PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE TECNOLOGÍA
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Versión 1

Enero 28 de 2025

CONTENIDO

1. LISTA DE TABLAS 3
2. LISTA DE ILUSTRACIONES 3
3. INTRODUCCIÓN 4
4. INFORMACIÓN GENERAL 4
5. EJE ESTRATÉGICO – OBJETIVO ESTRATÉGICO 4
6. OBJETIVO GENERAL 5
6.1 OBJETIVOS ESPECÍFICOS 5
7. ALCANCE 5
8. DEFINICIONES 6
9. NORMATIVIDAD 9
9.1 ACTUALIZACIÓN NORMOGRAMA OFICINA TIC 9
9.2 PERIODICIDAD DE ACTIVIDADES NORMOGRAMA OFICINA TIC 9
9.3 NORMATIVIDAD RELEVANTE PARA LA CONSTRUCCIÓN PESPI 9
10. FORMULACIÓN DEL PLAN 11
10.1 ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL MSPI 11
10.2 GENERALIDADES DEL PLAN 14
10.3 PORTAFOLIO DE PROYECTOS Y/O ACTIVIDADES 16
10.4 ANÁLISIS PRESUPUESTAL 17
10.5 CRONOGRAMA: CICLO PHVA: FASE - PLANEAR 18
10.6 CRONOGRAMA: CICLO PHVA: FASE – HACER 18
10.7 CRONOGRAMA: CICLO PHVA: FASE – VERIFICAR 19
10.8 CICLO PHVA: FASE – ACTUAR 19
11. SEGUIMIENTO Y EVALUACIÓN 20
11.1 INDICADORES 21
12. PLAN DE COMUNICACIONES 22
12.1 CANALES PRESENCIALES: 22
12.2 CANALES VIRTUALES: 22
12.3 GRUPOS DE INTERÉS PESI: 22
12.4 RESPONSABLES: 22
12.5 FRECUENCIA ACTUALIZACIÓN: 22
13. ANEXOS E INFORMACIÓN COMPLEMENTARIA 22

1. LISTA DE TABLAS

Tabla 1 - Información general del Plan Fuente: Elaboración Propia 4
Tabla 2 - Normatividad para desarrollo e implementación del PESI Fuente: Elaboración Propia.....10
Tabla 3 - Descripción De Las Estrategias Específicas (Ejes) Fuente: Guía Plan Estratégico de Seguridad de la Información.....15
Tabla 4 - Descripción del Portafolio de Proyectos / Actividades Fuente: Guía Plan Estratégico de Seguridad de la Información.....16
Tabla 5 - Catálogo Iniciativas y Proyectos de Seguridad Digital Fuente: "Catalogo de Iniciativas y Proyectos de Transformación Digital" 17
Tabla 6 - Cronograma Ciclo PHVA: Fase – Planear Fuente: Cronograma 2025 - Plan Estratégico de Seguridad y Privacidad de la Información.....18
Tabla 7 - Cronograma Ciclo PHVA: Fase – Hacer Fuente: Cronograma 2025 - Plan Estratégico de Seguridad y Privacidad de la Información.....19
Tabla 8 - Cronograma Ciclo PHVA: Fase – Verificar Fuente: Cronograma 2025 - Plan Estratégico de Seguridad y Privacidad de la Información.....19
Tabla 9 - Cronograma Ciclo PHVA: Fase – Actuar Fuente: Cronograma 2025 - Plan Estratégico de Seguridad y Privacidad de la Información.....20
Tabla 10 - Indicadores de Seguridad y Privacidad de la Información Fuente: Anexo 4 - Tablero de Indicadores de TI 21

2. LISTA DE ILUSTRACIONES

Ilustración 1 - Evaluación de efectividad de Controles - ISO 27001:2013 Fuente: Herramienta-Instrumento de Evaluación MSPI-Portada 11
Ilustración 2 - Brecha Anexo A ISO 27001:2013.....12
Ilustración 3 - Avance Ciclo de Funcionamiento Del Modelo De Operación (PHVA) Fuente: Instrumento de Evaluación MSPI – Portada.....12
Ilustración 4 - Nivel de Madurez MSPI.....13
Ilustración 5 – Gráfico Calificación Frente A Mejores Prácticas En Ciberseguridad (NIST) 13
Ilustración 6 – Hoja de Ruta Adaptada – Productos Tipo de Seguridad de la Información.....14
Ilustración 7 – Estrategia de Seguridad Digital.....14

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 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 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. 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, promoviendo la transparencia, la responsabilidad y la resiliencia ante posibles amenazas.

4. INFORMACIÓN GENERAL

Nombre del Plan de Acción	**Plan Estratégico de Seguridad y Privacidad de la Información 2025**
Nombre y código: **Rubro presupuestal**	**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:** $ 3.650.007.000
Área responsable	Oficina De Tecnología De La Información Y Las Comunicaciones
Política MIPG y otros	Política de Gobierno Digital – Política de Seguridad Digital
Proceso	Gestión De Tecnología De La Información Y Las Comunicaciones
Fecha inicio del plan	02/01/2025
Fecha fin del plan	31/12/2025

Tabla 1 - Información general del Plan
Fuente: Elaboración Propia

5. EJE ESTRATÉGICO – OBJETIVO ESTRATÉGICO

El eje estratégico #7: *Transformación Organizacional*, representa el ámbito de acción que debe ser desarrollado para abordar los retos institucionales desde la Oficina de Tecnología de la Información y las Comunicaciones, definiendo la ruta por la cual transitaremos para llegar al destino que la Caja de Vivienda Popular se ha propuesto y constituye una de las aspiraciones que quiere lograr la Entidad entre los años 2024 al 2028.

El objetivo estratégico # 7: *Fortalecer la capacidad y efectividad administrativa y la innovación organizacional, para la modernización de la Caja de Vivienda Popular y el incremento en la confianza ciudadana en la Entidad;* enmarca la gestión de la Oficina de Tecnología de la Información y las Comunicaciones *y* pone en manifiesto lo que se quiere lograr en la vigencia 2024-2028: La Implementación del 100% del Sistema de Información Misional de la CVP y la Garantía de la Disponibilidad de la Infraestructura Tecnológica.

6. 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 las vigencias 2025-2028. Este enfoque busca asegurar la continuidad de los procesos misionales de la Caja de la Vivienda Popular, alineándose con los objetivos estratégicos de la Entidad, y de esta manera reducir hasta niveles aceptables los riesgos a los que está expuesta la Entidad.

6.1 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** 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 documento Anexo 1 – "208-TIC-Nr-01 NORMOGRAMA-OTIC" que sirve como herramienta para delimitar las normas que regulan la gestión del proceso de la Oficina TIC, 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.

9.1 Actualización Normograma Oficina TIC

Para la actualización del Normograma de la Oficina TIC se recomienda seguir los siguientes pasos:

- Revisar la vigencia de las normas contenidas en el documento publicado.
- Incluir las nuevas normas aplicables al proceso.
- Validar la información con el responsable y el equipo de trabajo del proceso.
- Remitir a la Oficina Asesora de Planeación para consolidación y publicación.

9.2 Periodicidad de Actividades Normograma Oficina TIC

- *Seguimiento:* Trimestral
- *Reporte a Oficina Asesora Planeación:* Semestral
- *Socialización y Publicación:* Semestral.

9.3 Normatividad Relevante Para La Construcción PESPI

A continuación, se hace referencia a la normatividad más relevante a partir de la cual tienen sustento el desarrollo e implementación de este Plan de Seguridad y Privacidad de la Información, y que está incluida en el Normograma de la Oficina TIC, indicado anteriormente:

Se fundamenta 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"
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	Número	Fecha de Emisión			Tipo	Descripción
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".
Norma NTC-ISO/IEC	27001:2013	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.
Norma NTC-ISO/IEC	27001:2022.	25	10	2022	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"
CONPES	3701	14	7	2011	EXTERNO	"Lineamientos De Política Para Ciberseguridad Y Ciberdefensa"
Manual de Gobierno Digital	Decreto 767			2022	EXTERNO	"Es un instrumento centralizado, estandarizado y de fácil uso, donde los usuarios pueden consultar interactivamente información de interés sobre la Política de Gobierno Digital, establecida el 16 de mayo con el Decreto 767 de 2022".
Modelo de Seguridad y Privacidad de la Información – MINTIC.	Resolución 500			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 PESI
Fuente: Elaboración Propia

10. FORMULACIÓN DEL PLAN

10.1 Estado Actual de la Entidad Respecto al MSPI

Para el período comprendido entre el 9 de noviembre de 2022 al 11 de febrero de 2024, se reportó como logro del MSPI, el diseño y la implementación con una efectividad de la evaluación de controles ISO 27001:2013 ANEXO A en un 86%.

Sin embargo, acorde a la medición de FURAG 2023 donde se obtuvo una calificación de 81,9 en el habilitador de Seguridad y Privacidad de la Información, se evidencian en la hoja de ruta el planteamiento de las siguientes acciones de mejora:

I. Implementar el Modelo de Seguridad y Privacidad de la Información.

II. Elaborar un diagnóstico de Seguridad y Privacidad de la información para la Entidad a través de la herramienta de Autodiagnóstico del MSPI. Posteriormente presentar y lograr su aprobación en el Comité de Gestión y Desempeño Institucional.

III. Realizar auditorías internas, externas, y de certificación o recertificación respecto al estándar ISO 27001 en la Entidad.

Los resultados del autodiagnóstico del MSPI, tal como puede observarse en el Anexo 2 – "Informe Técnico Diagnóstico del MSPI"; evidencian en primera instancia, 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 1 - 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 2 - Brecha Anexo A ISO 27001:2013
Fuente: Instrumento de Evaluación MSPI – Portada

En segunda instancia, respecto del avance en el ciclo PHVA, la Caja de la Vivienda Popular obtiene un: 37% en planificación, 16% en implementación, 11% en evaluación y 8% en mejora continua; para un avance total del 72%.

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2024	Planificación	37%	40%
	Implementación	16%	20%
	Evaluación de desempeño	11%	20%
	Mejora continua	8%	20%
TOTAL		72%	100%

Ilustración 3 - Avance Ciclo de Funcionamiento Del Modelo De Operación (PHVA)
Fuente: Instrumento de Evaluación MSPI – Portada

Posteriormente, el nivel de madurez del MSPI es "Definido", con la necesidad de da darle continuidad al fortalecimiento de áreas clave en temas de seguridad de la información, para cada uno de los procesos estratégicos, misionales, de apoyo y de evaluación de la gestión.

		NIVEL DE CUMPLIMIENTO
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	SUFICIENTE
	Repetible	SUFICIENTE
	Definido	SUFICIENTE
	Administrado	INTERMEDIO
	Optimizado	CRÍTICO

Ilustración 4 - Nivel de Madurez MSPI
Fuente: Instrumento de Evaluación MSPI – Portada

Y, además, existen oportunidades de mejora en la protección, detección, respuesta y recuperación ante incidentes de ciberseguridad según las recomendaciones dentro del el Marco de Ciberseguridad NIST.

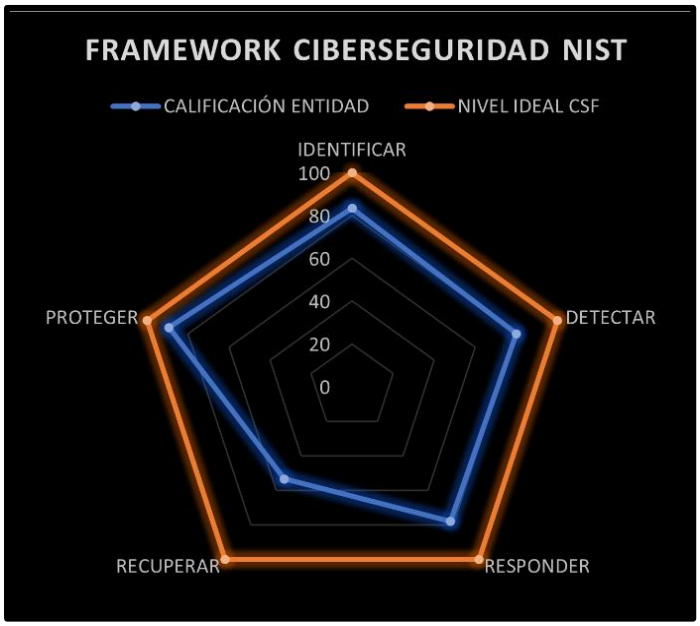

Ilustración 5 – Gráfico Calificación Frente A Mejores Prácticas En Ciberseguridad (NIST)
Fuente: Instrumento de Evaluación MSPI – Portada

En conclusión, se evidencia un buen progreso en la implementación del MSPI, pero se generan algunas recomendaciones para abordar las brechas identificadas mediante la construcción de un plan de acción; para el fortalecimiento del ciclo PHVA, la capacitación del personal de la Entidad, el monitoreo continuo de los controles, la optimización de recursos, el refuerzo en la gestión de incidentes y la actualización de políticas y procedimientos.

10.2 Generalidades del plan

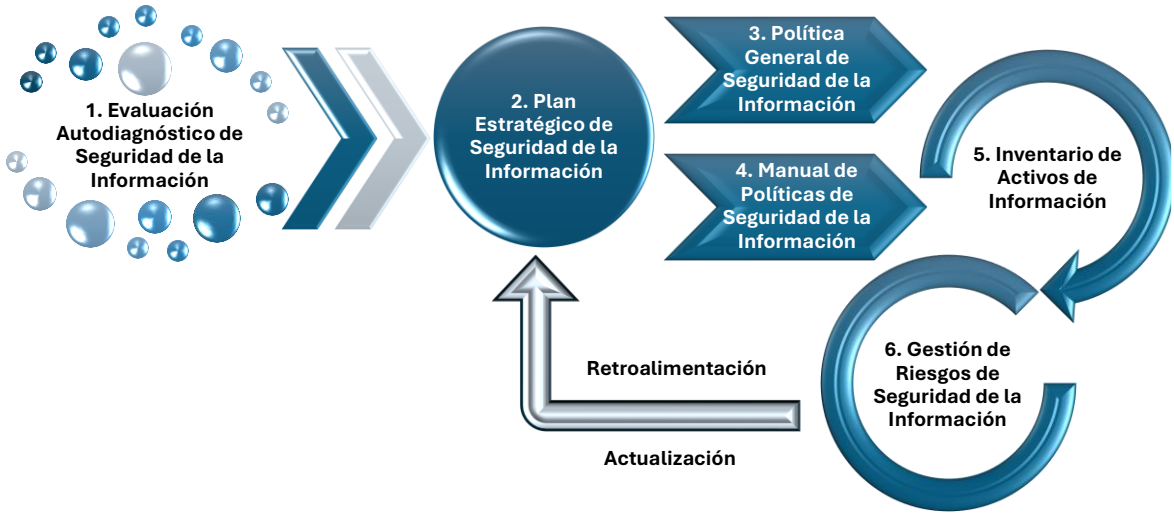

Ilustración 6 – Hoja de Ruta Adaptada – Productos Tipo de Seguridad de la Información
Fuente: Manual de Gobierno Digital – Habilitador: Seguridad y Privacidad de la Información

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.

Ilustración 7 – Estrategia de Seguridad Digital
Fuente: Guía Plan Estratégico de Seguridad de la Información

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del Modelo de Seguridad y Privacidad de la Información y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN / OBJETIVO
Liderazgo de Seguridad de la Información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información de la Caja de la Vivienda Popular, 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.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información de la Caja de la Vivienda Popular y mantener la confianza en la ejecución de los procesos de la Entidad mediante los controles tecnológicos y/o administrativos.
Gestión de riesgos	Determinar los riesgos de seguridad de la información de la Caja de la Vivienda Popular, a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados teniendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Caja de la Vivienda Popular.
Concientización	Fortalecer la construcción de la cultura organizacional en la Caja de la vivienda Popular con base en la seguridad de la información para que se convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la Entidad en seguridad y privacidad de la información.
Continuidad del Negocio	Implementar el Plan de Continuidad de Tecnología de la Información y las Comunicaciones, para que la Caja de la Vivienda Popular pueda tomar las acciones pertinentes con miras a la mitigación del impacto, la recuperación y restablecimiento de los servicios e infraestructuras críticas de Tecnología de la Información, interrumpidas por situaciones de desastre o emergencias ocurridas en cualquier instante dentro de la Entidad.

Tabla 3 - Descripción De Las Estrategias Específicas (Ejes)
Fuente: Guía Plan Estratégico de Seguridad de la Información

10.3 Portafolio de Proyectos y/o Actividades

Para cada estrategia específica, La Caja de la Vivienda Popular define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información (MSPI).

ESTRATEGIA / EJE	PROYECTO	PRODUCTO ESPERADO
Liderazgo de Seguridad de la Información	Actualizar la política de seguridad y privacidad de la información.	Política de Seguridad Formalizada e Implementada.
	Definición de Roles y Responsabilidades de Seguridad de la Información.	Definición de los Roles y Responsabilidades en Seguridad de la Información formalizados dentro de las políticas de seguridad.
Implementación de controles	Actualizar la Política de respaldos de información.	Política de respaldos de información. Actualizada.
	Actualizar el Procedimiento de Gestión de Cambios.	Procedimiento de Gestión de Cambios Actualizado.
	Actualizar la Clasificación de la información.	Inventario y Clasificación de Activos de la información Actualizado.
	Actualizar la documentación referente al MSPI (Políticas, Manuales, Procedimientos, Instructivos, Formatos, guías)	Documentación referente al MSPI Actualizada (Políticas, Manuales, Procedimientos, Instructivos, Formatos, guías).
	Implementación de solución DLP/SOC /WAF	DLP/SOC/WAF desplegado y funcional.
Gestión de riesgos	Identificar, valorar y clasificar los riesgos asociados a los activos de información.	Matriz de riesgos de seguridad digital.
	Definir el Plan de tratamiento de riesgos de seguridad.	Plan de tratamiento de riesgos de seguridad Actualizado.
Gestión de incidentes	Actualizar el procedimiento de Gestión de Incidentes de seguridad de la información.	Procedimiento de gestión de incidentes de seguridad actualizado.
	Capacitar al personal en la gestión de incidentes de seguridad de la información.	Sesiones de capacitación desarrolladas.
Concientización	Establecer desde el inicio de cada año la planeación de sensibilización para todo el año.	Anexo 3 – "Plan de Sensibilización de Seguridad y Privacidad de la Información".
	Realizar jornadas de sensibilización a todo el personal.	Evidencias de las actividades desarrolladas.
	Medir el grado de sensibilización a toda la Entidad.	Resultado de las encuestas de medición.

Tabla 4 - Descripción del Portafolio de Proyectos / Actividades
Fuente: Guía Plan Estratégico de Seguridad de la Información

10.4 Análisis Presupuestal

El análisis financiero se basa en la asignación presupuestal estimada para el Plan Anual de Adquisiciones de la vigencia 2025 y para la definición de los ejes estratégicos del Plan Estratégico de la CVP al 2028.

El desglose del presupuesto estimado de operación y funcionamiento se realiza mediante los dominios de gestión de TI, para los cuales se asocian las actividades de las iniciativas de la Oficina TIC que contribuyen al cumplimiento de las metas del Proyecto de Inversión.

Dentro de la estimación del presupuesto se tienen en cuenta los costos para la contratación de talento humano y prestación de servicios, para la adquisición y/o renovación de infraestructura, para la adquisición y/o renovación de software (licenciamiento), para el soporte y mantenimiento de los sistemas de información y servicios tecnológicos.

Es necesario aclarar que el flujo financiero por tipo de gasto no depende exclusivamente de la Oficina Tecnología de la Información y las Comunicaciones, debido a las modificaciones en la aprobación y distribución de los recursos de la Entidad y/o de las necesidades derivadas de ejecución del proyecto.

Con base a los proyectos definidos en el cronograma de actividades, se genera el presupuesto aproximado por cada uno y se presenta a la Alta Dirección para las consideraciones y viabilidad pertinentes. A continuación, se presenta un resumen del Catálogo de Iniciativas y Proyectos de Transformación Digital:

AÑO 2025		AÑO 2026		AÑO 2027	
Proyecto	**Inversión**	**Proyecto**	**Inversión**	**Proyecto**	**Inversión**
Actualizar los lineamientos técnicos e implementación de controles que se definan en el plan operacional de seguridad y privacidad de la información.	$84.000.000	Implementar el 100% del Modelo de Seguridad y Privacidad de la Información y gestionar la auditoría interna de cumplimiento.	$90.000.000	Mantener el funcionamiento del Modelo de seguridad y privacidad de la Información	$96.000.000
Configuración solución DLP en Correo Institucional	Incluido dentro del licenciamiento de Google Workspace	Adquisición y despliegue de solución DLP a nivel de red.	$20.000.000	Renovación de solución DLP a nivel de red.	$25.000.000
Implementación de solución SOC	$70.000.000	•Implementación de solución WAF / •Renovación solución SOC	$120.000.000	Renovación WAF / SOC	$150.000.000
Gestionar la auditoría interna de cumplimiento.	$5.000.000	Gestionar la preauditoria externa de cumplimiento.	$15.000.000	Gestionar auditoría externa de cumplimiento.	$20.000.000
TOTAL PRESUPUESTO 2025	**$159.000.000**	***TOTAL PRESUPUESTO 2023***	**$245.000.000**	***TOTAL PRESUPUESTO 2024***	**$291.000.000**

Tabla 5 - Catálogo Iniciativas y Proyectos de Seguridad Digital
Fuente: "Catalogo de Iniciativas y Proyectos de Transformación Digital"

10.5 Cronograma: Ciclo PHVA: Fase - Planear

N°	Estrategias / Acciones / Entregables	Fecha Inicio	Fecha Fin
CICLO PHVA: FASE - PLANEAR			
1.	**LIDERAZGO DE SEGURIDAD DE LA INFORMACIÓN**	**02-01-2025**	**31-01-2025**
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 un acto administrativo.*		
1.1.1.1.	Entregable: El acto administrativo que soporta la aprobación de los planes.		
1.2.	***Política de seguridad y privacidad de la información***	**02-01-2025**	**30-04-2025**
1.2.1.	*Actualizar la Resolución de la Adopción de la Política de la Seguridad y Privacidad de la Información. Resolución 4664 de la CVP (12-09-2016).*		
1.2.1.1.	Entregable: *El Acto administrativo con la adopción de la Política de seguridad y privacidad de la información.*		
1.3.	***Roles y responsabilidades***	**02-01-2025**	**30-04-2025**
1.3.1.	*Articular con las áreas o dependencias de la entidad, los roles y responsabilidades necesarios para la adopción del MSPI, el monitoreo del desempeño y el reporte y seguimiento ante el comité institucional de gestión y desempeño, para que sean aprobados y comunicados dentro de la entidad.*		
1.3.1.1.	Entregable: Matriz RACI para la adopción del MSPI.		
2.	**IMPLEMENTACIÓN DE CONTROLES**	**02-01-2025**	**31-12-2025**
2.1.	***Identificación de activos de información e infraestructura critica***	**01-02-2025**	**30-06-2025**
2.1.1.	*Publicar un Procedimiento y/o Documento Metodológico de inventario y clasificación de la información.*		
2.1.1.1.	Entregable: El Procedimiento y/o Documento Metodológico de inventario y clasificación de la información.		
2.1.2.	*Actualizar la identificación de activos de información e infraestructura crítica*		
2.1.2.1.	Entregable: El 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***	**01-03-2025**	**31-07-2025**
2.2.1.	*Actualizar la documentación referente al MSPI (Políticas, Manuales, Procedimientos, Instructivos, Formatos, Guías)*		
2.2.1.1	Entregable: Documentación Actualizada referente al MSPI.		
3.	**GESTIÓN DE RIESGOS**	**02-01-2025**	**15-12-2025**
3.1.	***Valoración de los riesgos de seguridad de la información***		
3.1.1.	*Actualizar el procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité de coordinación de control interno.*		
3.1.1.1.	Entregable: El capítulo de seguridad y privacidad de la información para inclusión en el procedimiento de gestión de riesgos.		
3.2.	***Plan de tratamiento de los riesgos de seguridad de la información***		
3.2.1.	*Actualizar el Plan de tratamiento de riesgos, aprobado por el comité institucional de gestión y desempeño.*		
3.2.1.1.	Entregable: El 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 la Matriz de Riesgos de seguridad de la información y privacidad de la información.*		
3.3.1.1.	Entregable: Matriz de Riesgos de seguridad de la información y privacidad de la información.		

Tabla 6 - Cronograma Ciclo PHVA: Fase – Planear
Fuente: Cronograma 2025 - Plan Estratégico de Seguridad y Privacidad de la Información

10.6 Cronograma: Ciclo PHVA: Fase – Hacer

N°	Estrategias / Acciones / Entregables	Fecha Inicio	Fecha Fin

CICLO PHVA: FASE - HACER			
3.4.	**PRUEBAS DE VULNERABILIDADES**	**01-06-2025**	**31-10-2025**
3.4.1.	*Implementar un Análisis de Vulnerabilidades de seguridad de la información.*		
3.4.1.1.	Entregable: Informe Técnico de Pruebas de Análisis de Vulnerabilidades a un (01) activo de información crítico de TI.		
3.5.	***DECLARACIÓN DE APLICABILIDAD (SOA)***	**01-07-2025**	**31-08-2025**
3.5.1.	*Elaborar y Aprobar la Declaración de aplicabilidad (SOA).*		
3.5.1.1.	Entregable: Declaración de aplicabilidad (SOA).		
4.	**GESTIÓN DE INICIATIVAS/PROYECTOS**	**02-01-2025**	**31-01-2025**
4.1.	***Recursos***		
4.1.1	*Determinar y proporcionar los recursos necesarios para adoptar el MSPI*		
4.1.1.1.	Entregable: Catalogo de Iniciativas y/o Proyectos de Seguridad y Privacidad de la Información.		
5.	**GESTIÓN DE INCIDENTES**	**02-01-2025**	**31-12-2025**
5.1.	***Implementar un Modelo de Gestión de Incidentes de seguridad de la información***		
5.1.1.	*Actualizar el Procedimiento de Gestión de Incidentes*		
5.1.1.1.	Entregable: El Procedimiento de Gestión de Incidentes y Sesiones de Capacitación desarrolladas.		
5.1.2.	*Implementar soluciones para detectar, analizar, responder y prevenir incidentes de seguridad, en tiempo real en la Entidad.*		
5.1.2.1.	Entregable: Solución SOC Implementada (Centro de Operaciones de Seguridad)		
6.	**CONCIENTIZACIÓN**	**03-02-2025**	**30-10-2025**
6.1.	***Competencia, toma de conciencia y comunicación***		
6.1.1.	*La entidad debe definir un plan de comunicación, capacitación, sensibilización y concientización del modelo de seguridad y privacidad de la información.*		
6.1.1.1.	Entregable: El Plan de Sensibilización de seguridad y privacidad de la Información y Sesiones de Capacitación/Sensibilización desarrolladas.		
7.	**ANÁLISIS DE IMPACTO DE NEGOCIOS BIA**	**03-02-2025**	**15-12-2025**
7.1.	***Continuidad del Negocio***		
7.1.1.	*Actualizar el Plan de Continuidad de Tecnología de la Información y las Comunicaciones, aprobado por el comité institucional de gestión y desempeño.*		
7.1.1.1.	Entregable: El Plan de Continuidad de TIC		

Tabla 7 - Cronograma Ciclo PHVA: Fase – Hacer
Fuente: Cronograma 2025 - Plan Estratégico de Seguridad y Privacidad de la Información

10.7 Cronograma: Ciclo PHVA: Fase – Verificar

N°	Estrategias / Acciones / Entregables	Fecha Inicio	Fecha Fin
CICLO PHVA: FASE - VERIFICAR			
8.	**SEGUIMIENTO Y EVALUACIÓN**	**02-01-2025**	**31-12-2025**
8.1.	***Seguimiento a Implementación del MSPI***		
8.1.1	*Conocer de manera semestral los avances en la gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital.*		
8.1.1.1.	Entregable: Presentación del Seguimiento del MSPI y PTRSPI.		
8.1.2.	*Realizar auditorías internas con el fin de obtener información sobre el cumplimiento del MSPI.*		
8.1.2.1.	Entregable: Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información.		
8.1.3.	*Los temas de seguridad y privacidad de la información, seguridad digital y en especial la Política y el Manual de Políticas de Seguridad y Privacidad de la Información deben ser tratados y aprobados en el comité institucional de gestión y desempeño, o cuando el nominador lo determine.*		
8.1.3.1.	Entregable: Acta, documento y compromisos de la revisión por la Alta Dirección.		

Tabla 8 - Cronograma Ciclo PHVA: Fase – Verificar
Fuente: Cronograma 2025 - Plan Estratégico de Seguridad y Privacidad de la Información

10.8 Ciclo PHVA: Fase – Actuar

N°	Estrategias / Acciones / Entregables	Fecha	Fecha

		Inicio	Fin
CICLO PHVA: FASE - ACTUAR			
9.	**MEJORAMIENTO CONTINUO**	**01-08-2025**	**31-12-2025**
9.1.	***Plan de Mejoramiento***		
9.1.1	*Implementar estrategias de mejoramiento continuo con el fin de realizar acciones correctivas, optimizar procesos o controles y mejorar el nivel de madurez del MSPI; acorde con las alertas y observaciones emitidas por el Comité de Coordinación de Control Interno*		
9.1.1.1.	Entregable: Seguimiento del nivel de madurez del MSPI.		
9.1.2.	*Implementar un plan de remediación de vulnerabilidades con el fin de realizar acciones para la mitigación de vulnerabilidades; acorde con el resultado, alertas y observaciones generadas de la ejecución del análisis de vulnerabilidades.*		
9.1.2.1.	Entregable: Plan de Remediación de Vulnerabilidades.		
9.1.3.	*Actualizar el Plan Estratégico de Seguridad y Privacidad de la Información, aprobado por el comité institucional de gestión y desempeño.*		
9.1.3.1.	Entregable: Plan Estratégico de Seguridad y Privacidad de la Información.		
9.1.3.	*Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, aprobado por el comité institucional de gestión y desempeño.*		
9.1.3.1.	Entregable: Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.		

Tabla 9 - Cronograma Ciclo PHVA: Fase – Actuar
Fuente: Cronograma 2025 - Plan Estratégico de Seguridad y Privacidad de la Información

11. SEGUIMIENTO Y EVALUACIÓN

La definición de los indicadores está alineada con los objetivos institucionales y de la Oficina TIC, acorde a la programación de metas establecidas en el Proyectos de Inversión de la Caja, para permitir tener una visión de los avances y resultados en el desarrollo de la Estrategia y la gestión integral de la Oficina TIC.

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 entidad.
- ✓ Comunicar valores de seguridad y privacidad de la información al interior de la entidad.
- ✓ Servir como insumos al plan de análisis y tratamiento de riesgos.

11.1 Indicadores

El detalle de indicadores para el proceso de la Oficina de Tecnología de la Información y las Comunicaciones se encuentra en el documento: Anexo 4 - "Tablero de Indicadores TI".

INDICADORES PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN					
Categoría Indicador	**Tipo Indicador**	**Nombre del Indicador**	**Descripción**	**Variables**	**Fórmulas**
Eficacia	Estratégico	Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).	Establecer el porcentaje de cumplimiento cronograma del Modelo de Seguridad y Privacidad de la Información.	***PCMSPI:*** *Porcentaje cumplimiento cronograma de Modelo de Seguridad y Privacidad de la Información.* ***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.*	***PCMSPI = (AE/AP) *100*** *CUMPLIMIENTO 100%:* *(Índice de Cumplimiento > 90%)*
Efectividad	Cumplimiento	Cumplimiento de Políticas de Seguridad y Privacidad de la Información	Identificar el nivel de estructuración de los procesos de la Entidad orientados a la seguridad de la información.	***VSI01:*** *¿La entidad ha definido una política general de seguridad de la información?* ***VSI02:*** *¿La entidad ha definido una organización interna en términos de personas y responsabilidades con el fin de cumplir las políticas de seguridad de la información y documenta estas actividades?* ***VSI03:*** *¿La entidad cumple con los requisitos legales, reglamentarios y contractuales con respecto al manejo de la información?* ***VSI04:*** *¿La entidad ha identificado y clasificado los activos de información e infraestructura crítica?* ***VSI05:*** *¿La entidad ha identificado y realizado el tratamiento, a los riesgos asociados a seguridad de la información?*	***VSIXX = 1 (SÍ se evidencia: CUMPLE)*** ***VSIXX = 0 (NO se evidencia: NO CUMPLE)*** *CUMPLIMIENTO 100%:* *(Índice de Cumplimiento = 1)*
Eficiencia	De Gestión	Implementación de Controles de Seguridad y Privacidad de la Información	Identificar el grado de avance en la implementación de controles de seguridad.	***PCIC:*** *Porcentaje cumplimiento de Controles Implementados de Seguridad y Privacidad de la Información.* ***CI:*** *Número de controles implementados, durante el período de tiempo analizado.* ***CP:*** *Número de controles planeados, durante el período de tiempo analizado.*	***PCIC: = (CI/CP) *100*** *CUMPLIMIENTO 100%:* *(Índice de Cumplimiento > 90%)*
Eficiencia	De Gestión	Implementación de Plan de Sensibilización de Seguridad y Privacidad de la Información	Calcular la efectividad del plan de sensibilización previamente definido como medio para el control de incidentes de seguridad.	***PCPS:*** *Porcentaje cumplimiento cronograma de Plan de Sensibilización de Seguridad y Privacidad de la Información.* ***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.*	***PCPSSPI: = (AE/AP) *100*** *CUMPLIMIENTO 100%:* *(Índice de Cumplimiento > 90%)*

Tabla 10 - Indicadores de Seguridad y Privacidad de la Información
Fuente: Anexo 4 - Tablero de Indicadores de TI

12. PLAN DE COMUNICACIONES

La comunicación de los resultados del desarrollo del Plan Estratégico de Seguridad y Privacidad de la Información (PESPI) y su puesta en marcha, 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 para los próximos cuatro años.

12.1 Canales Presenciales:

- ✓ Presentaciones técnicas y ejecutivas, apoyadas en material visual (presentaciones y/o videos).
- ✓ Talleres de sensibilización y apropiación del PESPI.

12.2 Canales Virtuales:

- ✓ Publicación y divulgación del PESPI a través de la sede virtual y carteleras digitales de la Entidad.
- ✓ Boletines Informativos comunicados mediante correo institucional.

12.3 Grupos de Interés PESI:

- ✓ 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.

12.4 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).

12.5 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.

13. ANEXOS E INFORMACIÓN COMPLEMENTARIA

Anexo 1 – “208-TIC-Nr-01 Normograma-OTIC”
Anexo 2 – “Informe Técnico Diagnóstico del MSPI”
Anexo 3 – “Plan de Sensibilización de Seguridad y Privacidad de la Información”.
Anexo 4 – “Tablero de Indicadores TI”