PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES

23 de diciembre de 2025

Versión 7

Tabla de Contenido

1. Lista de Tablas

2. Lista de Ilustraciones

3. Introducción

En un entorno dinámico y altamente interconectado, la información se ha convertido en uno de los activos más valiosos de cualquier organización. La Caja de la Vivienda Popular (CVP) reconoce la importancia de proteger la confidencialidad, integridad y disponibilidad de la información que gestiona, garantizando que esta sea tratada de manera responsable y conforme a los estándares legales, técnicos y éticos aplicables.

El Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) tiene como propósito establecer las directrices, controles y procedimientos necesarios para salvaguardar los datos que se generan, almacenan, procesan y comparten en el marco de las actividades de la Caja de la Vivienda Popular (CVP). Este plan está diseñado para identificar riesgos asociados al manejo de la información, definir medidas de protección adecuadas y fomentar una cultura de seguridad y privacidad entre todos los miembros de la organización.

Asimismo, el plan asegura el cumplimiento de las normativas nacionales e internacionales relacionadas con la protección de datos personales y la gestión segura de la información, respondiendo a los requerimientos específicos de la Ley 1581 de 2012 (Régimen General de Protección de Datos Personales) y demás disposiciones vigentes en Colombia, así como el Modelo de Seguridad y Privacidad de la información (MSPI).

La implementación de este plan busca no solo proteger los activos de información, sino también fortalecer la confianza de los ciudadanos, aliados estratégicos y otras partes interesadas en los procesos de la Caja de la Vivienda Popular (CVP), promoviendo la transparencia, la responsabilidad y la resiliencia ante posibles amenazas.

4. Información General

Nombre del Plan de acción o estrategia institucional	**Plan Estratégico de Seguridad y Privacidad de la Información 2026**
Nombre y código rubro presupuestal asociado	**Proyecto de Inversión: Código: O230117459920240191** Fortalecimiento de la capacidad institucional para la modernización de la Caja de la Vivienda Popular de la ciudad de Bogotá D.C
Presupuesto asignado ($)	Presupuesto Total del Proceso: $ 3.400.000.000
Área responsable	Oficina de Tecnología de la Información y las Comunicaciones
Política asociada y otros lineamientos	7. Gobierno digital 8. Seguridad digital
Proceso	Gestión de Tecnología de la Información y las Comunicaciones
Fecha de inicio	02/01/2026
Fecha de finalización	31/12/2026

Tabla 1 - Información general del Plan
Fuente: Elaboración Propia

5. Objetivo Estratégico

Fortalecer la capacidad y efectividad administrativa y la innovación organizacional, para la modernización de la Caja y el incremento de la confianza ciudadana en la Entidad

6. Objetivos del Plan

6.1.1. Objetivo General

Definir la estrategia para diseñar e implementar políticas, controles, lineamientos, procedimientos y buenas prácticas que contribuyan a proteger la disponibilidad, integridad y confidencialidad de los activos de información definidas en este documento para la vigencia 2026. Este enfoque busca asegurar la continuidad de los procesos misionales de la Caja de la Vivienda Popular, alineándose con los objetivos estratégicos de la CVP, y de esta manera reducir hasta niveles aceptables los riesgos a los que está expuesta la Entidad.

6.1.2. Objetivos Específicos

- Fortalecer las capacidades de seguridad de la información en la Entidad, protegiendo los datos de los ciudadanos y los servidores públicos, y garantizando su privacidad. Este esfuerzo está alineado con los lineamientos establecidos en el componente del habilitador de seguridad y privacidad de la información de la Política de Gobierno Digital.

- Contribuir con la continuidad de los procesos de la Caja de la Vivienda Popular, mediante la implementación de controles asociados a la seguridad de la información que contribuyan al mantenimiento de los niveles de riesgos aceptables de la entidad, a través de una adecuada gestión de incidentes de seguridad de la información.

- Planificar la evaluación y hacer seguimiento de los controles y lineamientos implementados en el Modelo de Seguridad y Privacidad de la Información MSPI.

- Promover una cultura de seguridad de la información en la Caja de la Vivienda Popular, mediante la adopción de buenas prácticas, sensibilización y generación de conciencia entre los servidores públicos y terceros. Este enfoque busca fomentar comportamientos responsables y proactivos frente a la protección y manejo adecuado de la información, contribuyendo al cumplimiento de los objetivos estratégicos de la Entidad.

7. Alcance

El Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) aplica a todos los servidores públicos, contratistas, y terceros de la Caja de la Vivienda Popular que tengan acceso, usen, produzcan o manejen información; de los procesos estratégicos, misionales, de apoyo y de evaluación; de la Entidad.

El plan inicia con la definición y adopción de la política de seguridad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad, a través del establecimiento de los roles y responsabilidades en seguridad de la información; así como la clasificación de los activos de información involucrados en los procesos estratégicos, misionales, de apoyo y de evaluación.

Posterior a ello, se enfoca en la identificación y tratamiento de los riesgos asociados a la seguridad de la información; luego se establece un marco de procedimientos, controles y buenas prácticas que refuerzan la protección integral de los activos de información de la Caja de la Vivienda Popular, asegurando su gestión responsable y segura.

Finalmente, se propenderá por una correcta evaluación del desempeño de la Seguridad y Privacidad de la Información de la Entidad, tras planear, implementar y gestionar el MSPI.

8. Definiciones

A los efectos del presente plan se deberán atender las siguientes definiciones:

• **Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

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

• **Activos de Información y recursos:** se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).

• **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

• **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 dicho 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).

• **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

• **Bases de Datos Personales:** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

• **Ciberseguridad:** Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.

• **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.

• **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las Entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

• **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

• **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público.

Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

• **Datos Personales Privados:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

• **Datos Personales Mixtos:** Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.

• **Datos Personales Sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

• **Derecho a la Intimidad:** Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

• **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).

• **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).

• **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.

• **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

• **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las Entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

• **Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

• **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).

• **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

• **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25).

• **Responsabilidad Demostrada:** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

• **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

• **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 en cualquier medio: impreso o digital. (ISO/IEC 27000).

• **Seguridad digital:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

• **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

• **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

• **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o Entidad. (ISO/IEC 27000).

• **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

9. Normatividad

La estrategia de TI se encuentra alineada al marco normativo de la Nación, el Distrito y la Entidad, el cual puede consultarse en el Normograma del Proceso de Gestión de Tecnología de la Información y las Comunicaciones, que sirve como herramienta para delimitar las normas que regulan la gestión del proceso, y permiten identificar las competencias, responsabilidades y funciones de la dependencia. Las normas están compendiadas y organizadas para que su accesibilidad permita consultarlas, estudiarlas y promoverlas de una manera más fácil para su aplicación.

A continuación, se hace referencia a la normatividad más relevante a partir de la cual tienen sustento el desarrollo e implementación de este Plan Estratégico de Seguridad y Privacidad de la Información, fundamentado en las directrices establecidas por la Política de Gobierno Digital, el marco de Seguridad Digital y los estándares internacionales de gestión de seguridad de la información.

Norma	Número	Fecha de Emisión			Tipo	Descripción
Ley	1581	17	10	2012	EXTERNO	"Por la cual se dictan disposiciones generales para la protección de datos personales".
Decreto	612	4	4	2018	EXTERNO	"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"
Decreto	1008	14	6	2018	EXTERNO	"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
Decreto	Decreto 767	16	5	2022	EXTERNO	"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
Resolución	500	10	3	2021	EXTERNO	"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
Norma NTC-ISO/IEC	27001: 2022	25	09	2013	EXTERNO	Norma internacional emitida por la Organización Internacional de Normalización (ISO) para gestionar la seguridad de la información en una organización pública o privada.
CONPES	3995	1	7	2020	EXTERNO	"Política Nacional De Confianza Y Seguridad Digital".
CONPES	3854	11	4	2016	EXTERNO	"Política Nacional De Seguridad Digital"
Modelo de Seguridad y Privacidad de la Información – MINTIC.	Resolución 500	10	03	2021	EXTERNO	"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, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

Tabla 2 - Normatividad para desarrollo e implementación del PESPI
Fuente: Elaboración Propia

10. Formulación del Plan

10.1. Estado Actual de la Entidad Respecto al MSPI

Para la vigencia 2025, se reportó como logro del MSPI el diseño e implementación de las metodologías de inventario y clasificación de los activos de información, y la definición y valoración de los riesgos de seguridad y privacidad de la información de la Entidad.

También, se implementaron las actividades de simulacro controlado de Phishing, análisis de vulnerabilidades de seguridad de la información a 3 activos críticos de la Entidad y se fortalece la participación en las jornadas de sensibilización en seguridad de la información por parte de los colaboradores de la Caja de la Vivienda Popular.

Adicionalmente, se avanza en la implementación de la estrategia de la Unidad de Monitoreo de Seguridad Digital (Centro de Operaciones de Seguridad: SOC), liderada por la Consejería Distrital de Tecnologías de la Información y las Comunicaciones, en la cual la CVP es una de las 25 entidades piloto del proyecto.

Por último, acorde a la medición de FURAG 2024; se obtuvieron las calificaciones de 89,6 en el habilitador de Seguridad y Privacidad de la Información, y de 88,4 en la Política de Seguridad Digital.

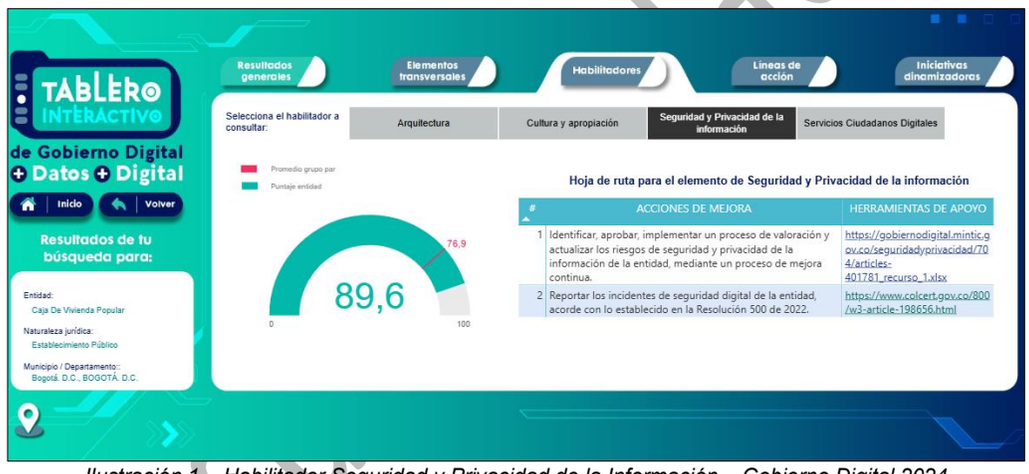

Ilustración 1 – Habilitador Seguridad y Privacidad de la Información – Gobierno Digital 2024
Fuente: Micrositio Gobierno Digital "Mediciones" – MinTIC

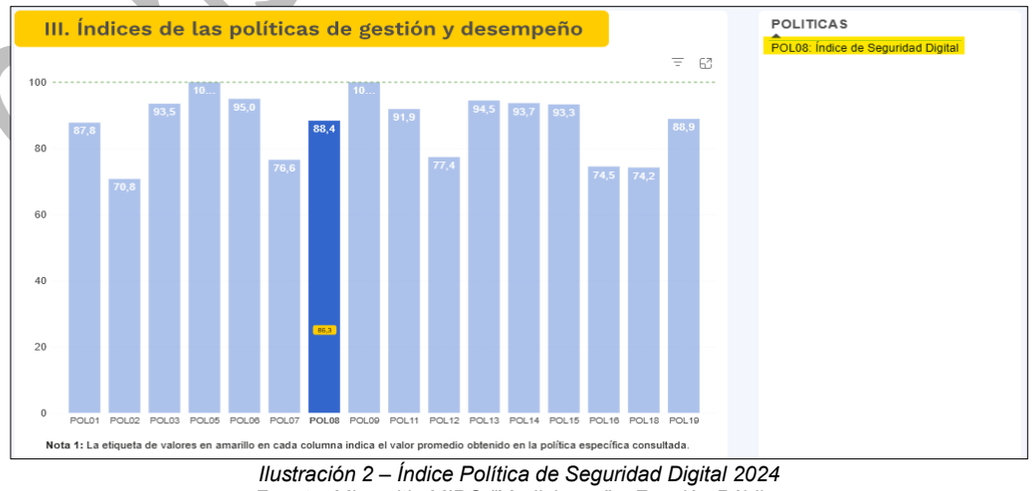

Ilustración 2 – Índice Política de Seguridad Digital 2024
Fuente: Micrositio MIPG "Mediciones" – Función Pública

Los resultados del autodiagnóstico del MSPI, tal como puede observarse en la siguiente imagen, evidencian una efectividad del 90% en los controles de seguridad, con áreas de mejora en la gestión de activos criptográficos, seguridad física, relación con proveedores y gestión de incidentes.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	93	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	97	100	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	85	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	100	100	OPTIMIZADO
A.10	CRIPTOGRAFÍA	80	100	GESTIONADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	88	100	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	96	100	OPTIMIZADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	95	100	OPTIMIZADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	93	100	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	74	100	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	80	100	GESTIONADO
A.18	CUMPLIMIENTO	100	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**90**	**100**	OPTIMIZADO

Ilustración 3 - Evaluación de efectividad de Controles - ISO 27001:2013
Fuente: Herramienta-Instrumento de Evaluación MSPI-Portada

La Entidad se encuentra en un proceso definido en relación con la implementación de medidas y controles destinados a garantizar la privacidad y seguridad de la información, así como la protección de los activos que la contienen. Las brechas identificadas se ilustran en el siguiente gráfico, permitiendo visualizar las áreas de mejora y priorización para fortalecer la gestión de la seguridad de la información.

Ilustración 4 - Brecha Anexo A ISO 27001:2013
Fuente: Instrumento de Evaluación MSPI – Portada

10.2. Generalidades del Plan

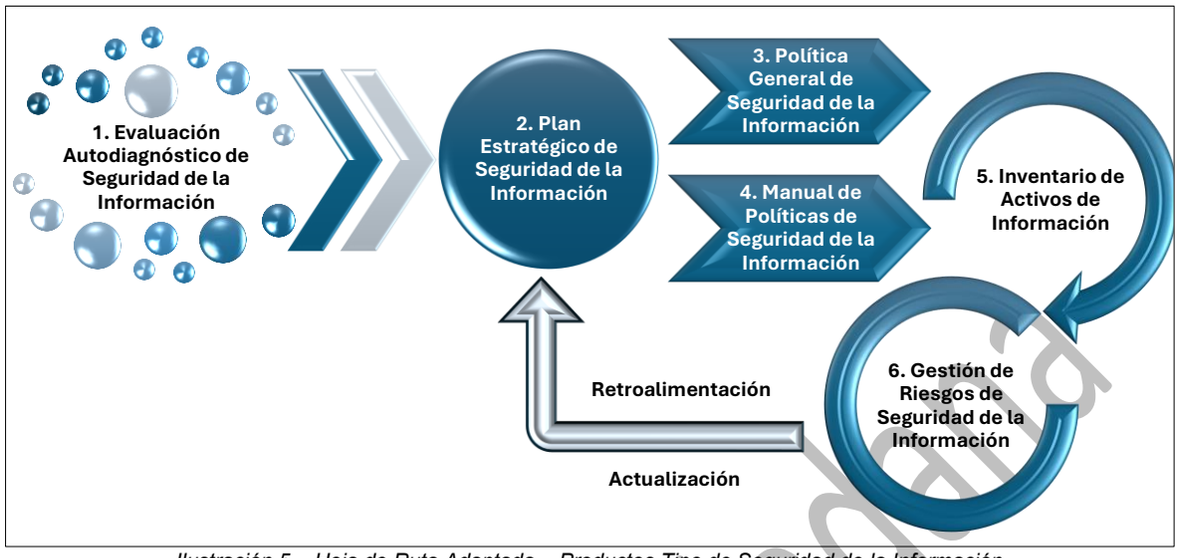

Ilustración 5 – Hoja de Ruta Adaptada – Productos Tipo de Seguridad de la Información
Fuente: Manual de Gobierno Digital – Habilitador: Seguridad y Privacidad de la Información

La Caja de la Vivienda Popular establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira en torno a la implementación del MSPI, mediante la hoja de ruta que se plantea en el diagrama representando el escenario ideal de implementación de los productos tipo de seguridad de la información, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes; sin embargo, esto no limita a que la Entidad desarrolle las actividades de forma paralela y no de forma lineal como se expone.

10.3. Cronograma

N°	Etapa o fase / Actividad / Tarea	Fecha Inicio	Fecha Fin
1.	**LIDERAZGO DE SEGURIDAD DE LA INFORMACIÓN**	**02-01-2026**	**31-01-2026**
1.1.	***Liderazgo y Compromiso***		
1.1.1	*Incluir dentro del Comité institucional de Gestión y Desempeño o quien haga sus veces, la presentación y aprobación del plan de seguridad y privacidad de la información, plan de tratamiento de riesgos de seguridad, adoptando, implementando, manteniendo y mejorando continuamente el MSPI, los cuales se aprobarán y divulgarán por medio de la sede electrónica (página web) de la CVP.*		
1.1.1.1.	Entregable: Plan publicado (URL)		
1.2.	***Manual de Políticas de seguridad y privacidad de la información***	**02-01-2026**	**30-06-2026**
1.2.1.	*Revisar y actualizar en caso de ser necesario el manual de Políticas de Seguridad y Privacidad de la Información. Presentar ante el Comité institucional de Gestión y Desempeño.*		
1.2.1.1.	Entregable: *Manual de Políticas de Seguridad y Privacidad de la Información actualizado y/o Política General de Seguridad de la Información.*		
1.3.	***Roles y responsabilidades***	**02-01-2026**	**30-11-2026**
1.3.1.	*Presentar al comité institucional de Gestión y Desempeño, los roles y responsabilidades necesarios para la articulación y adopción del MSPI que sean requeridos.*		
1.3.1.1.	Entregable: Presentaciones para el CIGD que contengan Roles y Responsabilidades.		

N°	Etapa o fase / Actividad / Tarea	Fecha Inicio	Fecha Fin
2.	**IMPLEMENTACIÓN DE CONTROLES**	**02-01-2026**	**31-12-2026**
2.1.	***Identificación de activos de información e infraestructura critica***	**01-02-2026**	**30-06-2026**
2.1.1.	*Revisar y actualizar en caso de ser necesario, el Documento Metodológico de inventario y clasificación de la información.*		
2.1.1.1.	Entregable: Documento Metodológico de inventario y clasificación de la información.		
2.1.2.	*Actualizar el inventario de activos de información e infraestructura crítica*		
2.1.2.1.	Entregable: Inventario y la clasificación de los Activos de Información.		
2.2.	***Desarrollar acciones para garantizar la implementación y mantenimiento de los requisitos de la Política de Gobierno Digital aplicables al MSPI***	**01-03-2026**	**30-08-2026**
2.2.1.	*Actualizar el Autodiagnóstico del MSPI*		
2.2.1.1	Entregable: *Autodiagnóstico del MSPI Actualizado*		
3.	**GESTIÓN DE RIESGOS**	**02-01-2026**	**15-12-2026**
3.1.	***Valoración de los riesgos de seguridad de la información***		
3.1.1.	*Definir manual de gestión de riesgos de seguridad y privacidad de la información alineado a la Guía de Riesgos V7.*		
3.1.1.1.	Entregable: M*anual de gestión de riesgos de seguridad y privacidad de la información.*		
3.2.	***Plan de tratamiento de los riesgos de seguridad de la información***		
3.2.1.	*Ejecutar el Plan de tratamiento de riesgos, aprobado por el comité institucional de gestión y desempeño.*		
3.2.1.1.	Entregable: Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información (PTRSPI).		
3.3.	***Identificación de los riesgos de seguridad de la información***		
3.3.1.	*Actualizar el mapa de Riesgos de seguridad de la información y privacidad de la información.*		
3.3.1.1.	Entregable: Mapa de Riesgos de seguridad de la información y privacidad de la información.		
3.4.	**ANÁLISIS DE VULNERABILIDADES**	**01-06-2026**	**30-11-2026**
3.4.1.	*Ejecutar Análisis de Vulnerabilidades de seguridad de la información y plan de remediación.*		
3.4.1.1.	Entregable: Informe Técnico de Pruebas de Análisis de Vulnerabilidades a tres (03) activos de información críticos de TI.		
3.5.	***DECLARACIÓN DE APLICABILIDAD (SOA)***	**01-02-2026**	**31-05-2026**
3.5.1.	*Elaborar y Aprobar la Declaración de aplicabilidad (SOA).*		
3.5.1.1.	Entregable: Declaración de aplicabilidad (SOA).		
4.	**GESTIÓN DE INCIDENTES**	**01-02-2026**	**30-06-2026**
4.1.	***Implementar un Modelo de Gestión de Incidentes de seguridad de la información***		
4.1.1	*Actualizar el Procedimiento de Gestión de Incidentes*		
4.1.1.1.	Entregable: Procedimiento de Gestión de Incidentes		
5.	**CONCIENTIZACIÓN**	**01-02-2026**	**30-11-2026**
5.1.	***Competencia, toma de conciencia y comunicación***		
5.1.1.	*La entidad debe definir un plan de comunicación, capacitación, sensibilización y concientización del modelo de seguridad y privacidad de la información.*		
5.1.1.1.	Entregable: El Plan de Sensibilización de seguridad y privacidad de la Información y Sesiones de Capacitación/Sensibilización desarrolladas.		
6.	**SEGUIMIENTO Y EVALUACIÓN**	**01-02-2026**	**30-11-2026**
6.1.	***Seguimiento a Implementación del MSPI***		
6.1.1.	*Presentar cuando se requiera al Comité Directivo los avances en la gestión, los logros de los resultados y metas propuestas, para la implementación del MSPI*		
6.1.1.1.	Entregable: Presentaciones.		

Tabla 3 - Cronograma PESPI 2026
Fuente: Elaboración Propia

10.4. Seguimiento y evaluación

Orientados a la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, se formulan los indicadores que servirán como insumo para el componente de mejora continua, permitiendo adoptar decisiones de mejora e identificar el nivel de estructuración de los procesos de la Entidad orientados a la seguridad de la información:

Los objetivos de estos procesos de seguimiento y evaluación en seguridad de la información son:

- ✓ Evaluar la efectividad de la implementación de los controles de seguridad.
- ✓ Evaluar la eficacia del Modelo de Seguridad y Privacidad de la Información al interior de la CVP.
- ✓ Comunicar valores de seguridad y privacidad de la información al interior de la Entidad.
- ✓ Servir como insumos al Plan de Tratamiento de riesgos de Seguridad y Privacidad de la información.

INDICADORES PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
Categoría Indicador	**Tipo Indicador**	**Nombre del Indicador**	**Descripción**	**Variables**	**Fórmulas**
Eficacia	Estratégico	Implementación del Plan Estratégico de Seguridad y Privacidad de la Información (PESPI).	Establecer el porcentaje de cumplimiento del cronograma del PESPI.	***PCP:*** *Porcentaje cumplimiento cronograma del Plan.* ***AE:*** *Número de actividades ejecutadas del cronograma, durante el período de tiempo analizado.* ***AP:*** *Número de actividades planeadas del cronograma, durante el período de tiempo analizado.*	***PCP = (AE/AP) *100***
Eficiencia	De Gestión	Nivel de participación de Servidores Públicos y/o Contratistas en actividades de sensibilización.	Medir el porcentaje de participación de Servidores Públicos y/o Contratistas, en actividades de sensibilización para concientizar sobre la seguridad de la información, y temas de TI.	***NPS:*** *Nivel de participación de Servidores Públicos y/o Contratistas en actividades de sensibilización.* ***SCS:*** *Número de Servidores Públicos y/o Contratistas sensibilizados, en el semestre.* ***SCES:*** *Número de Servidores Públicos y/o Contratistas estimados para ser sensibilizado, en el semestre.*	***NPS = (SCS /SCES) * 100***

Tabla 4 - Indicadores de Seguridad y Privacidad de la Información
Fuente: Hoja de Vida de Indicadores TI

11. Plan de Comunicaciones

La comunicación de las actividades para el desarrollo del Plan Estratégico de Seguridad y Privacidad de la Información (PESPI), y contempla las actividades tanto para socializar el PESPI como los grupos de interés a los que va dirigido. Este capítulo representa el punto de partida para generar confianza en cuanto al origen de la planeación tecnológica de la Entidad y la perspectiva de la Oficina TIC.

11.1. Canales Presenciales

- Presentaciones técnicas y ejecutivas, apoyadas en material visual (presentaciones y/o videos).

11.2. Canales Virtuales

- Publicación y divulgación del PESPI a través de la sede electrónica de la Entidad.

11.3. Grupos de Interés PESPI

- Funcionarios de la Alta Dirección de la Entidad.
- Directores y dueños de los procesos estratégicos, misionales, de apoyo y de evaluación.
- Funcionarios públicos y contratistas que se ven impactados con el PESPI.
- Entidades del estado y privadas.
- Ciudadanía en General.

11.4. Responsables

- El Comité de Gestión y Desempeño será el encargado de la aprobación del Plan Estratégico Seguridad y Privacidad de la Información (PESPI).
- El Líder del proceso Gestión de Tecnología de la Información y las Comunicaciones, será el responsable de la definición, actualización e implementación del Plan Estratégico Seguridad y Privacidad de la Información (PESPI).

11.5. Frecuencia Actualización

El Plan Estratégico Seguridad y Privacidad de la Información (PESPI) será integrado y divulgado a más tardar el 31 de enero de cada año según el decreto 612 de 2018. También, será actualizado y divulgado según las necesidades de la Entidad y acorde a las solicitudes requeridas.