

# CÁMARA DE REPRESENTANTES

## PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026.

OFICINA DE PLANEACIÓN Y SISTEMAS  
BOGOTÁ



**LA CÁMARA**  
*Se Transforma*

	<b>CÁMARA DE REPRESENTANTES</b> <b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>						
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE</b> <b>SEGURIDAD Y PRIVACIDAD DE LA</b> <b>INFORMACIÓN</b>						
	SUBPROCESO: 3GTIS2 PROCESO: 3GTI	<table border="1"> <tr> <td colspan="2">Código: 3-GTI-S2-PI-1</td> </tr> <tr> <td>Versión : 5</td> <td>Pág.: 2 de 16</td> </tr> <tr> <td colspan="2">Vigente desde: 27/04/2026</td> </tr> </table>	Código: 3-GTI-S2-PI-1		Versión : 5	Pág.: 2 de 16	Vigente desde: 27/04/2026
Código: 3-GTI-S2-PI-1							
Versión : 5	Pág.: 2 de 16						
Vigente desde: 27/04/2026							

## TABLA DE CONTENIDO

1. OBJETIVOS.....	4
1.1 OBJETIVO GENERAL .....	4
1.2 OBJETIVOS ESPECÍFICOS .....	4
2. ALCANCE .....	7
3. MARCO LEGAL .....	7
4. TÉRMINOS Y DEFINICIONES .....	10
5. LINEAMIENTOS DEL PLAN .....	12
6. PLAN DE TRATAMIENTO DE RIESGOS.....	13
7. SEGUIMIENTO Y EVALUACIÓN DEL PLAN.....	15
8. CONTROL DE CAMBIOS.....	16

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA CÁMARA DE REPRESENTANTES</p>	<b>CÁMARA DE REPRESENTANTES</b> <b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> SUBPROCESO: 3GTIS2 PROCESO: 3GTI	
	Código: 3-GTI-S2-PT-5 Versión : 5	Pág.: 3 de <b>16</b> Vigente desde: 28/05/2026

## 1. INTRODUCCIÓN

El entorno digital ha transformado significativamente la manera en que se desarrollan las actividades sociales, económicas e institucionales, incrementando tanto las oportunidades como los riesgos asociados al tratamiento e intercambio de información. Este escenario ha propiciado un aumento en las amenazas cibernéticas que enfrentan las organizaciones, derivadas del aprovechamiento de vulnerabilidades tecnológicas, humanas y operativas por parte de actores malintencionados. En este contexto, resulta fundamental fortalecer la seguridad digital mediante la implementación de medidas orientadas a la gestión adecuada de los riesgos, el fortalecimiento de los controles y la capacidad de respuesta frente a amenazas emergentes.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Cámara de Representantes se encuentra alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) y con la NTC ISO/IEC 27001:2022, constituyéndose como un instrumento estratégico orientado a fortalecer una cultura preventiva y de mejora continua en materia de seguridad y privacidad de la información. El plan prioriza acciones para la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de riesgos, en coherencia con las necesidades institucionales y el entorno digital en constante evolución.

Para la vigencia 2026, el plan incorpora un enfoque alineado con la Política de Gobierno Digital, priorizando la seguridad y privacidad desde el diseño, el fortalecimiento de controles sobre identidades y accesos, la gestión de vulnerabilidades y terceros, así como la protección de la información en iniciativas de interoperabilidad y servicios ciudadanos digitales.

Asimismo, el plan se articula con los objetivos estratégicos de la Cámara de Representantes, contribuyendo al fortalecimiento de la transformación digital, la protección de los activos de información y el cumplimiento de las disposiciones normativas aplicables. De esta manera, se promueve una gestión integral del riesgo que permita fortalecer la continuidad operativa y la confianza en el uso seguro de las tecnologías de la información.

Con este enfoque, la Cámara de Representantes reafirma su compromiso con la protección de la información institucional y establece un marco de actuación orientado a fortalecer la gestión de riesgos, la implementación de controles y la capacidad institucional para responder de manera oportuna frente a las amenazas y desafíos del entorno digital actual.

	<b>CÁMARA DE REPRESENTANTES</b>	
	<b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	
	SUBPROCESO: 3GTIS2 PROCESO: 3GTI	
	Código: 3-GTI-S2-PI-1	
	Versión : 5	Pág.: 4 de 16
	Vigente desde: 27/04/2026	


## 1. OBJETIVOS

### 1.1 OBJETIVO GENERAL

Establecer un marco estratégico para identificar, valorar, tratar y monitorear los riesgos asociados a la seguridad y privacidad de la información en la Cámara de Representantes, orientado a fortalecer la protección de los activos de información, apoyar la continuidad operativa y contribuir a la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), en alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la NTC ISO/IEC 27001:2022.

### 1.2 OBJETIVOS ESPECÍFICOS

- Identificar y clasificar los activos de información relevantes para el tratamiento de riesgos, aplicando los principios de confidencialidad, integridad y disponibilidad.
- Valorar y priorizar los riesgos asociados a la seguridad y privacidad de la información, considerando su impacto potencial en los objetivos institucionales.
- Definir y ejecutar acciones de tratamiento orientadas a mitigar, transferir, evitar o aceptar los riesgos de seguridad identificados, conforme a los criterios establecidos.
- Orientar la aplicación de controles preventivos y correctivos que contribuyan a la protección de los sistemas, datos y procesos estratégicos de la entidad.
- Realizar el seguimiento a los riesgos y a las acciones de tratamiento definidas, como insumo para la mejora continua.
- Promover una cultura de seguridad de la información mediante actividades de sensibilización y capacitación dirigidas a colaboradores y terceros que interactúan con los sistemas y activos de información

	<b>CÁMARA DE REPRESENTANTES</b> <b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> SUBPROCESO: 3GTIS2 PROCESO: 3GTI	
	Código: 3-GTI-S2-PT-5	Versión : 5
	Pág.: 7 de 16	Vigente desde: 27/04/2026

## 2. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026 aplica a la totalidad de los procesos, sistemas, servicios y activos de información gestionados por la Cámara de Representantes, incluyendo los recursos tecnológicos, humanos y físicos involucrados en su protección.

En consecuencia, el plan abarca:


- **Procesos organizacionales:** todos los procesos administrativos, misionales, operativos y estratégicos que generen, recolecten, procesen, almacenen, consulten, transmitan o dispongan información relevante, sensible o crítica para el cumplimiento de los objetivos institucionales.
- **Activos de información:** información en formato físico y digital; bases de datos; aplicaciones; sistemas de información; infraestructura tecnológica; redes; plataformas y servicios (internos o tercerizados); equipos y dispositivos que soportan la operación, continuidad y prestación de servicios de la entidad.
- **Personal y terceros:** servidores públicos, contratistas, proveedores y demás terceros que tengan acceso a la información institucional o participen en su gestión, protección, administración, monitoreo y supervisión, conforme a los niveles de autorización establecidos.
- **Normatividad y estándares aplicables:** cumplimiento de las disposiciones legales y regulatorias vigentes, así como de los lineamientos de Gobierno Digital, la ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI).

El plan se extiende a todas las dependencias de la Cámara de Representantes y tiene como finalidad fortalecer la confidencialidad, integridad, disponibilidad y accesibilidad de la información, mediante un enfoque integral de gestión del riesgo, implementación de controles, seguimiento a su efectividad y mejora continua.

	<b>CÁMARA DE REPRESENTANTES</b>	
	<b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	
	SUBPROCESO: 3GTIS2 PROCESO: 3GTI	
	Código: 3-GTI-S2-PI-1	
	Versión : 5	Pág.: 8 de 16
	Vigente desde: 27/04/2026	

### 3. MARCO LEGAL

NORMA	AÑO	DESCRIPCIÓN
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se actualizan las disposiciones del Decreto 1078 de 2015, relacionado con el sector de Tecnologías de la Información y las Comunicaciones.
Ley 1266	2008	Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de información contenida en bases de datos personales, especialmente en los sectores financiero, crediticio y comercial.
Ley 1273	2009	Por la cual se modifica el Código Penal, se crea el bien jurídico "Protección de la Información y los Datos" y se establecen sanciones para quienes vulneren la seguridad de los sistemas de información.
Ley 1581	2012	Ley General de Protección de Datos Personales, que regula el tratamiento y la protección de datos personales en Colombia.
Ley 1712	2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública, que regula el acceso y la divulgación de información pública nacional.
MSPI (Modelo de Seguridad y Privacidad de la Información)	2025	Modelo de Seguridad y Privacidad de la Información del Ministerio TIC (MSPI), actualizado mediante la Resolución 02277 de 2025. Establece principios, controles y directrices para gestionar la seguridad y privacidad de la información en entidades públicas, articulado con la Política de Gobierno Digital.
Ley 1474	2011	Ley Anticorrupción, que establece mecanismos para prevenir, investigar y sancionar actos de corrupción, incluyendo disposiciones relacionadas con la gestión pública.
MGRSD	2018	Modelo Nacional de Gestión de Riesgos de Seguridad Digital, que establece lineamientos para gestionar riesgos relacionados con la seguridad digital en entidades públicas.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA CÁMARA DE REPRESENTANTES</p>	<b>CÁMARA DE REPRESENTANTES</b>		
	<b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>		
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>		Código: 3-GTI-S2-PT-5
	SUBPROCESO: 3GTIS2 PROCESO: 3GTI	Versión : 5	Pág.: 9 de 16
		Vigente desde: 27/04/2026	

Guía para la Gestión Integral del Riesgo en Entidades Públicas (DAFP)	2025	Guía del Departamento Administrativo de la Función Pública (DAFP) que orienta la identificación, análisis, evaluación, tratamiento, seguimiento y comunicación del riesgo en entidades públicas, incluyendo riesgos asociados a seguridad digital y controles.
NTC ISO/IEC 27005	2022	Norma internacional para la Gestión de Riesgos de la Seguridad de la Información, que establece metodologías para identificar y tratar riesgos relacionados con la seguridad de los activos de información.
ISO 31000 para la Gestión de Riesgos	2018	Norma internacional que establece directrices y principios para la gestión integral de riesgos, aplicables a todo tipo de organizaciones.
CONPES 3995	2020	Política Nacional de Confianza y Seguridad Digital, que promueve la gestión de riesgos digitales y la protección de infraestructuras críticas en el país.
NTC ISO/IEC 27001	2022	Norma internacional para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), que establece los requisitos para proteger los activos de información bajo los principios de confidencialidad, integridad y disponibilidad.
Decreto 767	2022	Actualización de los lineamientos de la Política de Gobierno Digital, que fortalece la transformación digital y la inclusión de estándares avanzados de ciberseguridad.
Manual de Gobierno Digital (MinTIC)	2022	Caja de herramientas y lineamientos de implementación de la Política de Gobierno Digital, incluyendo habilitadores, componentes y recomendaciones de seguridad digital para entidades públicas.
Estrategia Nacional Digital de Colombia 2023–2026	2023	Estrategia nacional que orienta la transformación digital del país (2023–2026) y promueve el uso seguro, ético y confiable de la tecnología, fortaleciendo capacidades institucionales y de seguridad digital.
CONPES 4144	2025	Política Nacional de Inteligencia Artificial con visión a 2030. Incluye líneas para gestión de riesgos, gobernanza de datos, y adopción responsable de IA, relevantes para seguridad y privacidad de la información.

	<b>CÁMARA DE REPRESENTANTES</b>	
	<b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	
	SUBPROCESO: 3GTIS2 PROCESO: 3GTI	
	Código: 3-GTI-S2-PI-1	
	Versión : 5	Pág.: 10 de 16
	Vigente desde: 27/04/2026	

#### 4. TÉRMINOS Y DEFINICIONES

- **Aceptar el Riesgo:** Decisión informada de no implementar medidas adicionales para modificar la probabilidad o el impacto de un riesgo, considerando que este se encuentra dentro de los niveles aceptables establecidos por la entidad. *(ISO 31000:2018)*
- **Actividades de Control:** Acciones específicas establecidas a través de políticas y procedimientos que aseguran la implementación de controles diseñados para mitigar los riesgos identificados y garantizar el cumplimiento de los objetivos institucionales. *(Guía para la Administración del Riesgo - DAFP, 2020)*
- **Activo de Información:** Recursos valiosos para la organización, tales como datos, aplicaciones, sistemas, redes, hardware y documentos físicos o digitales, que requieren protección para garantizar la continuidad operativa. *(ISO/IEC 27001:2022)*
- **Amenaza:** Evento o situación potencial que puede explotar una vulnerabilidad y causar un impacto negativo en los activos de información o en los objetivos de la organización. *(ISO/IEC 27005:2022)*
- **Causa:** Factores internos o externos que pueden desencadenar la materialización de un riesgo. *(ISO 31000:2018)*
- **Compartir el Riesgo:** Transferencia parcial del riesgo a un tercero, como aseguradoras o proveedores, mediante contratos o acuerdos formales. *(ISO 31000:2018)*
- **Consecuencia:** Efectos o impactos negativos derivados de la materialización de un riesgo que afectan los procesos, objetivos o la reputación de la organización. *(ISO 31000:2018)*
- **Control:** Medida implementada para modificar el riesgo, como políticas, procedimientos, tecnologías o prácticas específicas. *(ISO/IEC 27001:2022)*
- **Control Preventivo:** Diseñado para evitar la ocurrencia de eventos no deseados que puedan materializar un riesgo. *(Guía de Gestión de Riesgos de Seguridad Digital - MINTIC, 2018)*
- **Control Detectivo:** Diseñado para identificar eventos no previstos después de que estos hayan ocurrido, permitiendo su corrección y mitigación. *(ISO/IEC 27001:2022)*

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA CÁMARA DE REPRESENTANTES</p>	<b>CÁMARA DE REPRESENTANTES</b> <b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	
	SUBPROCESO: 3GTIS2 PROCESO: 3GTI	
	Código: 3-GTI-S2-PT-5	Versión : 5
		Vigente desde: 27/04/2026

- **Evitar el Riesgo:** Decisión de no iniciar o continuar actividades que puedan dar lugar a un riesgo identificado. *(ISO 31000:2018)*
- **Gestión de Riesgos:** Proceso continuo y sistemático para identificar, analizar, evaluar y tratar riesgos, con el objetivo de garantizar el cumplimiento de los objetivos estratégicos de la entidad. *(ISO 31000:2018)*
- **Impacto:** Consecuencias que la materialización de un riesgo puede tener sobre los activos de información, procesos u objetivos organizacionales. *(ISO/IEC 27005:2022)*
- **Mapa de Riesgos:** Documento que consolida los riesgos identificados, su valoración, controles asociados y estrategias de tratamiento. *(Guía para la Administración del Riesgo - DAFP, 2020)*
- **Monitorear:** Supervisar y registrar las actividades relacionadas con los riesgos, con el fin de identificar cambios y ajustar controles o estrategias. *(ISO 31000:2018)*
- **Política de Administración de Riesgos:** Declaración oficial de la dirección que establece los lineamientos y directrices para la gestión integral de riesgos en la organización. *(ISO 31000:2018)*
- **Probabilidad:** Medida que refleja la posibilidad de que ocurra un evento riesgoso, evaluada mediante análisis cualitativos o cuantitativos. *(ISO/IEC 27005:2022)*
- **Reducir el Riesgo:** Implementación de medidas para disminuir la probabilidad, impacto o ambos, a niveles aceptables. *(ISO 31000:2018)*
- **Riesgo de Seguridad Digital:** Combinación de amenazas y vulnerabilidades en el entorno digital que puede comprometer la confidencialidad, integridad y disponibilidad de los activos de información. *(Guía de Gestión de Riesgos de Seguridad Digital - MINTIC, 2018)*
- **Riesgo Inherente:** Riesgo existente antes de la implementación de controles o medidas de mitigación. *(ISO/IEC 27005:2022)*.
- **Riesgo Residual:** Riesgo que permanece después de aplicar controles o medidas de tratamiento. *(ISO/IEC 27001:2022)*
- **Vulnerabilidad:** Debilidad o falla en un activo de información, sistema o proceso que puede ser

	<b>CÁMARA DE REPRESENTANTES</b>	
	<b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	
	SUBPROCESO: 3GTIS2 PROCESO: 3GTI	
	Código: 3-GTI-S2-PI-1	
	Versión : 5	Pág.: 12 de 16
	Vigente desde: 27/04/2026	

explotada por una amenaza para causar un impacto negativo. (ISO/IEC 27005:2022)

## 5. LINEAMIENTOS DEL PLAN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se basa en principios claros de gestión que aseguran la asignación de responsabilidades, la ejecución efectiva de las acciones y el monitoreo constante de los riesgos. Estos lineamientos se estructuran bajo el Modelo de Líneas de Defensa, promovido por el Departamento Administrativo de la Función Pública (DAFP), y aprobado por el Comité Institucional de Coordinación de Control Interno de la Cámara de Representantes.

### Responsables y Roles

#### 1. Línea Estratégica (Alta Dirección y Coordinación de Control Interno):

- Definir y aprobar la política para la administración de riesgos.
- Analizar riesgos institucionales que puedan afectar los objetivos estratégicos.
- Monitorear el cumplimiento de la política de riesgos y garantizar la alineación con los objetivos organizacionales.

#### 2. Primera Línea de Defensa (Oficina de Planeación y Sistemas y líderes de proceso):

- Identificar, analizar y documentar los riesgos en los procesos, proyectos y programas a su cargo.
- Establecer controles y actividades de mitigación, evaluando su eficacia de manera continua.
- Reportar a la Segunda Línea de Defensa los riesgos identificados, los cambios que generen nuevos riesgos y los resultados de las acciones implementadas.

#### 3. Segunda Línea de Defensa (Supervisores, Interventores y Coordinadores de Sistemas de Gestión):

- Asesorar y acompañar a la Primera Línea de Defensa en la identificación y valoración de riesgos.
- Monitorear los riesgos identificados y los controles implementados, proponiendo mejoras.
- Consolidar la información de riesgos y elaborar reportes para la Línea Estratégica.

#### 4. Tercera Línea de Defensa (Oficina de Control Interno):

- Supervisar de manera independiente la efectividad de la gestión de riesgos y los controles.

 <p>CONGRESO DE LA REPÚBLICA DE COLOMBIA CÁMARA DE REPRESENTANTES</p>	<b>CÁMARA DE REPRESENTANTES</b> <b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> SUBPROCESO: 3GTIS2 PROCESO: 3GTI	
	Código: 3-GTI-S2-PT-5 Versión : 5	Pág.: 13 de <b>16</b> Vigente desde: 27/04/2026

- Realizar auditorías periódicas y emitir recomendaciones para fortalecer las acciones del plan.
- Proporcionar aseguramiento sobre la pertinencia y eficacia de las políticas y controles implementados.

### Responsabilidades Clave

#### 1. Oficina de Planeación y Sistemas:

- Brindar asesoría a la Primera Línea de Defensa en la identificación y monitoreo de los riesgos.
- Liderar la consolidación del **Mapa de Riesgos Institucional** y garantizar su actualización.
- Coordinar la elaboración de reportes para la Oficina de Control Interno y el Comité Institucional.

#### 2. Líderes de Procesos (Primera Línea de Defensa):

- Documentar los riesgos, sus controles y las actividades de tratamiento.
- Evaluar periódicamente el contexto estratégico y los riesgos asociados a sus procesos.
- Implementar acciones correctivas y preventivas para garantizar la mejora continua.
- 

#### 3. Oficina de Control Interno:

- Realizar auditorías independientes para evaluar la efectividad de las acciones del plan.
- Emitir recomendaciones para fortalecer las políticas de administración de riesgos.
- Garantizar la retroalimentación continua al Comité Institucional sobre el estado de los riesgos.

### Alineación Estratégica

Estos lineamientos aseguran la articulación entre las políticas de administración de riesgos, las funciones institucionales y los objetivos estratégicos, promoviendo una cultura organizacional orientada a la protección de los activos de información y la mejora continua.

## 6. PLAN DE TRATAMIENTO DE RIESGOS

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Cámara de Representantes define las acciones estratégicas necesarias para gestionar los riesgos identificados, asegurando su mitigación, monitoreo y evaluación continua. Este plan está alineado con los objetivos institucionales, garantizando la protección de los activos de información, el cumplimiento de

	<b>CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	
	SUBPROCESO: 3GTIS2 PROCESO: 3GTI	Código: 3-GTI-S2-PI-1 Versión : 5      Pág.: 14 de 16 Vigente desde: 27/04/2026

normativas aplicables y la mejora continua en la seguridad de la información. A través de la implementación de políticas, procedimientos y controles específicos, se busca minimizar los impactos potenciales de los riesgos y fortalecer la resiliencia organizacional frente a las amenazas emergentes.

Acción Estratégica	Descripción	Responsable	Resultados Esperados	Porcentaje de Cumplimiento Esperado	Fecha de Implementación	
					Inicial	Final
<b>Identificación, análisis y valoración de riesgos de seguridad y privacidad de la información</b>	Revisar y actualizar la identificación, análisis y valoración de riesgos conforme a la metodología definida por el MSPI, considerando riesgos tecnológicos, organizacionales y asociados a terceros.	Oficina de Planeación y Sistemas	Mapa de riesgos actualizado; riesgos priorizados conforme a criterios definidos.	75%	01/06/2026	31/12/2026
<b>Definición de opciones de tratamiento para riesgos no aceptables</b>	Definir opciones de tratamiento para los riesgos que superan el nivel de aceptación, considerando medidas organizacionales, técnicas o administrativas, así como responsables y plazos.	Oficial de Seguridad de la Información / Líderes de Proceso	Opciones de tratamiento definidas y documentadas para los riesgos priorizados.	75%	01/09/2026	31/12/2026

	<b>CÁMARA DE REPRESENTANTES</b>	
	<b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	
	SUBPROCESO: 3GTIS2 PROCESO: 3GTI	
	Código: 3-GTI-S2-PT-5	
	Versión : 5	Pág.: 15 de 16
	Vigente desde: 27/04/2026	

<b>Definición y documentación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</b>	Consolidar y documentar el Plan de Tratamiento de Riesgos, integrando los riesgos priorizados, las opciones de tratamiento definidas, los responsables y los plazos, como parte del proceso institucional de gestión del riesgo.	Oficial de Seguridad de la Información	Plan de Tratamiento de Riesgos documentado y disponible para su aplicación institucional .	75%	01/10/2026	31/12/2026
<b>Sensibilización sobre gestión de riesgos de seguridad de la información</b>	Desarrollar actividades de sensibilización orientadas a fortalecer el conocimiento institucional sobre la gestión de riesgos y las responsabilidades asociadas.	Seguridad de la Información	Actividades de sensibilización realizadas; registro de participación.	75%	01/02/2026	31/12/2026


## 7. SEGUIMIENTO Y EVALUACIÓN DEL PLAN

Para la vigencia 2026, el seguimiento y evaluación del plan se realizará de manera continua y documentada, con reportes trimestrales de avance y una revisión integral semestral del estado de los riesgos y la eficacia de los controles.


	<b>CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	
	SUBPROCESO: 3GTIS2 PROCESO: 3GTI	Código: 3-GTI-S2-PI-1 Versión : 5      Pág.: 16 de 16 Vigente desde: 27/04/2026

## 8. CONTROL DE CAMBIOS

REVISIONES DEL DOCUMENTO				
Ver sió n	Fecha	Proyectado por	Descripción	Aprobado por
1.0	08/10/2021	Ing. Carlos Manuel Gómez Damián	Creación del Documento	<b>Oficina de Planeación y Sistemas</b> Dr. Juan José Gómez Vélez – Jefe OPS Revisión Técnica: Ing. Alejandro Muñoz Sandoval Aprobado en el Comité Institucional de Gestión y Desempeño, mediante Acta No. 3 del 16 de Diciembre de 2021.
2.0	15/12/2022	Oficina de Planeación y Sistemas	Ajustes al documento	<b>Oficina de Planeación y Sistemas</b> Dr. Andrés Francisco Lozano Campos – Jefe OPS Revisión y ajustes: Ing. Alejandro Muñoz Sandoval Aprobado en el Comité Institucional de Gestión y Desempeño, mediante Acta No. 01 del 31 de Enero de 2023.

	<b>CÁMARA DE REPRESENTANTES</b>	
	<b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	
SUBPROCESO: 3GTIS2	Código: 3-GTI-S2-PT-5	Versión : 5
PROCESO: 3GTI		Pág.: 17 de 16
		Vigente desde: 27/04/2026

3.0	20/01/2024	Oficina de Planeación y Sistemas	Ajustes al documento	<b>Oficina de Planeación y Sistemas</b> Dr. Jorge Edison Castro— Jefe ( E ) OPS Revisión y ajustes: Ing. Daniela Andrade Muñoz Ing. Juan David Acosta Jiménez Aprobado en el Comité Institucional de Gestión y Desempeño, mediante Acta No. 01 del 31 de Enero de 2024.
4.0	27/01/2025	Oficina de Planeación y Sistemas	Revisión integral del documento alineado a normativas actualizadas como ISO/IEC 27001:2022 y MSPI. Incorporación de ajustes en alcance, marco normativo, lineamientos del plan y tratamiento de riesgos. Actualización de términos y definiciones para reflejar conceptos actualizados en la gestión de riesgos.	<b>Oficina de Planeación y Sistemas</b> Dr. Jorge Edison Castro— Jefe ( E ) OPS Revisión y ajustes: Ing. Daniela Andrade Juan David Acosta Aprobado en el Comité Institucional de Gestión y Desempeño, mediante Acta No. 01 del 31 de Enero de 2024.
5.0	28/05/2026	Oficina de Planeación y Sistemas	Actualización de vigencia 2026. Ajustes al marco legal (MSPI, Guía DAFP v7, Manual de Gobierno Digital, END 2023—	<b>Oficina de Planeación y Sistemas</b> Ing. Jorge Edison Castro - Jefe Revisión Técnica:


	<b>CÁMARA DE REPRESENTANTES</b>	
	<b>OFICINA DE PLANEACIÓN Y SISTEMAS</b>	
	<b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	
SUBPROCESO: 3GTIS2 PROCESO: 3GTI	Código: 3-GTI-S2-PI-1	Versión : 5
		Pág.: 18 de 16
		Vigente desde: 27/04/2026

			2026, CONPES 4144). Refuerzo de lineamientos del plan de tratamiento para soportar Gobierno Digital: servicios ciudadanos digitales, interoperabilidad, gestión de datos y ciberseguridad. Ajustes de seguimiento con indicadores/KPI y periodicidad de reporte.	Ing. Daniela Andrade Ing. Elkin Rojas Roa Ing. Fabian Lizarazo Aprobación: Comité Institucional de Gestión y Desempeño 28/05/2026
--	--	--	--	--

**JORGE EDISON CASTRO SALCEDO**

Jefe Oficina de Planeación y Sistemas

Cámara de Representantes

Revisión: Ing. Daniela Andrade cps\_0529\_2026 

Ing. Elkin Rojas Roa cps\_0384\_2026

Ing. Fabian Lizarazo 