

CÁMARA DE REPRESENTANTES

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

OFICINA DE PLANEACIÓN Y SISTEMAS
BOGOTÁ



LA CÁMARA
Se Transforma

	CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS	
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 3-GTI-S2-PT-5
		Versión: 2 Pág.: 2 de 11
		Vigente desde: 28/05/2026

ÍNDICE DE CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVOS	3
2.1. OBJETIVO GENERAL	3
2.2. OBJETIVOS ESPECÍFICOS	3
3. NORMATIVIDAD	4
4. ALCANCE Y ÁMBITO DE APLICACIÓN	5
5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	5
5.1. LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN	5
6. REVISIÓN	6
7. DIVULGACIÓN Y CULTURA EN SEGURIDAD	6
8. ROLES Y RESPONSABILIDADES	7
9. INCUMPLIMIENTO DE LA POLÍTICA	10
10. REFERENCIAS	10
11. ANEXOS	11
12. CONTROL DE CAMBIOS	11

	CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS	
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 3-GTI-S2-PT-5
		Versión: 2 Pág.: 3 de 11 Vigente desde: 28/05/2026

1. INTRODUCCIÓN

La información constituye uno de los activos más relevantes de la Cámara de Representantes, en la medida en que soporta el cumplimiento de sus funciones constitucionales, legales y administrativas, así como la operación y gestión de sus procesos institucionales.

En atención a su valor, la Alta Dirección reconoce la necesidad de establecer lineamientos orientados a su protección, frente a amenazas y riesgos que puedan afectar su confidencialidad, integridad y disponibilidad.

En este contexto, la Cámara de Representantes adopta la presente Política de Seguridad y Privacidad de la Información como marco general para orientar la gestión de la seguridad y privacidad de la información, en coherencia con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y con los requisitos de la ISO/IEC 27001:2022.

La presente política tiene como propósito fortalecer el Sistema de Gestión de Seguridad de la Información de la Entidad, orientar la gestión de los riesgos de seguridad y privacidad de la información, promover la implementación de controles y consolidar una cultura institucional orientada a la protección de la información.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

Establecer los lineamientos generales para fortalecer la seguridad y privacidad de la información en la Cámara de Representantes, en coherencia con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), mediante la gestión integral de riesgos, la implementación de controles y el desarrollo de capacidades institucionales que permitan proteger la información y promover una cultura organizacional de seguridad y privacidad de la información.

2.2. OBJETIVOS ESPECÍFICOS

- Actualizar y fortalecer la gestión de la seguridad y privacidad de la información en la Cámara de Representantes, de acuerdo con los componentes definidos en el MSPI.
- Fortalecer la gestión institucional de riesgos de seguridad de la información en la Cámara de Representantes, de acuerdo con el MSPI, a fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información, procesos y servicios institucionales.

	CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS		
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		Código: 3-GTI-S2-PT-5
			Versión: 2
			Pág.: 4 de 11
			Vigente desde: 28/05/2026

- Fortalecer la cultura institucional de seguridad y privacidad de la información en la Cámara de Representantes, mediante estrategias de sensibilización, capacitación y apropiación de buenas prácticas, con el fin de prevenir incidentes y proteger la información institucional.

3. NORMATIVIDAD

NORMA	AÑO	DESCRIPCIÓN
Ley 1150	2007	Seguridad de la información electrónica en contratación en línea.
Ley 1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341	2009	Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Ley 1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Decreto 4632 de 2011 Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712	2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 1755	2015	Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Título II Capítulo I.
Ley 1928	2018	Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”.
Conpes 3854	2016	Política Nacional de Seguridad Digital
Decreto 1074	2015	Decreto Único del Sector Comercio, Industria y Turismo (protección de datos personales y fin
Decreto 1081	2015	Decreto Reglamentario Único del Sector Presidencia de la República Libro 2 título 1. Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional.
Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

	CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS	
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 3-GTI-S2-PT-5
		Versión: 2 Pág.: 5 de 11 Vigente desde: 28/05/2026

Decreto 1499	2017	Por medio del cual se modifica el Decreto número 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión
Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital
Resolución 02277	2025	Por la cual el Ministerio TIC actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI) y su anexo técnico, aplicable a las entidades públicas del orden nacional.
NTC ISO/IEC 27001	2022	Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

4. ALCANCE Y ÁMBITO DE APLICACIÓN

La presente Política de Seguridad y Privacidad de la Información aplica a todos los procesos, servicios y dependencias de la Cámara de Representantes, y es de obligatorio cumplimiento para todos los funcionarios, contratistas, proveedores y terceros que, en el desarrollo de sus actividades, accedan, generen, procesen, almacenen, transmitan o gestionen activos de información de la entidad. Aplica a todos los activos de información, independientemente de su forma, medio o estado, incluyendo aquellos en formato físico y digital, así como a los sistemas de información, infraestructuras tecnológicas y demás activos asociados, en todos los entornos donde estos sean tratados, tanto dentro como fuera de las instalaciones de la entidad, incluyendo servicios tercerizados y plataformas tecnológicas autorizadas.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Cámara de Representantes establece la presente política como marco general para la gestión de la seguridad y privacidad de la información, en el marco del Sistema de Gestión de Seguridad de la Información y en coherencia con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y los requisitos de la ISO/IEC 27001:2022, con el propósito de proteger los activos de información y preservar su confidencialidad, integridad y disponibilidad.

La Alta Dirección y la Oficina de Planeación y Sistemas se comprometen a liderar, implementar, mantener y mejorar de manera continua el Sistema de Gestión de Seguridad de la Información, mediante la asignación de recursos, la gestión de riesgos de seguridad y privacidad de la información, la implementación de controles y el fortalecimiento de la cultura institucional en seguridad de la información.

5.1. LINEAMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

	CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS	
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 3-GTI-S2-PT-5
		Versión: 2 Pág.: 6 de 11 Vigente desde: 28/05/2026

A continuación, se establecen los lineamientos generales de seguridad y privacidad que soportan el Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de la Cámara de Representantes:

- La Cámara de Representantes formaliza, implementa, mantiene y mejora de manera continua su Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de acuerdo con las necesidades de la entidad, sus objetivos institucionales y el cumplimiento de la normatividad vigente, asegurando que la seguridad esté presente durante todo el ciclo de vida de los activos de información y los sistemas de información.
- La Cámara de Representantes identifica y gestiona de manera integral los riesgos de seguridad y privacidad de los activos de información y de la infraestructura tecnológica, orientando su tratamiento a la reducción de impactos y a la protección de los procesos e infraestructuras críticas, con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información.
- La Cámara de Representantes protege los activos de información creados, procesados y transmitidos como parte de sus procesos, mediante la implementación de controles de acceso y controles de operación sobre la información, los sistemas y los recursos de red de la entidad, de acuerdo con su nivel de clasificación y criticidad.
- La Cámara de Representantes promueve el cumplimiento de las obligaciones, responsabilidades, estándares, normativas, directrices legales, regulatorias, contractuales y organizacionales en materia de seguridad y privacidad de la información, así como de los requisitos aplicables a proveedores y terceros.
- La Cámara de Representantes promueve el fortalecimiento de la cultura de seguridad y privacidad de la información en todos los actores involucrados, definiendo roles y responsabilidades, y desarrollando procesos continuos de divulgación, sensibilización y capacitación.
- La Cámara de Representantes asegura la continuidad de los procesos críticos y la disponibilidad de los activos de información ante la materialización de incidentes o riesgos que puedan afectar la operación institucional.

6. REVISIÓN

La presente Política de Seguridad y Privacidad de la Información será revisada al menos una vez al año, o cuando se presenten cambios significativos en el contexto organizacional, normativo o tecnológico que requieran su actualización.

La revisión será liderada por la Oficina de Planeación y Sistemas y presentada al Comité Institucional de Gestión y Desempeño, quien evaluará su pertinencia, eficacia y alineación con los objetivos institucionales, el Sistema de Gestión de Seguridad de la Información y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y la ISO/IEC 27001:2022.

La política deberá ser aprobada por el Comité Institucional de Gestión y Desempeño, mediante el acto administrativo o mecanismo formal definido por la entidad.

	CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS	
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 3-GTI-S2-PT-5
		Versión: 2 Pág.: 7 de 11 Vigente desde: 28/05/2026

7. DIVULGACIÓN Y CULTURA EN SEGURIDAD

La Cámara de Representantes fortalece la generación y fortalecimiento de la cultura en ciberseguridad, seguridad y privacidad de la información. Para ello, se deben tomar iniciativas de divulgación, sensibilización y concientización de manera continuada en toda la entidad (funcionarios, contratistas y terceros) respecto a la importancia de las Políticas de TI y el papel que cumple cada uno en garantizar la ciberseguridad y la protección de los datos. Adicionalmente, la Política de Seguridad y Privacidad de la Información debe ser publicada, socializada y debe estar disponible para las partes interesadas.

8. ROLES Y RESPONSABILIDADES

Rol	Responsabilidades
Alta Dirección	• Liderar y respaldar estratégicamente la implementación, sostenimiento y mejora continua del SGSI. • Aprobar las directrices generales, prioridades estratégicas y recursos requeridos para la gestión de la seguridad y privacidad de la información. • Promover una cultura organizacional basada en la seguridad de la información, la gestión del riesgo y el cumplimiento normativo. • Asegurar que la seguridad de la información esté alineada con los objetivos institucionales, la planeación estratégica y la gestión integral de la entidad.
Comité Institucional de Gestión y Desempeño	• Aprobar los recursos para la implementación y el mantenimiento del sistema de gestión de seguridad de la información. • Vigilar el cumplimiento de la normativa. • Orientar, coordinar y hacer seguimiento a la implementación, operación y mejora continua del SGSI. • Revisar periódicamente el estado de los riesgos, incidentes, vulnerabilidades, controles y planes de tratamiento asociados a la seguridad y privacidad de la información. • Evaluar la eficacia de las políticas, procedimientos, lineamientos y controles implementados. • Recomendar acciones de mejora, priorización de iniciativas y decisiones de tratamiento del riesgo a nivel institucional.

	CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS	
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 3-GTI-S2-PT-5
		Versión: 2 Pág.: 8 de 11 Vigente desde: 28/05/2026

Oficina de Planeación y Sistemas	• Liderar la implementación técnica y operativa del SGSI en articulación con las áreas responsables. • Diseñar, actualizar, administrar y socializar políticas, procedimientos, estándares, guías y demás documentos del marco de seguridad de la información. • Implementar, administrar y fortalecer controles tecnológicos, preventivos, detectivos y correctivos para la protección de los activos de información. • Coordinar actividades de monitoreo, gestión de vulnerabilidades, gestión de incidentes, continuidad tecnológica y protección de la infraestructura tecnológica. • Apoyar la integración de la seguridad de la información en proyectos, servicios, plataformas y procesos tecnológicos de la entidad.
División de Personal	• Incorporar criterios de seguridad de la información en los procesos de vinculación, inducción, reinducción, capacitación, cambios de rol, vacaciones, suspensión y desvinculación del personal. • Asegurar que el personal conozca y acepte sus responsabilidades frente al uso adecuado de la información y los activos institucionales. • Coordinar, junto con las áreas competentes, la ejecución de actividades de sensibilización y fortalecimiento de la cultura de ciberseguridad. • Gestionar, en articulación con las áreas responsables, la aplicación oportuna de controles relacionados con ingreso, permanencia y retiro del personal.
Oficial de Seguridad de la Información	• Liderar la definición, implementación, mantenimiento y mejora continua del marco de seguridad y privacidad de la información de la entidad. • Asesorar a la Alta Dirección, comités y líderes de proceso en la toma de decisiones relacionadas con riesgos, controles, cumplimiento y madurez del SGSI. • Diseñar, actualizar y hacer seguimiento al plan estratégico, planes de trabajo, indicadores, lineamientos, metodologías y mecanismos de control en materia de seguridad de la información. • Coordinar la identificación, análisis, evaluación, tratamiento y seguimiento de riesgos de seguridad y privacidad de la información. • Promover la adopción de controles alineados con el contexto institucional, la normatividad vigente y las buenas prácticas nacionales e internacionales.

	CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS	
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 3-GTI-S2-PT-5
		Versión: 2 Pág.: 9 de 11 Vigente desde: 28/05/2026

	• Realizar seguimiento al cumplimiento de la política de seguridad de la información, reportar desviaciones y proponer acciones correctivas y de mejora. • Articular la gestión de incidentes, concienciación, cumplimiento, clasificación de activos y demás componentes del SGSI con los procesos institucionales.
Líderes de proceso, jefes de área y propietarios de la información	• Implementar y asegurar el cumplimiento de las políticas, lineamientos, procedimientos y controles de seguridad de la información dentro de sus procesos o áreas de responsabilidad. • Identificar, inventariar, clasificar, custodiar y revisar periódicamente la información y los activos asociados a su proceso, de acuerdo con su nivel de criticidad. • Definir y validar necesidades de acceso a la información, garantizando la aplicación de los principios de mínimo privilegio, necesidad de saber y segregación de funciones. • Gestionar los riesgos de seguridad y privacidad asociados a sus procesos, apoyar la definición de controles y hacer seguimiento a los planes de tratamiento. • Reportar incidentes, debilidades de control y situaciones que puedan comprometer la seguridad de la información.
Usuarios de la información / funcionarios y contratistas	• Cumplir integralmente las políticas, procedimientos, lineamientos y controles de seguridad de la información definidos por la entidad. • Usar de manera responsable, segura y ética la información, los sistemas de información, los recursos tecnológicos y los servicios institucionales. • Proteger las credenciales de acceso, evitar prácticas inseguras y reportar oportunamente incidentes, eventos sospechosos o incumplimientos. • Participar en actividades de capacitación, sensibilización y fortalecimiento de la cultura de seguridad de la información. • Apoyar, cuando corresponda, actividades de identificación de activos, valoración de riesgos e implementación de controles en sus procesos.

	CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS	
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Código: 3-GTI-S2-PT-5
		Versión: 2 Pág.: 10 de 11 Vigente desde: 28/05/2026

Proveedores y terceros	• Cumplir las obligaciones contractuales, requisitos de seguridad de la información, acuerdos de confidencialidad, niveles de servicio y controles establecidos por la entidad. • Implementar las medidas técnicas, administrativas y organizativas necesarias para proteger la información institucional a la que accedan, procesen, almacenen o transmitan. • Reportar oportunamente incidentes de seguridad, vulnerabilidades o eventos que puedan afectar la información o los servicios prestados a la entidad. • Permitir, cuando aplique contractualmente, actividades de verificación, seguimiento, evaluación o auditoría sobre el cumplimiento de requisitos de seguridad.
-------------------------------	---

9. INCUMPLIMIENTO DE LA POLÍTICA

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio para todos los funcionarios, contratistas, proveedores y terceros vinculados a la Cámara de Representantes. Cualquier incumplimiento, violación, omisión o negligencia frente a las disposiciones establecidas en la presente política podrá dar lugar a la aplicación de las acciones disciplinarias, administrativas, contractuales o legales correspondientes, de acuerdo con la normatividad vigente.

En el caso de los servidores públicos, el incumplimiento será tratado conforme a lo establecido en la Ley 1952 de 2019 y la Ley 2094 de 2021 (Código General Disciplinario). Para proveedores y contratistas, el incumplimiento se considerará una falta a las obligaciones contractuales, pudiendo dar lugar a la terminación del contrato y a las acciones legales a que haya lugar.

10. REFERENCIAS

- Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC, versión vigente.
- NTC ISO/IEC 27001:2022– Sistemas de Gestión de Seguridad de la Información.
- Ley 1581 de 2012 – Protección de datos personales.
- Ley 1273 de 2009 – Delitos informáticos.
- Ley 1712 de 2014 – Transparencia y acceso a la información pública.

	CÁMARA DE REPRESENTANTES OFICINA DE PLANEACIÓN Y SISTEMAS	
	POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	
	Código: 3-GTI-S2-PT-5	Versión: 2 Pág.: 11 de 11
Vigente desde: 28/05/2026		

11. ANEXOS

Manual de Políticas de Seguridad y Privacidad de la Información.

12. CONTROL DE CAMBIOS

N° VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO	
1	16/12/2021	06/10/2020 Creación del Documento. 06/11/2020 Ajuste al Formato.	Oficina de Planeación y Sistemas Ing. Elgar Castillo Rueda – Jefe OPS Revisión Técnica: Ing. Alejandro Muñoz Sandoval Ing. Sebastián Del Toro Montalvo Ing. Álvaro Carreño Ortiz Aprobación: Comité Institucional de Gestión y Desempeño 16/12/2021
2	28/05/2026	La actualización de la política, incluye ajustes en introducción, objetivos, alcance y lineamientos; actualización de la normatividad; alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la ISO/IEC 27001:2022; mejora de redacción general y depuración de contenidos.	Oficina de Planeación y Sistemas Ing. Jorge Edison Castro Revisión Técnica: Ing. Daniela Andrade Muñoz 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