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

Ministerio de Vivienda, Ciudad y Territorio

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 a la seguridad y privacidad de la información. El intercambio permanente 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 para evitar la pérdida, alteración, divulgación no autorizada o indisponibilidad de la información.

En este contexto, la gestión de los 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 de manera oportuna las amenazas que puedan materializarse en incidentes de seguridad digital. Diversos análisis y experiencias institucionales evidencian que una proporción significativa de los incidentes de seguridad tiene su origen en debilidades en los controles, fallas en los procesos o en el desconocimiento y comportamiento de los usuarios, lo que refuerza la necesidad de una gestión integral del riesgo.

El Ministerio de Vivienda, Ciudad y Territorio – MVCT, en concordancia con lo dispuesto en el Decreto 1078 de 2015 y en articulación con el 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 principiosde 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 enfoque de Ciberseguridad de Zero Trust (Cero Confianza), con el fin 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 a los procesos, activos de información, servicios tecnológicos y usuarios del Ministerio de Vivienda, Ciudad y Territorio, mediante su identificación, análisis, valoración, priorización, tratamiento y seguimiento, con el propósito de salvaguardar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional, en concordancia con el SGSI, el MSPI, la norma ISO/IEC 27001:2022 y la estrategia de Ciberseguridad de Zero Trust, considerando lo siguiente:

- 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 a 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 de riesgos orientados a reducir, mitigar, aceptar, transferir o evitar los riesgos identificados, de acuerdo con el nivel de riesgo definido por la Entidad.
- Integrar los riesgos de seguridad y privacidad de la información con la gestión de riesgos institucional y con el enfoque de Zero Trust, fortaleciendo los controles preventivos, detectivos y correctivos.
- Realizar seguimiento y evaluación periódica a la efectividad de los controles y 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 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 que hacen uso, gestionan o administran información institucional, independientemente del 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, abarcando las actividades de definición del contexto estratégico, identificación, análisis, valoración, priorización y tratamiento de los riesgos de seguridad digital, así como el seguimiento y evaluación de la efectividad de los controles implementados.

Así mismo, el alcance comprende 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 de Zero Trust y los lineamientos del MSPI y la norma ISO/IEC 27001:2022.

El 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 de la información y la continuidad de los servicios del Ministerio.

5. MARCO NORMATIVO

TIPO DE NORMA	NÚMERO	AÑO	Descripción - Epígrafe
Constitución Política		1991	Artículos 15, 20, 23 y 74.
Ley	23	1982	Derechos de autor
Ley	44	1993	Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
Ley	527	1999	Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
Ley	594	2000	Por la que se expide la Ley General de Archivos.
Ley	850	2003	Por medio de la cual se reglamentan las veedurías ciudadanas.
Ley	962	2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones

			públicas o prestan servicios públicos.
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	1221	2008	Por la cual se establecen normas para promover y regular el Teletrabajo 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 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 de espectro y se dictan otras disposiciones.
Ley	1437	2011	Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
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.
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	1915	2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Ley	1952	2019	Por medio de la cual se expide el código general disciplinario.
Decreto	2609	2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
Decreto	0884	2012	Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
Decreto	1377	2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto	886	2014	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Decreto	103	2015	Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto	1074	2015	Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Art 25 y 26.
Decreto	1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

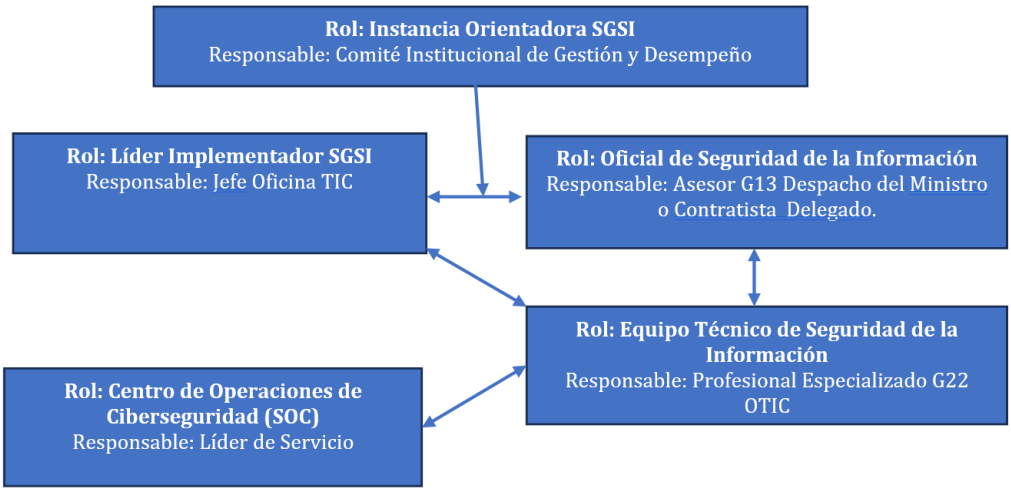
Decreto	1081	2015	Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
Decreto	728	2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto	1499	2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto	612	2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Resolución	0331	2021	Por la cual se actualiza la Política del Sistema de Gestión de Seguridad de la Información en el Ministerio de Vivienda, Ciudad y Territorio.
CONPES	3701	2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES	3854	2016	Política Nacional de Seguridad digital
CONPES	3995	2020	Política Nacional de Confianza y Seguridad Digital.

5.1. OTROS DOCUMENTOS DE REFERENCIA

G.INF.01 Guía del dominio de información del MSPI del Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC)
Normas NTC-ISO-IEC 27001:2013, GTC-ISO-IEC 27002:2015, NTC-ISO-IEC 27005:2008

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: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

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

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de

telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información - SGSI, de la organización, tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

MSPI: El Modelo de Seguridad y Privacidad de la Información - MSPI, imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Riesgo: 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/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

8. DESARROLLO DEL PLAN

8.1 DIAGNÓSTICO

Para el análisis de riesgos se tienen en cuenta las directrices establecidas en el Manual de Gestión de Riesgos DET-M-07, así mismo, se tiene en cuenta la guía de metodología integrada para la administración del riesgo del Departamento Administrativo De La Función Pública y se adopta el enfoque de manejo de riesgos basado en la norma ISO/IEC 27005:2022.

La evaluación realizada a la infraestructura tecnológica del Ministerio bajo el modelo de seguridad y privacidad de la información arrojaron una serie de hallazgos críticos pero que no limitan la existencia de posibles riesgos adicionales que pudieran existir en la revisión permanente de riesgos de seguridad de la información para cada uno de los procesos 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	Líder de Servicio	Realizar el cierre de brechas de infraestructura tecnológica con la aplicación de parches y actualizaciones del plan de remediación de vulnerabilidades.	Remediaciones y actualizaciones a los servicios e infraestructura tecnológica.	1 informe realizado	1 jul	30 nov
Decreto 612-2018	Líder de Servicio	Validar la activación de NTP sincronización de relojes en todos los elementos de Red e Infraestructura del MVCT.	Actualización de sincronización de relojes en infraestructura y redes.	1 informe realizado	1 abr	30 may

Decreto 612-2018	Oficial de Seguridad	Restringir el uso de credenciales de administrador a través de directiva interna	Memorando a Coordinador del GAT	1 informe realizado	1 mar	30 mar
Decreto 612-2018	Oficial de Seguridad	Revisar y ajustar el procedimiento de asignación de derecho de acceso a las aplicaciones.	Procedimiento de asignación de accesos a aplicaciones ajustado.	1 procedimiento ajustado	1 feb	30 jun
Decreto 612-2018	Centro de Operaciones de Seguridad	Revisar y actualizar las configuraciones de los registros de Zona DNS: DMARC y DNSSEC	Actualización de los registros de Zona DNS	1 reporte trimestral de Zona DNS realizado	1 feb	31 dic
Decreto 612-2018	Centro de Operaciones de Seguridad	Actualizar los certificados de seguridad de aplicaciones e infraestructura.	Actualización de los Certificados SSL.	1 informe de actualización de certificados realizado	15 nov	15 dic
Decreto 612-2018	Centro de Operaciones de Seguridad	Revisar y actualizar los flujos de información del WAF de todas las aplicaciones publicadas en Internet del MVCT.	Actualización de los flujos de trafico https de las aplicaciones web publicadas.	2 reportes realizados	1 feb	30 nov
Decreto 612-2018	Centro de Operaciones de Seguridad	Endurecer los servicios de filtrado de correo electrónico con la implementación de servicios de ATP e integrarlos al SIEM.	Documento de implementación de filtrado ATP integrado al SIEM.	1 informe realizado	1 may	30 oct
Decreto 612-2018	Líder de Servicio	Ampliar la capacidad de los servicios de almacenamiento en nube.	Ampliación de capacidad de almacenamiento en la nube.	20% de capacidad ampliada	1 feb	30 abr
Decreto 612-2018	Equipo Técnico de Seguridad de la Información	Actualizar los procedimientos de registro y retención documental de los archivos digitales.	Procedimiento de retención documental de archivos digitales actualizado.	1 procedimiento ajustado	1 feb	30 ago
Decreto 612-2018	Equipo Técnico de Seguridad de la Información	Depurar los File Servers onpremise y los contenedores de información en nube.	Informe de optimización del almacenamiento de archivos digitales.	1 informe realizado	1 feb	30 nov
Decreto 612-2018	Centro de Operaciones de Seguridad	Valorar activos críticos y cargas de trabajo.	Listado de activos críticos y cargas de trabajo de alto valor priorizados	1 informe realizado	1 mar	30 jul
Decreto 612-2018	Oficial de Seguridad	Actualizar la política, metodología y lineamientos de la gestión de riesgos	Documentación actualizada en el SPG	1 informe realizado	1 sep	30 nov
Decreto 612-2018	Equipo Técnico de Seguridad de la Información	Identificar Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Documento y Matriz de riesgos actualizados de acuerdo con los criterios de disponibilidad, integridad, confidencialidad y costo.	1 informe realizado	1 sep	15 nov
Decreto 612-2018	Oficial de Seguridad	Aceptar y aprobar tratamiento de riesgos identificados.	Documento de aceptación y tratamiento de riesgos.	1 documento aprobado por CIGD.	15 nov	15 dic
Decreto 612-2018	Oficial de Seguridad	Publicar Mapas de riesgos en el SPG	Mapas de riesgo actualizados en el SPG.	1 informe realizado	1 jul	30 nov
Decreto 612-2018	Equipo Técnico de Seguridad de la Información	Implementar controles con las oportunidades de mejora acorde a los riesgos identificados.	Reporte de Seguimiento a los mapas de riesgos.	1 informe realizado	1 feb	30 nov

Decreto 612-2018	Oficial de Seguridad	Presentar reporte de indicadores.	Reporte de Indicadores.	2 reportes de indicadores	1 may	30 sep

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	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	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