PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2026

MINISTERIO DE VIVIENDA CIUDAD Y TERRITORIO

Ministerio de Vivienda, Ciudad y Territorio

Oficina de Tecnologías de la Información y las Comunicaciones

CONTENIDO

1. MARCO ESTRATÉGICO

ARTICULACIÓN MARCO ESTRATÉGICO	
Objetivo de Desarrollo Sostenible	N/A
Plan Nacional de Desarrollo (2022-2026)	5.31. Bloque estratégico III 3. Bloque habilitador de la convergencia regional
Plan Estratégico Sectorial	N/A
Plan Estratégico Institucional (2022-2026)	*5. Fortalecimiento institucional y gestión social.*
Política Modelo Integrado de Planeación y Gestión	Gobierno Digital
Proceso Institucional	Gestión de tecnologías de la Información y las Comunicaciones

2. INTRODUCCIÓN

La transformación digital del Estado y la creciente interconexión de redes, sistemas de información y servicios digitales han incrementado de manera significativa la exposición de las entidades públicas a riesgos asociados con la seguridad y la privacidad de la información. El intercambio constante de grandes volúmenes de datos, tanto al interior de las entidades como con actores externos, amplía la superficie de ataque y exige la adopción de enfoques preventivos, sistemáticos y basados en riesgos que permitan evitar la pérdida, alteración, divulgación no autorizada o indisponibilidad de la información.

En este contexto, la gestión de riesgos de seguridad y privacidad de la información se consolida como un componente esencial del habilitador de Seguridad Digital de la Política de Gobierno Digital, orientado a anticipar, analizar y tratar oportunamente las amenazas que puedan materializarse en incidentes de seguridad digital. Diversos análisis y experiencias institucionales evidencian que una proporción significativa de estos incidentes tiene su origen en debilidades de control, fallas de proceso o en el desconocimiento y comportamiento de los usuarios, lo cual refuerza la necesidad de mantener una gestión integral del riesgo.

El Ministerio de Vivienda, Ciudad y Territorio (MVCT), en cumplimiento de lo dispuesto en el Decreto 1078 de 2015 y en articulación con su Sistema de Gestión de Seguridad de la Información (SGSI), ha venido fortaleciendo la gestión de los riesgos de seguridad de la información y ciberseguridad como un proceso continuo,

alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC y con los principios establecidos en la norma ISO/IEC 27001:2022.

Para la vigencia 2026, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se concibe como un instrumento de gestión que permite evolucionar desde la identificación y valoración de riesgos hacia su priorización, tratamiento, seguimiento y evaluación de efectividad, integrando criterios de impacto, probabilidad, criticidad de los activos y un enfoque de ciberseguridad, con el propósito de fortalecer la resiliencia digital del Ministerio.

3. OBJETIVO

Gestionar de manera integral, sistemática y continua los riesgos de seguridad y privacidad de la información asociados con los procesos, activos de información, servicios tecnológicos y usuarios del Ministerio de Vivienda, Ciudad y Territorio (MVCT), mediante su identificación, análisis, valoración, priorización, tratamiento y seguimiento. Este proceso busca salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional, en concordancia con el Sistema de Gestión de Seguridad de la Información (SGSI), el Modelo de Seguridad y Privacidad de la Información (MSPI), la norma ISO/IEC 27001:2022 y la Estrategia de Ciberseguridad, considerando los siguientes lineamientos:

- Definir y mantener actualizado el contexto estratégico de la gestión de riesgos de seguridad y privacidad de la información, alineado con los objetivos institucionales y los procesos del MVCT.
- Identificar y actualizar de manera periódica los riesgos de seguridad digital asociados con los activos de información críticos, los procesos tecnológicos y los servicios digitales del Ministerio.
- Analizar y valorar los riesgos de seguridad y privacidad de la información aplicando criterios de impacto, probabilidad y criticidad que permitan su adecuada priorización.
- Establecer y ejecutar planes de tratamiento orientados a reducir, mitigar, aceptar, transferir o evitar los riesgos identificados, conforme con el nivel de riesgo definido por la Entidad.
- Integrar la gestión de riesgos de seguridad y privacidad de la información con la gestión de riesgos institucional, fortaleciendo los controles preventivos, detectivos y correctivos.
- Realizar seguimiento y evaluación periódica de la efectividad de los controles y las acciones de tratamiento implementadas.
- Fortalecer la cultura de gestión del riesgo en seguridad y privacidad de la información, mediante la articulación con actividades de sensibilización y apropiación institucional.
- Generar insumos para la toma de decisiones de la alta dirección y la mejora continua del SGSI, a partir del análisis de tendencias y resultados derivados de la gestión del riesgo.

4. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2026 aplica a todos los procesos, dependencias, funcionarios, contratistas, terceros y activos de información del Ministerio de Vivienda, Ciudad y Territorio (MVCT) que hagan uso, gestionen o administren información institucional, sin importar el medio o formato en que esta se encuentre.

El Plan se desarrolla en el marco del habilitador de Seguridad y Privacidad de la Información de la Política de Gobierno Digital, y se articula con el Sistema de Gestión de Seguridad de la Información (SGSI). Su alcance incluye las actividades de definición del contexto estratégico, identificación, análisis, valoración, priorización y tratamiento de los riesgos de seguridad digital, así como el seguimiento y la evaluación de la efectividad de los controles implementados.

Asimismo, abarca la aplicación de los procedimientos y controles de seguridad sobre la infraestructura tecnológica, redes, sistemas de información, aplicaciones, servicios en la nube y demás componentes del ecosistema digital del MVCT, incorporando el enfoque de ciberseguridad y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001:2022.

Este Plan constituye un instrumento dinámico y de mejora continua, cuyos resultados servirán como insumo para la gestión institucional del riesgo, la planeación estratégica, el fortalecimiento del SGSI y la definición de acciones preventivas y correctivas orientadas a garantizar la protección integral de la información y la continuidad de los servicios del Ministerio.

5. MARCO NORMATIVO

TIPO DE NORMA	NÚMERO	AÑO	Descripción - Epígrafe
CONPES	3701	2011	Lineamientos Política Ciberseguridad y Ciberdefensa.
CONPES	3854	2016	Política Nacional de Seguridad Digital.
CONPES	3995	2020	Política Nacional de Confianza y Seguridad Digital.
Constitución Política	-	1991	Artículos 15, 20, 23 y 74.
Decreto	2609	2012	Reglamenta gestión documental (Ley 594/2000).
Decreto	884	2012	Reglamenta parcialmente Ley 1221/2008.
Decreto	1377	2013	Reglamenta parcialmente Ley 1581/2012.
Decreto	886	2014	Reglamenta Registro Nacional de Bases de Datos.
Decreto	103	2015	Reglamenta parcialmente Ley 1712/2014.
Decreto	1074	2015	Reglamentario Sector Comercio; reglamenta Ley 1581/2012 (Art. 25-26).
Decreto	1078	2015	Decreto Único Reglamentario Sector TIC.
Decreto	1081	2015	Decreto Reglamentario Sector Presidencia.
Decreto	728	2017	Adiciona DUR TIC para Gobierno Digital (zonas WiFi públicas).
Decreto	1499	2017	Modifica Decreto 1083/2015 (Sistema de Gestión).
Decreto	612	2018	Directrices para integración de planes institucionales al

			Plan de Acción.
Decreto	338	2022	Fortalece gobernanza seguridad digital (ICC, SE).
Estrategia Nacional	-	2025-2027	Seguridad Digital (resiliencia, gobernanza).
Ley	23	1982	Derechos de autor.
Ley	44	1993	Modifica Ley 23 de 1982, Ley 29 de 1994 y Decisión Andina 351 (Derechos de autor).
Ley	527	1999	Acceso y uso de mensajes de datos, comercio electrónico y firmas digitales.
Ley	594	2000	Ley General de Archivos.
Ley	850	2003	Reglamenta veedurías ciudadanas.
Ley	962	2005	Racionalización de trámites administrativos.
Ley	1266	2008	Disposiciones generales del Habeas Data y manejo de bases de datos personales.
Ley	1221	2008	Normas para promover el teletrabajo.
Ley	1273	2009	Modifica Código Penal; protege información y datos (bien jurídico tutelado).
Ley	1341	2009	Sociedad de la información y organización TIC; crea Agencia Nacional del Espectro.
Ley	1437	2011	Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
Ley	1474	2011	Fortalecimiento de mecanismos anticorrupción.
Ley	1581	2012	Protección de datos personales.
Ley	1712	2014	Ley de Transparencia y Acceso a Información Pública.
Ley	1915	2018	Modifica Ley 23 de 1982 en derechos de autor.
Ley	1952	2019	Código General Disciplinario.
Resolución MinTIC	500	2021	Lineamientos MSPI, gestión riesgos e incidentes.
Resolución MinTIC	2277	2025	Actualiza MSPI (Anexo Res. 500/2021).
Resolución MVCT	331	2021	Actualiza Política SGSI MVCT.

5.1. OTROS DOCUMENTOS DE REFERENCIA

- G.INF.01 - Guía del dominio de información del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) - Resolución 2277 de 2025.

- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas - Departamento Administrativo de la Función Pública (DAFP) - 2025.

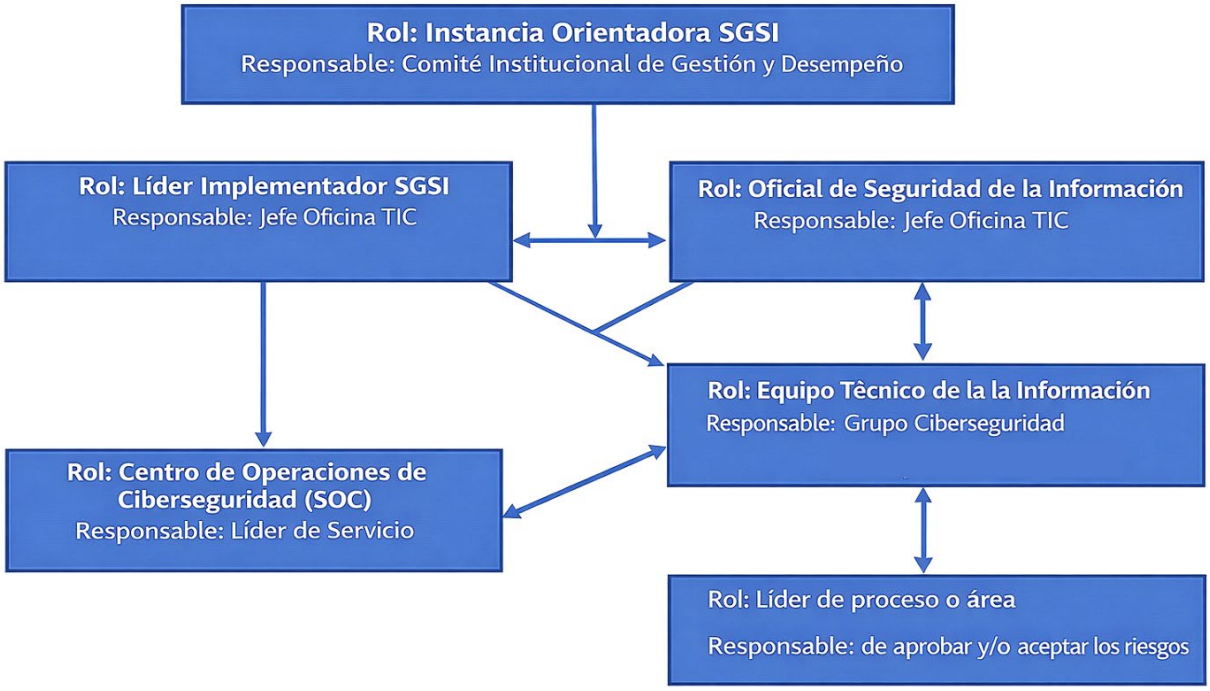
- NTC-ISO/IEC 27001:2022 - Sistemas de gestión de la seguridad de la información - Requisitos.

- NTC-ISO/IEC 27002:2022 - Tecnologías de la información - Técnicas de seguridad - Códigos de práctica para controles de seguridad de la información.

- NTC-ISO/IEC 27005:2022 - Tecnologías de la información - Técnicas de seguridad - Gestión de riesgos de seguridad de la información.

6. RESPONSABLES

El siguiente diagrama muestra los roles y actores involucrados en la gestión de la Seguridad de la Información y del Tratamiento de Riesgos:



7. DEFINICIONES

- **Activo:** Todo elemento (información, procesos, sistemas, redes, personas, instalaciones) con valor para la organización que requiere protección. (ISO/IEC 27000:2022)

- **Activo de Información:** Información y sus soportes (digitales/físicos) procesados por la organización; incluye datos públicos/personales bajo custodia del sujeto obligado. (MSPI MinTIC / Ley 1581/2012)

- **Amenaza:** Potencial causa de un evento no deseado que podría resultar en daño a un sistema u organización. (ISO/IEC 27000:2022)

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar su nivel. (ISO/IEC 27000:2022)

- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluar su conformidad con criterios establecidos. (ISO/IEC 27000:2022)

- **Ciberespacio:** Entorno físico/virtual de sistemas computacionales, redes, datos e información para interacción de usuarios. (Res. CRC 2258/2009)

- **Ciberseguridad:** Capacidad para minimizar riesgos a ciudadanos/Estado ante amenazas cibernéticas, preservando disponibilidad, integridad, confidencialidad y no repudio en interacciones digitales. (CONPES 3995/2020)

- **Control:** Medida (política, procedimiento, práctica u organización) que modifica el riesgo, sinónimo de salvaguarda o contramedida. (ISO/IEC 27000:2022)

- **Declaración de Aplicabilidad (DA):** Documento que justifica controles seleccionados en el SGSI tras evaluación/tratamiento de riesgos. (ISO/IEC 27001:2022)

- **Evaluación de Riesgo:** Proceso global (análisis + comparación con criterios) para decidir tratamiento de riesgos. (ISO/IEC 27000:2022)

- **Gestión de Incidentes de Seguridad:** Procesos para detectar, reportar, evaluar, responder, mitigar y aprender de incidentes de seguridad de la información. (ISO/IEC 27000:2022)

- **Información Pública Clasificada:** Información en poder del sujeto obligado, de ámbito privado/semiprivado, cuyo acceso puede negarse por derechos protegidos (Ley 1712/2014, Art. 18)

- **Información Pública Reservada:** Información exceptuada de acceso por daño a intereses públicos, cumpliendo requisitos del Art. 19 Ley 1712/2014

- **MSPI:** Modelo de Seguridad y Privacidad de la Información del MinTIC; lineamientos para entidades públicas en ciclo de vida de seguridad (planeación, implementación, evaluación, mejora continua). (Res. MinTIC 2277/2025)

- **Nivel de Riesgo:** Magnitud del riesgo expresado cualitativa o cuantitativamente. (ISO/IEC 27000:2022)

- **Plan de Continuidad del Negocio (PCN):** Documento para continuar funciones críticas ante interrupciones. (ISO/IEC 27000:2022)

- **Riesgo:** Efecto de la incertidumbre en objetivos (generalmente impacto x probabilidad); en seguridad, combinación de consecuencia de un evento y su likelihood. (ISO/IEC 27000:2022)

- **Riesgo Residual:** Nivel de riesgo restante tras aplicar controles/tratamientos. (ISO/IEC 27005:2022)

- **Seguridad de la Información:** Preservación de confidencialidad, integridad y disponibilidad (CID) de la información; incluye autenticidad, no repudio y trazabilidad. (ISO/IEC 27000:2022)

- **SGSI:** Parte del sistema de gestión que gestiona riesgos de seguridad de la información mediante política, objetivos, procesos y mejora continua. (ISO/IEC 27000:2022)

- **Tratamiento de Riesgo:** Proceso de seleccionar/modificar opciones (evitar, mitigar, transferir, aceptar) para riesgos. (ISO/IEC 27000:2022)

- **Vulnerabilidad:** Debilidad de un activo que puede ser explotada por una amenaza. (ISO/IEC 27000:2022)

8. DESARROLLO DEL PLAN

8.1 DIAGNÓSTICO

Para el análisis de riesgos se adoptan las directrices del Manual de Gestión de Riesgos DET-M-07, la Guía de Metodología Integrada para la Administración del Riesgo del Departamento Administrativo de la Función Pública (DAFP) y el enfoque de gestión de riesgos establecido en la NTC-ISO/IEC 27005:2022.

La evaluación de la infraestructura tecnológica del Ministerio, realizada bajo el Modelo de Seguridad y Privacidad de la Información (MSPI), identificó hallazgos críticos que no excluyen la existencia de riesgos adicionales, los cuales se identificarán mediante la revisión permanente de los riesgos de seguridad de la información asociados a cada proceso y sus activos.

8.2. MATRIZ OPERATIVA DEL PLAN

A continuación, se establece una relación de acciones que se deberán desarrollar para controlar los riesgos identificados en el proceso de análisis dentro de la matriz de valoración de riesgos.

Matriz Operativa del Plan 2026						
Alineación Estratégica	Responsable	Actividades	Resultado	Indicador	Fecha de inicio	Fecha de finalización
Decreto 612-2018	Oficial de Seguridad de la Información	Actualizar lineamientos, instrumentos y procedimientos de gestión de riesgos de seguridad y privacidad de la información.	Metodología, lineamientos e instrumentos actualizados.	1 Metodología ajustada	10/02/2026	30/11/2026
Decreto 612-2018	Oficial de Seguridad de la Información	Identificar riesgos de seguridad, privacidad de la información y seguridad digital asociados a procesos, activos críticos.	Matriz de riesgos de seguridad y privacidad por proceso/área, con valoración de impacto, probabilidad y criticidad.	1 Informe realizado	1/05/2026	30/10/2026
Decreto 612-2018	Líder de proceso, área o su delegado	Aprobar y aceptar formalmente los riesgos identificados por parte de los responsables de procesos.	Acta o documento de aprobación de riesgos aceptados.	1 Informe realizado	1/05/2026	30/10/2026
Decreto 612-2018	Líder de proceso, área o su delegado	Socializar los mapas de riesgo a los responsables y equipos de cada proceso/área.	Acta de socialización de matrices de riesgos, con registro de participantes y compromisos asumidos.	1 Informe realizado	1/05/2026	30/10/2026
Decreto 612-2018	Líder de proceso, área o su delegado	Realizar seguimiento y monitoreo como segunda linea de defensa	Informe Trimestral de monitoreo de segunda linea de defensa	1 Informe realizado	15/03/2026	15/12/2026

9. RECURSOS

Fuente de financiación: Presupuesto General de la Nación

Proyecto de Inversión: Fortalecimiento de la gestión integral de las tecnologías de la información y las comunicaciones en el Ministerio de Vivienda, Ciudad y Territorio a nivel Nacional.

10. SEGUIMIENTO Y MEDICIÓN DEL PLAN

Matriz Operativa del Plan							Seguimiento	
Alineación Estratégica	**Responsable**	**Actividades**	**Resultado**	**Indicador**	**Fecha de inicio**	**Fecha de finalización**	**Avance cuantitativo**	**Avance cualitativo**
Decreto 612-2018	Oficial de Seguridad de la Información	Monitoreo y revisión trimestral del plan y de los indicadores implementados	Informe de avance o resumen ejecutivo.	Indicador de seguimiento al Plan de Tratamiento de Riesgos.	1 feb	15 dic		
Decreto 612-2018	Oficial de Seguridad de la Información	Revisión de la evaluación de los niveles de riesgo y riesgo residual después de la aplicación de controles y medidas administrativas.	Informe de avance o resumen ejecutivo.	Indicador de seguimiento al Plan de Tratamiento de Riesgos.	1 feb	15 dic		

Toda vez que el presente Plan está articulado al Plan de Acción Institucional de la vigencia, como líder de cada plan, se realizará seguimiento constante a las actividades definidas en la matriz operativa.

En este sentido y a fin de tomar decisiones tempranas por parte de la alta dirección se presentará el estado del plan de manera semestral en sesión del Comité Institucional de Gestión y Desempeño.

Finalmente, es importante indicar que los informes de seguimiento realizados a este plan serán publicados en la sección oficial de SharePoint de la Oficina TIC.

CONTROL DE CAMBIOS			
Versión	**Fecha**	**Instancia de Aprobación**	**Descripción**
01	20/01/2026	Comité Institucional de Gestión y Desempeño	Formulación del Plan
02	26/03/2026	Comité Institucional de Gestión y Desempeño	Se ajustaron y actualizaron las actividades, definiciones, responsables y los documentos de referencia.