;"></span>
Bajo	<span style="display:inline-block; width:15px; height:15px; background-color:green;"></span>

**IMPORTANTE:**  
La probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

### 8.3.4 Controles asociados a la seguridad de la información

Las entidades públicas podrán mitigar/tratar los riesgos de seguridad de la información empleando como mínimo los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el anexo 4. “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, siempre y cuando se ajusten al análisis de riesgos.

Acorde con el control seleccionado, será necesario considerar las características de diseño y ejecución definidas para su valoración.

A continuación, se incluyen algunos ejemplos de controles y los dominios a los que pertenecen, la lista completa se encuentra en del documento maestro del modelo de seguridad y privacidad de la información (MSPI):

Controles para riesgos de seguridad de la información

Procedimientos operacionales y responsabilidades	Objetivo: asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información
Procedimientos de operación documentados	Control: los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
Gestión de cambios	Control: se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
Gestión de capacidad	Control: para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, llevar a cabo los ajustes y las proyecciones de los requisitos sobre la capacidad futura.
Separación de los ambientes de desarrollo, pruebas y operación	Control: se deberían separar los ambientes de desarrollo, prueba y operación para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
Protección contra códigos maliciosos	Objetivo: asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
Controles contra códigos maliciosos	Control: se deberían implementar controles de detección, prevención y recuperación, combinados con la toma de conciencia apropiada por parte de los usuarios para protegerse contra códigos maliciosos.

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila



<b>Copias de respaldo</b>	Objetivo: proteger la información contra la pérdida de datos.
<b>Respaldo de información</b>	Control: se deberían hacer copias de respaldo de la información, del <i>software</i> y de las imágenes de los sistemas, ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.


Fuente: Ministerio de Tecnologías de la Información y Comunicaciones Min TIC 2018.

Figura 24 Formato mapa riesgos seguridad de la información

N.	RIESGO	ACTIVO	TIPO	AMENAZAS	TIPO	PROBABILIDAD	IMPACTO	RIESGO RESIDUAL	OPCIÓN TRATAMIENTO	ACTIVIDAD DE CONTROL	SOPORTE	RESPONSABLE	TIEMPO	INDICADOR
2	<b>Pérdida de la integridad</b>	Base de datos de nómina	Seguridad digital	Modificación no autorizada	Ausencia de políticas de control de acceso	<b>Probable</b>	<b>Menor</b>	<b>Moderado</b>	Reducir	A.9.1.1 Política de control de acceso	Política creada y comunicada	Oficina TI	Tercer trimestre de 2018	<b>EFICACIA:</b> Índice de cumplimiento actividades= (# de actividades cumplidas / # de actividades programadas) x 100  <b>EFFECTIVIDAD:</b> Efectividad del plan de manejo de riesgos= (# de modificaciones no autorizadas)
									Reducir	A.9.4.3 Sistema de gestión de contraseñas	Procedimientos para la gestión y protección de contraseñas	Oficina TI	Tercer trimestre de 2018	
									Reducir	A 9.4.2 Procedimiento de ingreso seguro	Procedimiento para ingreso seguro	Oficina TI	Tercer trimestre de 2018	
									Reducir	A.11.2.8 Equipos de usuario desatendidos	Configuraciones para bloqueo automático de sesión	Oficina TI	Tercer trimestre de 2018	

\*En este ejemplo el responsable de las actividades de control fue la Oficina de TI, sin embargo existen actividades para el área de personal, recursos físicos o cada oficina en particular. El análisis de riesgos determinará los controles y los responsables en cada caso.




	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

### Herramienta para la gestión de los riesgos de Seguridad Digital:

Herramienta en Excel, que incluye 11 hojas, así:


1. Hoja # 1: METODOLOGÍA ESTABLECIDA, no se diligencia, solo para tener en cuenta para la gestión de los Riesgos de Seguridad Digital”.
2. Hoja # 2: Mapa de Riesgos de Riesgos de Seguridad Digital. No requiere diligenciamiento, porque ésta se genera automáticamente de la Hoja # 3, mientras no se dañen los link automáticos.
3. Hoja # 3: MATRIZ DE IDENTIFICACIÓN, VALORACIÓN, TRATAMIENTO Y SEGUIMIENTO DE RIESGOS SEGURIDAD DIGITAL. Es la hoja de trabajo, que enlaza las otras hojas.
4. Hoja # 4. ANÁLISIS DEL CONTEXTO PARA LA ADMINISTRACIÓN DE LOS RIESGOS DE SEGURIDAD DIGITAL. Permite realizar el análisis de contexto interno, externo y de proceso. Así mismo identificar OPORTUNIDADES asociadas a riesgos de corrupción.
5. Hoja # 5 CRITERIOS PARA IDENTIFICAR LA CRITICIDAD DE LOS ACTIVOS DE SEGURIDAD DIGITAL
6. Hoja # 6: CRITERIOS PARA VALORAR RIESGOS DE SEGURIDAD DIGITAL. Tenerlos en cuenta
7. Hoja # 7: CRITERIOS DE ANÁLISIS (PROBABILIDAD E IMPACTO), PARA VALORAR RIESGOS DE SEGURIDAD DIGITAL. Aplicar estos criterios, según corresponda Tabla 1 y tabla 2.
8. Hoja # 8: EVALUACIÓN DE CONTROLES PARA RIESGOS DE SEGURIDAD DIGITAL. Diligencia esta hoja, según causas vs controles establecidos y efectuar la evaluación según tabla. Estos resultados pasan automáticamente a la hoja # 3.
9. Hoja # 9 LISTA DE CONTROLES según el Anexo A de la ISO 27001:2013
10. Hoja # 10. CRITERIOS RIESGO RESIDUAL. Esta hoja incluye 2 pasos automáticos con fórmulas preestablecidas y un paso 3 que debe ser tenido en cuenta para determinar el riesgo residual, según desplazamientos establecidos.
11. Hoja # 11. MATRIZ DE TRAZABILIDAD RIESGOS DE SEGURIDAD DIGITAL. Permite llevar la trazabilidad del comportamiento de los riesgos de Seguridad digital, año a año, con el fin de generar los análisis respectivos.




	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

## 9. DEFINICIONES


- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **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:** Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sea posible el logro de los objetivos de la entidad.
- **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** Causa principal o básica, correspondiente a las razones por las cuales se puede presentar el riesgo.
- **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

- **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:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo y su magnitud o ambos son aceptables o tolerables.
- **Factores de riesgo:** Son las fuentes generadoras de riesgos.
- **Gestión del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.
- **Identificación del riesgo:** Proceso de análisis para encontrar una potencial desviación de los objetivos.
- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Integridad:** Propiedad de exactitud y completitud.<sup>5</sup>
- **Mapa de calor:** Plano en el que se presentan simultáneamente las escalas de medición de impacto y de 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, administrado por la Oficina Asesora de Planeación o quien haga sus veces.
- **Materialización del Riesgo:** Ocurrencia o desarrollo del riesgo

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional del alcanzar los objetivos.
- **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:** Se entiende como la posibilidad de ocurrencia del riesgo. se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Puntos de Riesgo:** Son actividades dentro del flujo del proceso donde existe evidencia o se tiene indicios que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo
- **Riesgo:** Efecto que causa sobre los objetivos de las entidades, debido a eventos potenciales.  
**Nota:** Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, falla o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo 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 deshonesto o engañosa.

	POLITICA	CODIGO	PA-GSC-PO04
	<b>POLÍTICA Y METODOLOGIA PARA LA ADMINISTRACIÓN DE LOS RIEGOS DE GESTION, CORRUPCION Y SEGURIDAD DIGITAL</b>	VERSIÓN	01
		VIGENCIA	OCTUBRE 2020

- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC27000).
- **Riesgo inherente:** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Severidad:** Nivel de un riesgo, dado por una probabilidad y un impacto. En cada nivel se define el tratamiento y los niveles de responsabilidad.
- **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.

  
**JORGE GARCIA QUIROGA**  
 Director



Proyecto. Esperanza Patricia Ausique Ramirez

Carrera 18 Calle 17 esquina Unidad Deportiva-Sede Administrativa  
 Despacho 875 04 31- 875 04 23 – 875 04 39 [www.inderhuila.gov.co](http://www.inderhuila.gov.co) - [atencionusuario@inderhuila.gov.co](mailto:atencionusuario@inderhuila.gov.co)  
 Neiva-Huila