PLAN DE TRATAMIENTO DE RIESGOS 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

2. LISTA DE ILUSTRACIONES

3. INTRODUCCIÓN

En un entorno cada vez más digitalizado y globalizado, la seguridad y privacidad de la información se han convertido en pilares fundamentales para la gestión efectiva de cualquier organización, especialmente en entidades públicas como la Caja de la Vivienda Popular (CVP). La información, considerada uno de los activos más valiosos, requiere de prácticas y estrategias sólidas que permitan proteger su integridad, confidencialidad y disponibilidad, asegurando así la continuidad de los procesos institucionales y el cumplimiento de los objetivos misionales.

La creciente sofisticación de las amenazas cibernéticas, los riesgos asociados a accesos no autorizados y la vulnerabilidad ante la pérdida o alteración de datos sensibles obligan a la implementación de lineamientos claros de seguridad y privacidad. Estos lineamientos deben estar fundamentados en normativas vigentes, tanto a nivel nacional como internacional.

La presente propuesta establece directrices específicas para la protección de los activos de información de la CVP, mediante la definición de políticas, controles y mecanismos efectivos. Dichas medidas buscan mitigar riesgos, prevenir incidentes de seguridad y garantizar la continuidad operativa de los procesos críticos, fortaleciendo la confianza de los ciudadanos y demás partes interesadas en la Entidad.

4. INFORMACIÓN GENERAL

Nombre del Plan de Acción	**Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información**
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

- Establecer los lineamientos de buenas prácticas en seguridad y privacidad de la información, con el fin de garantizar la integridad, confidencialidad y disponibilidad de los activos de información de la Caja de la Vivienda Popular (CVP).

- Implementar políticas, controles y mecanismos adecuados que permitan mitigar riesgos, prevenir accesos no autorizados, proteger los datos sensibles, y asegurar la continuidad operativa de los procesos críticos, en cumplimiento de las normativas vigentes y los estándares reconocidos de seguridad de la información.

- Planificar la evaluación y hacer seguimiento de la gestión de los riesgos de seguridad de la información, con el fin de asegurar la disponibilidad de los servicios críticos de TI y mitigar las interrupciones, que aportan a la eficiencia operativa de la Caja de la Vivienda Popular.

- 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 gestión de riesgos de seguridad de la información, contribuyendo al cumplimiento de los objetivos estratégicos de la Entidad.

7. ALCANCE

El **Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)** 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 los lineamientos para la gestión de riesgos de seguridad y privacidad 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; 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 y privacidad de la información, en el 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 por medio de la implementación de controles.

Finalmente, se propenderá por una correcta evaluación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de la Entidad; consolidando la información necesaria para los reportes de gestión.

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 PTRSPI

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 Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI), 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
Guía DAFP A.R.G.C.S.I.	Versión 6		11	2022	EXTERNO	Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas. Versión 6 – Noviembre de 2022
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".
Ley	1581	17	10	2012	EXTERNO	"Por la cual se dictan disposiciones generales para la protección de datos personales".
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 PTRSPI
Fuente: Elaboración Propia

10. FORMULACIÓN DEL PLAN

La Caja de la Vivienda Popular cuenta con una Política de Administración de Riesgos, integrada al Proceso de Gestión Estratégica, que establece un esquema adaptado a los procesos institucionales para apoyar el logro de los objetivos y la mejora continua. Esta política permite gestionar la incertidumbre mediante el uso de información y conocimiento para tomar decisiones acertadas frente a eventos y efectos adversos.

Adicionalmente, incluye la Política de Administración de Riesgos de Seguridad de la Información, orientada a mitigar los riesgos relacionados con los activos de información de la Entidad.

10.1 Generalidades del Plan

La política de seguridad de la información se vincula al modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Gobierno Digital, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital. La Caja de la Vivienda Popular cuenta con la mediante el liderazgo de la Oficina de Tecnología de la Información y las Comunicaciones, establece los lineamientos y metodología para el manejo de los riesgos de seguridad y privacidad de la información, con el propósito de salvaguardar la integridad, confidencialidad y disponibilidad de la información de la Entidad.

Conforme lo indica el ámbito de aplicación del Decreto 1078 de 2015 respecto a la estrategia de Gobierno Digital, las entidades públicas deben realizar la implementación del *Modelo de Seguridad y Privacidad de la Información (MSPI)* con el objetivo de implementar un Sistema de Gestión de Seguridad de la Información al interior de la Entidad.

El *MSPI* integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad de la información, ya que esta práctica constituye su base fundamental. Junto a la guía para la gestión del riesgo de función pública, llevarán a cumplir dichas tareas de gestión de riesgo de seguridad de la información requeridas en el *MSPI*.

En esencia, la interacción entre ambos modelos puede resumirse de la siguiente manera:

- Las actividades de identificación de activos, identificación, análisis, evaluación y tratamiento de los riesgos se alinean con la fase de PLANIFICACIÓN del MSPI.

- Las actividades de implementación de los planes de tratamiento de riesgos se alinean con la fase de IMPLEMENTACIÓN del MSPI.

- Las actividades de monitoreo y revisión, revisión de los riesgos residuales, efectividad de los planes de tratamiento o los controles implementados y auditorías se alinean con la fase de EVALUACIÓN DEL DESEMPEÑO del MSPI.

- Las actividades de MEJORAMIENTO CONTINUO en ambos modelos son similares y trabajan simultáneamente, ya que dependerán de las fases de Medición del Desempeño para identificar aspectos a mejorar en la aplicación de ambos Modelos.

A continuación, se ilustra en que acciones del MPSI se tendrá interacción directa con el Modelo de Gestión de Riesgos de Seguridad de la información:

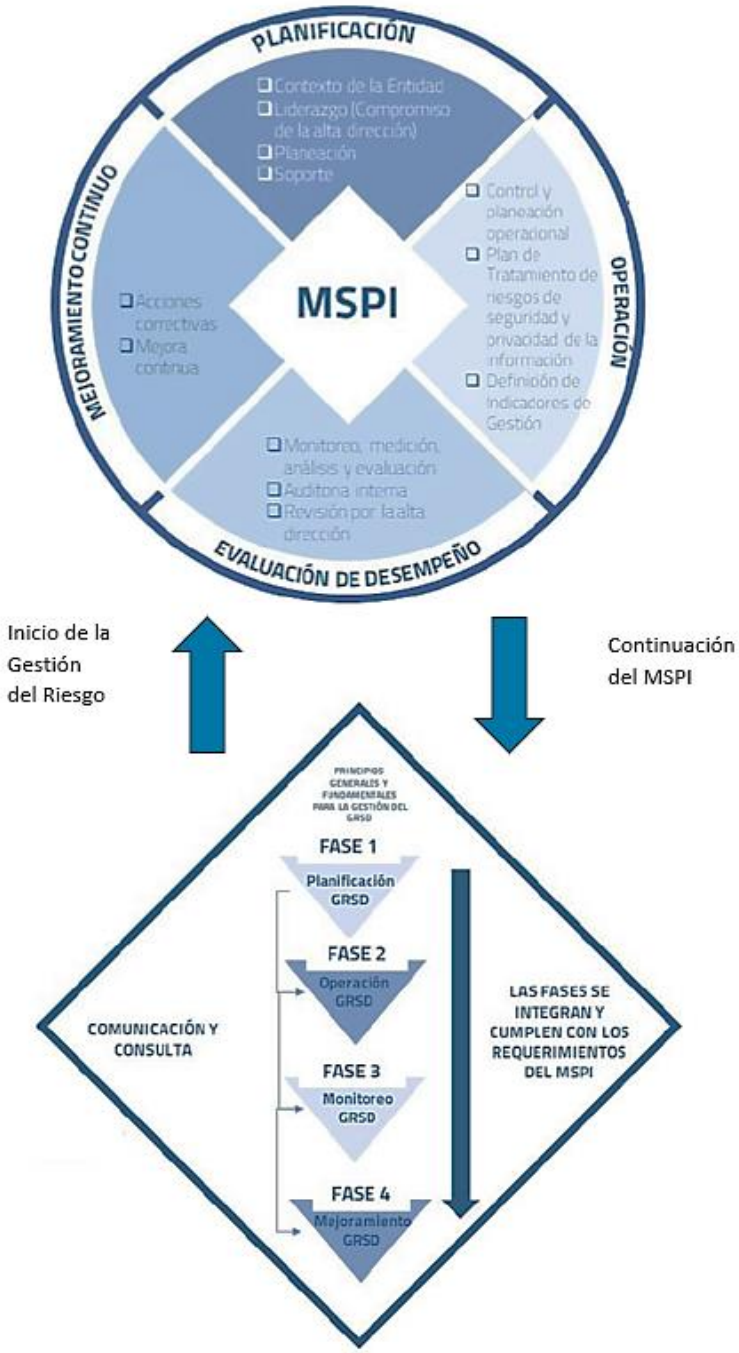

Ilustración 1 - Integración del modelo de seguridad y privacidad de la Información (MSPI)
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

La metodología para el tratamiento de riesgos de seguridad y privacidad de la información en los procesos y actividades de la Entidad está integrada en la Política de Administración del Riesgo, la cual establece los criterios para definir el nivel de impacto y el nivel de probabilidad (mínimas y máximas frecuencias de ocurrencia), permitiendo identificar, valorar y gestionar los riesgos hasta alcanzar niveles aceptables, garantizando un seguimiento continuo para prevenir su materialización.

10.1.1 Criterio de Impacto

	Afectación Económica	Afectación Reputacional
Leve 20%	Afectación menor al 1,3% del presupuesto asignado para la Entidad	El riesgo afecta la imagen de una o más áreas de la Entidad.
Menor (40%)	Afectación entre el 1,3% y el 2,4% del presupuesto asignado para la Entidad	El riesgo afecta la imagen de la entidad a nivel interno y de una población especifica.
Moderado (60%)	Afectación entre 2,5% el 3,6% del presupuesto asignado para la Entidad	El riesgo afecta la imagen de la entidad a nivel de la población beneficiaria, del consejo directivo y/o de proveedores.
Mayor (80%)	Afectación entre 3,7% y el 4,8% del presupuesto asignado para la Entidad	El riesgo afecta la imagen de la entidad a nivel sectorial, de la población beneficiaria y frente a actores de relevancia para el logro de los objetivos institucionales.
Catastrófico (100%)	Afectación del 4,9% o mas del presupuesto asignado para la Entidad	El riesgo afecta la imagen de la entidad con efecto en medios de comunicación sostenido a nivel del Distrito Capital y la ciudadanía en general.

Ilustración 2 - Criterio de Impacto

Fuente: Adaptación Guía para la administración del riesgo y el diseño de controles en entidades públicas - V6.

10.1.2 Criterio de Frecuencia

	Frecuencia de la Actividad	Probabilidad
Muy Baja (20%)	La actividad que conlleva el riesgo se ejecuta como máximos 10 veces por año	20%
Baja (40%)	La actividad que conlleva el riesgo se ejecuta de 11 a 100 veces por año	40%
Media (60%)	La actividad que conlleva el riesgo se ejecuta de 101 a 250 veces por año	60%
Alta (80%)	La actividad que conlleva el riesgo se ejecuta de 251 a 500 veces por año	80%
Muy alta (100%)	La actividad que conlleva el riesgo se ejecuta más de 500 veces por año	100%

Ilustración 3 – Criterio de Frecuencia

Fuente: Adaptación Guía para la administración del riesgo y el diseño de controles en entidades públicas - V6.

10.1.3 Mapa de Calor Riesgos

Luego de desarrollar el análisis y definir la probabilidad de ocurrencia y el impacto ante la materialización de un riesgo, se debe evaluar estos dos criterios a través de su combinación, para definir la zona de calor en la cual está ubicado el riesgo inherente (Ubicación dentro del mapa de calor).

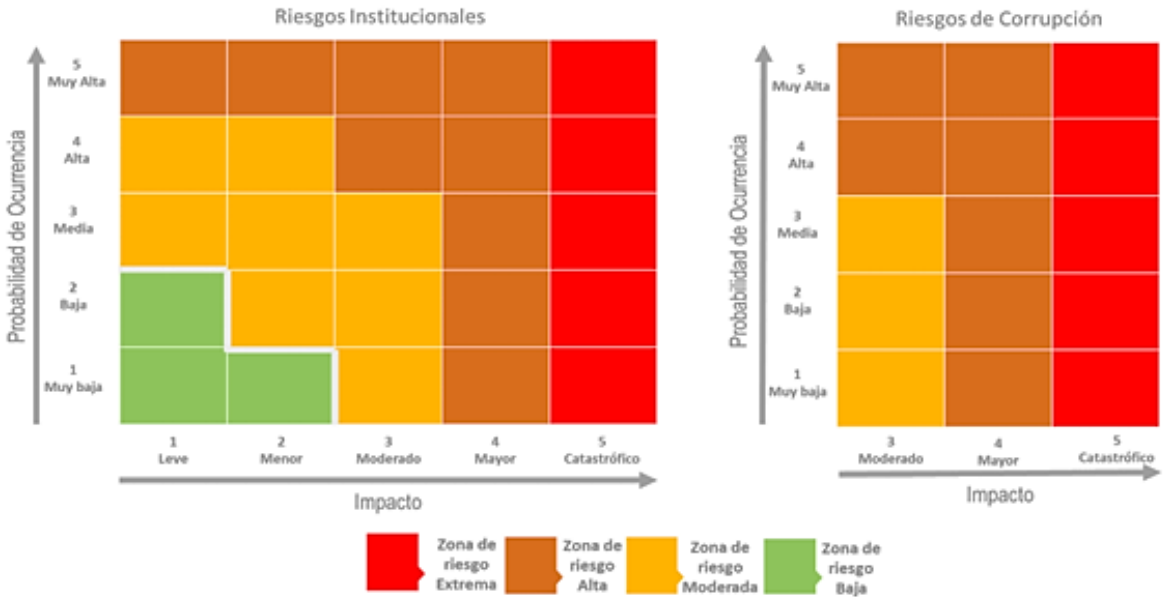

Ilustración 4 - Mapa de Calor de Riesgos
Fuente: Departamento Administrativo de la Función Pública – 2023

10.1.4 Opción de Tratamiento de Riesgos

- *Aceptar el riesgo (Asumir):* No se implementan medidas que modifiquen la probabilidad o el impacto del riesgo. Esta opción solo es viable cuando el riesgo residual se encuentra clasificado en una zona de calor "Baja" o "Muy Baja".

- *Reducir el riesgo:* El nivel de riesgo se gestiona mediante la implementación de controles que permitan reevaluar el riesgo residual hasta que sea aceptable para la Entidad. Estos controles están diseñados para disminuir la probabilidad y/o el impacto del riesgo.

- *Evitar el riesgo:* Cuando los escenarios de riesgo identificado se consideran demasiado extremos, se puede optar por evitarlo mediante la cancelación de una actividad o conjunto de actividades relacionadas. Aunque esta medida es simple y puede ser la menos arriesgada y costosa desde el punto de vista de los responsables de la toma de decisiones, también puede limitar el desarrollo de las actividades de la Entidad, por lo que no siempre resulta una opción viable.

- *Compartir el riesgo:* Cuando la Entidad encuentra dificultades para reducir el riesgo a un nivel aceptable o carece de los conocimientos necesarios para gestionarlo, puede optar por compartirlo con otra parte interesada que tenga la capacidad de manejarlo con mayor eficacia. Es importante destacar que, aunque el riesgo se comparta, la responsabilidad última sobre el mismo generalmente no se transfiere.

10.2 Plan de Tratamiento de Riesgos de Seguridad de la Información

El presente plan se elabora con base en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP) V6, la Política de Administración del Riesgo vigente de la Caja de la Vivienda Popular (CVP), el Modelo de Seguridad y Privacidad de la Información (MSPI), y la estrategia de seguridad digital. En cumplimiento de la Resolución 500 del 10 de marzo de 2021; este plan se integra con el Plan Estratégico de Tecnología de la Información y las Comunicaciones, y el Plan de Seguridad y Privacidad de la Información, asegurando un enfoque coordinado y alineado con las mejores prácticas y lineamientos normativos.

Los riesgos de seguridad y privacidad de la información se fundamentan en la posible afectación de tres (3) criterios esenciales asociados a un activo o conjunto de activos dentro de un proceso: integridad, confidencialidad y disponibilidad.

10.2.1 Lineamientos para la Gestión de Riesgos

- **Compromiso Institucional**:
  La Entidad se compromete a gestionar los riesgos de seguridad de la información mediante la identificación, análisis, tratamiento y monitoreo continuo de los eventos que puedan comprometer su plataforma estratégica, objetivos institucionales y procesos.

- **Evaluación Periódica de Riesgos**:
  Realizar evaluaciones periódicas para identificar y priorizar los riesgos asociados a la seguridad de la información, considerando los criterios de confidencialidad, integridad y disponibilidad de los activos de información.

- **Establecimiento de Controles**:
  Diseñar e implementar controles técnicos, organizativos y administrativos que permitan mitigar los riesgos a niveles aceptables para la Entidad.

- **Responsabilidad Compartida**:
  Definir roles y responsabilidades claras en la gestión de riesgos, asegurando la participación de las áreas involucradas y de los responsables de la toma de decisiones.

- **Cumplimiento Normativo**:
  Alinear la gestión de riesgos a las normativas legales, regulatorias y estándares internacionales aplicables, tales como la Ley 1581 de 2012, el Decreto 2157 de 2017 e ISO/IEC 27001, entre otros.

- **Capacitación y Sensibilización**:
  Promover una cultura de gestión de riesgos mediante programas de formación y sensibilización que fortalezcan la capacidad del personal para identificar y responder a amenazas.

- **Monitoreo y Mejora Continua**:
  Implementar un sistema de monitoreo y evaluación constante que permita ajustar las estrategias y controles en función de la evolución de las amenazas y vulnerabilidades.

- **Planes de Contingencia y Continuidad**:
  Incluir los riesgos identificados en los planes de contingencia y continuidad del negocio, asegurando la resiliencia operativa ante eventos adversos.

Estos lineamientos buscan garantizar una gestión efectiva de los riesgos de seguridad de la información, protegiendo los activos críticos y fortaleciendo la confianza en los servicios ofrecidos por la entidad. Por ello con el fin de lograr esta tarea para darle más cohesión y claridad se proponen las siguientes actividades para evaluar los riesgos de seguridad de la información en la Caja de la Vivienda Popular:

- Se deben identificar los activos de información asociados a cada proceso con el fin de lograr una gestión integral de los riesgos.

- Es necesario generar grupos de activos con el fin de facilitar la medición y evaluación del riesgo, optimizando el análisis por categorías.

- Se deben identificar las vulnerabilidades de los activos con el fin de determinar los puntos débiles que podrían ser explotados.

- Se deben identificar las amenazas que afectan a los activos con el fin de establecer las posibles fuentes de riesgos.

- Es fundamental identificar los riesgos asociados a los activos con el fin de obtener un panorama claro de las posibles afectaciones, y realizar una descripción detallada de los riesgos con el fin de documentar su naturaleza y posibles impactos.

- Se debe analizar la probabilidad y el impacto de ocurrencia de los riesgos con el fin de priorizarlos adecuadamente; además de calcular el riesgo inherente con el fin de determinar el nivel de exposición inicial antes de aplicar controles.

- Se deben aplicar controles específicos a los riesgos identificados con el fin de reducir su probabilidad o impacto a niveles aceptables.

- Los controles implementados deben incluir una frecuencia de aplicación claramente definida con el fin de garantizar su efectividad continua.

- La tolerancia al riesgo corresponde al nivel que la Entidad puede o está dispuesta a soportar. Esto aplica a los riesgos que se encuentren en zona residual "Baja", mientras que los riesgos en otras zonas serán tratados con el fin de alinearse con los lineamientos establecidos en el procedimiento de Gestión de Riesgos de la Caja de la Vivienda Popular.

- Los riesgos identificados deben ser monitoreados permanentemente con el fin de asegurar que los controles implementados sean eficaces y eficientes, y para obtener información que permita mejorar la evaluación y gestión de estos.

10.2.2 Controles de Seguridad de la Información

Como lo indica la Guía de DAFP, arriba mencionada, una vez establecidos y valorados los riesgos inherentes, la Caja de la Vivienda Popular procederá a la identificación y evaluación de los controles existentes para evitar trabajo o costos innecesarios, para lo cual se tendrá como un insumo base los controles del Anexo A de la ISO/IEC 27001:2013, estos controles se encuentran en el Anexo 2 - “Capítulo 11.1. Controles y objetivos de control, del Documento Maestro del MSPI”.

10.2.3 Cronograma

N°	Estrategias / Acciones / Entregables	Fecha Inicio	Fecha Fin
1.	**GESTIÓN DE RIESGOS**	**02-01-2025**	**31-12-2025**
1.1.	***Valoración de los riesgos de seguridad de la información***	**02-01-2025**	**15-12-2025**
1.1.1.	*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.*		
1.1.1.1.	Entregable: El capítulo de seguridad y privacidad de la información para inclusión en el procedimiento de gestión de riesgos.		
1.2.	***Plan de tratamiento de los riesgos de seguridad de la información***	**02-01-2025**	**31-01-2025**
1.2.1.	*Actualizar el Plan de tratamiento de riesgos, aprobado por el comité institucional de gestión y desempeño.*		
1.2.1.1.	Entregable: El Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información (PTRSPI).		
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.		
2.3.	***Identificación de los riesgos de seguridad de la información***	**01-07-2025**	**30-11-2025**
2.3.1.	*Actualizar la Matriz de Riesgos de seguridad de la información y privacidad de la información.*		
2.3.1.1.	Entregable: Matriz de Riesgos de seguridad de la información y privacidad de la información.		
2.4.	***Pruebas de Vulnerabilidades***	**01-06-2025**	**31-10-2025**
2.4.1.	*Implementar un Análisis de Vulnerabilidades de seguridad de la información.*		
2.4.1.1.	Entregable: Informe Técnico de Pruebas de Análisis de Vulnerabilidades a un (01) activo de información crítico de TI.		
2.5.	***Declaración de Aplicabilidad (SOA)***	**01-07-2025**	**31-08-2025**
2.5.1.	*Elaborar y Aprobar la Declaración de aplicabilidad (SOA).*		
2.6.1.	Entregable: Declaración de aplicabilidad (SOA).		
3.	**SEGUIMIENTO Y EVALUACIÓN**	**02-01-2025**	**31-12-2025**
3.1.	***Seguimiento al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI)***	**02-01-2025**	**31-12-2025**
3.1.1	*Conocer de manera anual 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.*		
3.1.1.1.	Entregable: Seguimiento del PTRSPI.		
4.	**MEJORAMIENTO CONTINUO**	**01-11-2025**	**01-11-2025**
4.1.1.	*Actualizar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, aprobado por el comité institucional de gestión y desempeño.*	**01-11-2025**	**31-12-2025**
4.1.1.1.	Entregable: Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información.		

Tabla 3 – Cronograma de Actividades
Fuente: Elaboración Propia

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 formula el indicador que servirá 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 al tratamiento de riesgos de seguridad y privacidad de la información.

11.1.1 Indicador

El objetivo del proceso de seguimiento y evaluación es determinar la eficacia del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información al interior de la entidad, mediante el siguiente indicador:

Indicador Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información					
Categoría Indicador	**Tipo Indicador**	**Nombre del Indicador**	**Descripción**	**Variables**	**Fórmulas**
Eficacia	*Estratégico*	*Implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI).*	Establecer el porcentaje de cumplimiento cronograma del PTRSPI.	***PCPTRSPI:*** *Porcentaje cumplimiento cronograma PTRSPI* ***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.*	***PCPTRSPI = (AE/AP) *100*** *CUMPLIMIENTO 100%:* *(Índice de Cumplimiento > 90%)*

Tabla 4 - Indicador Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
Fuente: Tablero de Indicadores de TI

11.1.2 Reporte de la gestión del riesgo: A Línea Estratégica y Líneas de Defensa

Alineado a la Política de Gestión del Riesgo de la Entidad, el responsable de seguridad digital deberá realizar seguimiento y reportes, periódicamente a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno), y a las partes interesadas; con el fin de consolidar la siguiente información para determinar la aplicación y efectividad de los controles Asociados a los riesgos:

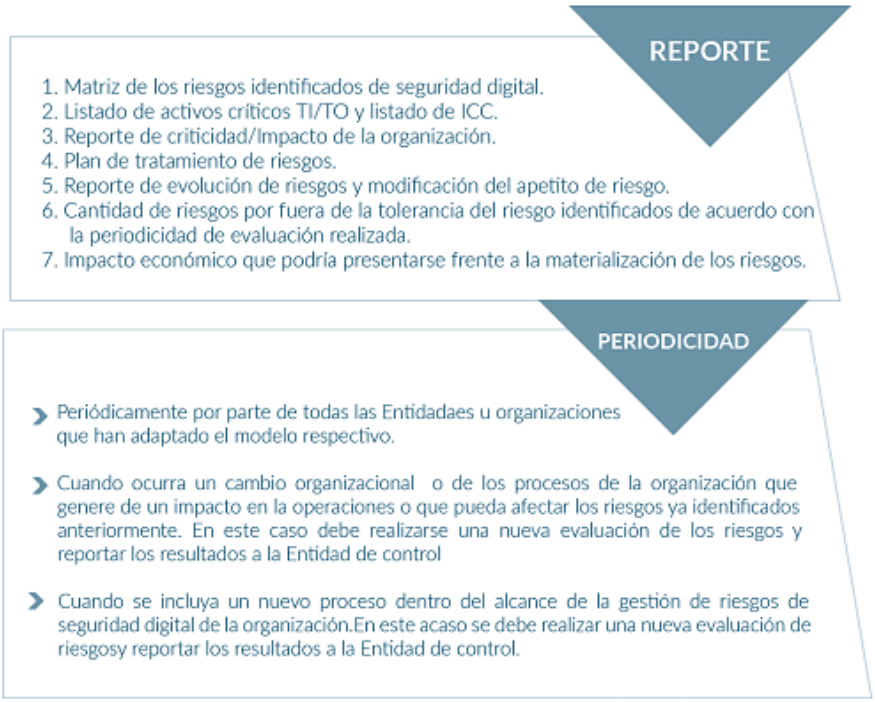

Ilustración 5 - Reportes de Información por parte de la Entidad

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

12. PLAN DE COMUNICACIONES

La comunicación de los resultados del desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) y su puesta en marcha, contempla las actividades tanto para socializar el PTRSPI como los grupos de interés a los que va dirigido.

12.1 Canales Presenciales:

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

12.2 Canales Virtuales:

- ✓ Publicación y divulgación del PTRSPI 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 PTRSPI.
- ✓ 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 de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI).
- ✓ El Líder del proceso Gestión de Tecnología de la Información y las Comunicaciones, será el responsable de la definición, actualización e implementación Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI).

12.5 Frecuencia Actualización:

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSPI) 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 - "Capítulo 11.1. Controles y objetivos de control, del Documento Maestro del MSPI".