Diana Carolina Donoso Casas

 ddonosoc@cajaviviendapopular.gov.co

Oficina de Tecnologías de la Información y las Comunicaciones

Bogotá D.C., Julio de 2018

Versión 1.0

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAJA DE LA VIVIENDA POPULAR

**TABLA DE CONTENIDO**

[1. OBJETIVO 2](#_Toc520717095)

[2. ALCANCE 2](#_Toc520717096)

[3. RESPONSABLES 2](#_Toc520717097)

[4. DEFINICIONES 3](#_Toc520717098)

[5. DOCUMENTOS DE REFERENCIA 5](#_Toc520717099)

[6. ANTECEDENTES 6](#_Toc520717100)

[6.1. Política de Seguridad Informática 6](#_Toc520717101)

[6.2. Inventario de Activos de Información 7](#_Toc520717102)

[6.3. Política de Tratamiento de Datos 7](#_Toc520717103)

[6.4. Plan de Tratamiento de Riesgos 8](#_Toc520717104)

[7. DIAGNÓSTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 8](#_Toc520717105)

[8. PLAN 11](#_Toc520717106)

[9. CONTROL DE CAMBIOS 15](#_Toc520717107)

# **OBJETIVO**

Diseñar e implementar un Plan de Seguridad y Privacidad de la Información, alineado a los requisitos de la Política de Gobierno Digital y la aplicación de la norma ISO 27001:2013, que coadyuve a salvaguardar la disponibilidad, integridad y confidencialidad de los activos de información, con el propósito de garantizar la continuidad en los procesos misionales de La Caja de la Vivienda Popular.

# **ALCANCE**

La Caja de la Vivienda Popular produce, recibe, maneja, intercambia y divulga información clasificada, reservada y pública, relacionada con la población de estratos 1 y 2 que habita en barrios de origen informal o en zonas de riesgo, así como la de sus funcionarios, contratistas y/o terceros.

Este Plan de Seguridad y Privacidad de la Información, facilita el fortalecimiento de la seguridad de la información en la Caja de la Vivienda Popular, con el fin de garantizar la protección de esta y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana, dando cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la Política de Gobierno Digital.

# **RESPONSABLES**

El Responsable por la actualización del Manual es la Oficina de Tecnología de Información y las Comunicaciones – TIC.

# **DEFINICIONES**

A continuación, se relacionan los conceptos y definiciones aplicables al presente plan:

* ***Activos de Información***: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
* ***Confidencialidad***: Propiedad que impide la divulgación de información a personas o sistemas no autorizados.
* ***Dato Abierto***: 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).
* ***Dato Privado***: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
* ***Dato Sensible***: 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.
* ***Disponibilidad***: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
* ***Información***: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.
* ***Información Clasificada***: Es aquella información que estando en poder o custodia de un sujeto, 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 de manera motivada y por escrito, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados estipulados en el artículo 18 de la Ley 1712 de 2014 y su acceso pudiere causar un daño a ciertos derechos, contemplados en la misma ley.
* ***Información 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).
* ***Integridad***: garantía de la exactitud y completitud de la información de la información y los métodos de su procesamiento.
* ***No repudio***: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
* ***Privacidad***: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
* ***Seguridad de la Información***: Protección de los activos de información, contra amenazas que garanticen la continuidad del negocio, minimizando el riesgo y maximizando las oportunidades de la unidad.
* ***Sistema de Información***: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
* ***Tecnología de la Información***: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
* ***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).
* ***Vulnerabilidad***: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000)

# **DOCUMENTOS DE REFERENCIA**

La Caja de la Vivienda Popular ha elaborado el Plan de Seguridad y Privacidad de la Información, en cumplimiento de la siguiente normatividad:

Ley 1474 de 2011, reglamentada por el Decreto Nacional 734 de 2012 y reglamentada parcialmente por el Decreto Nacional 4632 de 2011, por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales.

Ley 1712 de 2014, reglamentada parcialmente por el Decreto Nacional 103 de 2015, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Conpes 3854 de 2016, que es la Política de Seguridad Digital para Colombia y en la cual se establecen nuevos lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.

Decreto 1413 de 2017, Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

Decreto 1008 de 2018, 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 número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

Decreto 612 de 2018, por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

# **ANTECEDENTES**

La Caja de la Vivienda Popular ha avanzado en acciones que apuntan a fortalecer la seguridad y privacidad de la información, de las cuales se tienen los siguientes productos:

# **Política de Seguridad Informática**

Mediante Resolución 4664 del 12 de septiembre de 2016, la Caja de la Vivienda Popular ha adoptado la Política de Seguridad Informática para la Entidad, la cual dispone de lineamientos técnicos y legales para preservar la confidencialidad, integridad y disponibilidad de la información de la Caja de la Vivienda Popular - CVP, incluye la adopción de controles que respondan a las necesidades de la entidad y que contribuyan al alcance de las metas institucionales.

Esta política debe ser aplicada por todos los (as) funcionarios (as), contratistas, proveedores, consultores y todo personal externo que utilice los servicios informáticos que ofrece la Entidad, deben conocer y aceptar el reglamento vigente sobre su uso, su desconocimiento no exonera de responsabilidad al usuario, ante cualquier eventualidad que involucre la seguridad de la información o de la red institucional.

Esta política se actualizará de acuerdo con las disposiciones legales, técnicas o institucionales que defina el Estado colombiano, el Distrito Capital y/o la CVP.

# **Inventario de Activos de Información**

La Caja de la Vivienda Popular ha desarrollado el inventario y clasificación de activos hace parte de la debida diligencia que a nivel estratégico se ha definido en el Modelo de Seguridad y Privacidad de la Información con respecto a la seguridad de los activos de información de los procesos de una entidad, y cuyo objetivo es dar cumplimiento a cuatro puntos principales descritos en el Ítem 8 de la Tabla 2 – de la guía Controles del Anexo A del estándar ISO/IEC 27001:2013. Este inventario permite clasificar los activos a los que se les debe brindar mayor protección, identificando claramente sus características y rol al interior de cada uno de los procesos, utilizando la metodología documentada y aprobada por MinTIC, la cual propone su actualización periódica, la cual debe ser desarrollada por el equipo de seguridad de la información y apoya la gestión para su aprobación por parte de la alta dirección.

# **Política de Tratamiento de Datos**

Desde el año 2015 se cuenta en la entidad con una Política de Tratamiento de Datos, la cual fue elaborada en cumplimiento a lo dispuesto en la Ley estatutaria 1581 de 2012 y a su Decreto Reglamentario 1377 de 2013, Circular Interna de fecha 29 de abril de 2014 Asunto recomendaciones a manera de Tratamiento de la Información y la Resolución interna 855 del 01 de julio de 2014.

Con dicha política se da cumplimiento a lo dispuesto en la Ley Estatutaria 1581 de 2012 articulo 17 en el literal k), dentro del cual se encuentra el de adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley y en especial, para la atención de consultas y reclamos. Así mismo tiene la finalidad de regular los procedimientos para el tratamiento de los datos de carácter personal que realiza la Entidad, a fin de garantizar y proteger el derecho fundamental de habeas data en el marco de lo establecido en la misma Ley.

# **Plan de Tratamiento de Riesgos**

En cumplimiento al Decreto 612 de 2018, el cual establece que las Entidades del Estado, deberán integrar sus planes institucionales y estratégicos, y publicarlos en la página web anualmente, la Caja de la Vivienda Popular elaboró el plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Este plan tiene como objetivo establecer los lineamientos de buenas prácticas de seguridad y privacidad de la información, que permita definir criterios para la identificación, análisis, valoración y gestión de los riesgos potenciales que afecten la confiabilidad, disponibilidad e integridad de la información de la Caja de la Vivienda Popular.

# **DIAGNÓSTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

En este capítulo se presenta el diagnóstico de Seguridad y Privacidad de la Información que permite identificar el estado actual de la Caja de la Vivienda Popular con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información a través del diligenciamiento del instrumento de evaluación.

Brecha Anexo A ISO 27001:2013: En este componente se muestra el resultado del análisis de brecha frente a los controles del Anexo A, del estándar ISO 27001:2013, y la guía de controles (Guía #8) del Modelo de Seguridad de Privacidad de la Información.

En la siguiente gráfica se puede evidenciar la calificación de cada dominio frente a la escala de evaluación definida y también en comparación con la calificación objetivo correspondiente, estipulada en el Manual de Gobierno en Línea:



Avance PHVA: Este componente permite evidenciar el avance en el ciclo del modelo de seguridad definido en el Modelo de Seguridad y Privacidad de la Información, el cual está alineado con los plazos para la implementación de las actividades que se establecieron para el Manual de Gobierno en Línea, y a través del Decreto 1078 de 2015, en el Titulo 9, Capitulo 1, Sección 3.



Como se puede observar, en la medición realizada en el mes de julio de 2018, se obtuvo un promedio total de 67% en la evaluación de los controles, lo cual evidencia la gestión del grupo de seguridad de la información.

De acuerdo con la anterior gráfica los dominios que más incrementaron fueron políticas de seguridad de la información , control de acceso, seguridad física y del entorno y seguridad de las comunicaciones. El dominio que no presentó avance fue criptografía, y finalmente los que requieren mayor trabajo fueron organización de la seguridad de la información, gestión de activos, seguridad de las operaciones, adquisición, desarrollo y mantenimiento de sistemas, y finalmente gestión de incidentes de seguridad de la información.

# **PLAN**

De acuerdo con lo evidenciado en los capítulos anteriores, se evidencia que la Caja de la Vivienda Popular ha tenido avances significativos frente a la implementación del Modelo de Seguridad y Privacidad de la Información, sin embargo, se deben definir ciertas actividades que garanticen el cumplimiento del total de los lineamientos establecidos en dicho modelo.

Es importante tener en cuenta el Modelo de Madurez de Seguridad y Privacidad de la Información, establecido por el Ministerio de las TIC, el cual mide la brecha entre el nivel actual de la entidad y el nivel optimizado.

La figura a continuación muestra los diferentes niveles que hacen parte de este modelo de madurez:



En la siguiente tabla se presentan las características de cada uno de los niveles de madurez con una descripción general:

| **NIVEL** | **DESCRIPCION** |
| --- | --- |
| Inexistente | * Se han implementado controles en su infraestructura de TI, seguridad física, seguridad de recursos humanos entre otros, sin embargo, no están alineados a un Modelo de Seguridad.
* No se reconoce la información como un activo importante para su misión y objetivos estratégicos.
* No se tiene conciencia de la importancia de la seguridad de la información en la entidad.
 |
| Inicial | * Se han identificado las debilidades en la seguridad de la información.
* Los incidentes de seguridad de la información se tratan de forma reactiva.
* Se tiene la necesidad de implementar el MSPI, para definir políticas, procesos y procedimientos que den respuesta proactiva a las amenazas sobre seguridad de la información que se presentan en la Entidad.
 |
| Repetible | * Se identifican en forma general los activos de información.
* Se clasifican los activos de información.
* Los servidores públicos de la entidad tienen conciencia sobre laseguridad de la información.
* Los temas de seguridad y privacidad de la información se tratan en los comités del modelo integrado de gestión.
* La entidad cuenta con un plan de diagnóstico para IPv6.
 |
| Definido | * La Entidad ha realizado un diagnóstico que le permite establecer el estado actual de la seguridad de la información.
* La Entidad ha determinado los objetivos, alcance y límites de laseguridad de la información.
* La Entidad ha establecido formalmente políticas de Seguridad de la información y estas han sido divulgadas.
* La Entidad tiene procedimientos formales de seguridad de laInformación.
* La Entidad tiene roles y responsabilidades asignados en seguridad y privacidad de la información.
* La Entidad ha realizado un inventario de activos de informaciónaplicando una metodología.
* La Entidad trata riesgos de seguridad de la información a través de una metodología.
* Se implementa el plan de tratamiento de riesgos.
* La entidad cuenta con un plan de transición de IPv4 a IPv6
 |
| Administrado | * Se revisa y monitorea periódicamente los activos de información de la Entidad.
* Se utilizan indicadores para establecer el cumplimiento de las políticas de seguridad y privacidad de la información.
* Se evalúa la efectividad de los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.
* La entidad cuenta con ambientes de prueba para el uso del protocolo IPv6.
 |
| Optimizado | * En este nivel se encuentran las entidades en las cuales la seguridad es un valor agregado para la organización.
* Se utilizan indicadores de efectividad para establecer si la entidad encuentra retorno a la inversión bajo la premisa de mejora en el cumplimiento de los objetivos misionales.
* La entidad genera tráfico en IPv6
 |

A continuación, se presenta el esquema de actividades establecido por la Oficina TIC de la Entidad:

La metodología definida, establece cuatro fases, con tres actividades principales, cada una. En cada fase se busca avanzar en los diferentes Niveles de Madurez, con el propósito de llegar al nivel Optimizado, que es el más alto del modelo y en el cual la Entidad se encontraría en una búsqueda constante de la mejora continua.

Para cada macro actividad se deben definir los tiempos, recursos y entregables esperados, sin embargo el primer paso será realizar un diagnóstico de la situación actual de la Caja de la Vivienda Popular frente al Modelo de Seguridad y Privacidad de la Información, que permita identificar los dominios que tienen menor avance, y con base en este resultado priorizar aquellos en los que se trabajará en las primeras instancias.

# **CONTROL DE CAMBIOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | **Fecha Aprobación (dd-mm-aaaa)** | **Cambios** | **Revisó (Nombre y Cargo)** |
| 1 | 27-07-2018 | Creación del documento | Diana Carolina Donoso CasasJefe Oficina TIC  |