# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

OFICINA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

ENERO-2023

CAJA DE LA VIVIENDA POPULAR | BOGOTÁ

## TABLA DE CONTENIDO



## LISTA DE FIGURAS

## 1. OBJETIVO

Establecer los lineamientos de buenas prácticas de seguridad y privacidad de la información, que permita salvaguardar la integridad, confidencialidad y disponibilidad de la información de la Caja de la Vivienda Popular-CVP.

## 2. ALCANCE

El presente Plan de Tratamiento aplica para toda la Caja de la Vivienda Popular, funcionarios, contratistas y terceros, que tengan acceso, usen, produzcan o manejen información de los procesos estratégicos, misionales, de apoyo y de evaluación, de la Entidad.

## 3. RESPONSABLES

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

## 4. DEFINICIONES Y SIGLAS

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.
- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Confidencialidad:** Propiedad que impide la divulgación de información apersonas o sistemas no autorizados.
- **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.

- Disponibilidad: Característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- Encargado del Tratamiento de Datos: Persona natural o jurídica, pública privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de2012, 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. (NTC/ISO:27000).

- 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 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 de2014. (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.
- Plan de continuidad del negocio: Plan orientado a permitir la continuación 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 implantarlos controles necesarios para proteger la misma. (ISO/IEC 27000).
- 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.
- 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).
- Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua (ISO/IEC 27000)
- 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.
- 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.

## 5. DESARROLLO DEL CONTENIDO

### 5.1 Metodología

La Caja de la Vivienda Popular cuenta con la política de administración de riesgos, la cual se encuentra dentro del Proceso Gestión Estratégica, donde establece un esquema adaptado e integrado a los procesos de la entidad que aporte al logro de los objetivos y facilite la mejora continua, mediante el análisis de la incertidumbre como un factor que se puede manejar a través del uso de información y conocimiento

para la toma de decisiones acertadas frente a posibles eventos y sus efectos adversos. Adicionalmente en esta se contempla la política de administración de riesgos de seguridad digital.

Dentro de esta metodología para la valoración de los riesgos se tienen en cuenta los siguientes criterios:

### 5.1.1 Criterios de Frecuencia

**Excepcional:** Puede ocurrir sólo en circunstancias excepcionales y bajo condiciones muy puntuales.

**Improbable:** Puede ocurrir en algún momento, pero su probabilidad de ocurrencia es casi nula.

**Posible:** Puede ocurrir en algún momento bajo circunstancias normales.

**Probable:** La probabilidad de que ocurra bajo condiciones normales alta.

**Casi Seguro:** Se espera que ocurra en la mayoría de las circunstancias.

### 5.1.2 Criterios de Impacto

**Insignificante:** El riesgo no conlleva a consecuencias significativas, la afectación es intrascendente en temas referentes al cumplimiento de objetivos.

**Menor:** El riesgo conlleva a consecuencias mínimas, la afectación en temas referentes al cumplimiento de objetivos presenta niveles bajos.

**Moderado:** La materialización de este riesgo conllevaría a consecuencias y afectaciones mesuradas, de no darse un manejo adecuado, puede verse comprometido el cumplimiento de objetivos de los procesos.

**Mayor:** La materialización de este riesgo conlleva a afectaciones significativas, que comprometen el cumplimiento de los objetivos de los diferentes procesos de la entidad.

**Catastrófico:** El Riesgo afecta negativamente la vida y/o bienes inmuebles y representa una enorme pérdida financiera. Si el riesgo es de un proceso de apoyo,

estratégico o de evaluación, su materialización impide el cumplimiento del objetivo del proceso.

### 5.1.3 Mapa de Calor de Riesgos

Una vez determinado el nivel de frecuencia y consecuencia del riesgo se debe estimar el nivel de riesgo a través de la ubicación en la siguiente matriz de Nivel de Riesgo. Así se determinará el nivel de riesgo al que está expuesto el proceso por la materialización de los factores identificados previamente.

| | | IMPACTO | | | | |
|---|---|---|---|---|---|---|
| | | **Insignificante** | **Menor** | **Moderado** | **Mayor** | **Catastrófico** |
| FRECUENCIA | **Excepcional** | Bajo | Bajo | Medio | Alto | Alto |
| | **Improbable** | Bajo | Bajo | Medio | Alto | Extremo |
| | **Posible** | Bajo | Medio | Alto | Extremo | Extremo |
| | **Probable** | Medio | Alto | Alto | Extremo | Extremo |
| | **Casi Seguro** | Alto | Alto | Extremo | Extremo | Extremo |

*Ilustración 1- Mapa de Calor de Riesgos*

De acuerdo con los resultados obtenidos en la valoración de riesgos podemos obtener los siguientes resultados:

**Extremo:** Zona de nivel de riesgo en la que es aconsejable eliminar la causa raíz que genera el riesgo en la medida que sea posible. Se deben implementar acciones de prevención para tratar de eliminar la frecuencia del riesgo y/o disminuir el Impacto mediante acciones de mitigación.

**Alto:** Zona de nivel de riesgo en que las consecuencias deben ser controladas con acciones. En este nivel de riesgo se deben tomar acciones y controles que lleven en lo posible al riesgo a zonas moderada y baja.

**Medio:** Zona de nivel de riesgo que es posible asumirlo, es decir, el riesgo se encuentra en un nivel que puede ser aceptado tras la implantación de algunas medidas de control diferentes a las que se poseen.

**Bajo:** Estos riesgos son de menor frecuencia de ocurrencia y más bajo impacto, sin embargo, representan una posible alteración al normal desarrollo de las labores de la entidad, por lo tanto, pueden asumirse.

### 5.1.4 Tratamiento del Riesgo

Para dar desarrollo de este importante componente de la administración de riesgos, es prioritario resaltar que en la definición de las metas se contemple la fácil medición y por ende la realización de estas en un periodo de tiempo determinado. De esta manera se debe fijar una meta obligatoria para cada riesgo identificado y clasificado en la zona de riesgo como Altos o Extremos, teniendo en cuenta los siguientes aspectos:

- El límite de tiempo para la ejecución de la acción será de un año a partir de la aprobación del Mapa de Riesgos.
- Tener en cuenta aspectos de viabilidad jurídica, técnica, institucional y financiera.

***Criterios para el tratamiento del riesgo***

**Mitigar:** Se desarrolla mediante la generación de cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

**Prevenir:** La prevención del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles. Ejemplo: Planes de contingencia.

**Dispersar:** Se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

**Transferir:** Hace referencia a buscar respaldo y compartir con otro, parte del riesgo como por ejemplo tomar pólizas de seguros, esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.

**Asumir:** Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el responsable del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

## 6. PLAN DE ACCIÓN O CRONOGRAMA DE TRABAJO

### 6.1 Plan de Tratamiento de Riesgos

Los riesgos de seguridad y privacidad de la información se basan en la afectación de tres (3) criterios en un activo o un grupo de activos dentro del proceso:

Integridad, confidencialidad o disponibilidad.

La entidad, se compromete a gestionar los riesgos, identificando y administrando los eventos potenciales que pueden afectar la plataforma estratégica, los objetivos institucionales y los procesos de la entidad.

Para la adecuada gestión integral del riesgo en la CVP, se presenta los siguientes lineamientos:

1. Se adoptará las metodologías para gestionar los riesgos de la entidad a través del análisis del contexto, entendido como el entorno externo e interno, y valoración de los mismos, es decir, su identificación, análisis y evaluación, y su posterior tratamiento, todo esto manteniendo comunicación y Consulta constante y permanente monitoreo y revisión, para evitar así su materialización.

2. Los riesgos que se gestionan en la Caja de la Vivienda Popular son los siguientes:
   a. Riesgos Estratégicos: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impacta en toda la entidad.
   b. Riesgos gerenciales: Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
   c. Riesgos operativos: Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
   d. Riesgos financieros: Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas dependencias involucradas con el proceso financiero.
   e. Riesgos tecnológicos: Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de la entidad.
   f. Riesgos de cumplimiento: Posibilidad de ocurrencia de eventos que afectan la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones.
   g. Contractuales.
   h. Riesgo de imagen o reputacional: posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.
   i. Riesgos de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
   j. Riesgos de seguridad digital: Combinación de amenazas vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

3. Se deben identificar los activos de información por cada proceso.
4. Se deben identificar los dueños de los activos.
5. Se deben clasificar los activos acordes a los procesos de la entidad (Misional, Apoyo a la Gestión, Estratégicos y Procesos de Evaluación).
6. Se debe determinar la criticidad de los activos.
7. Se deben identificar las vulnerabilidades de los activos.

8. Se deben identificar las amenazas de los activos.
9. Se deben identificar los riesgos de los activos.
10. Se debe realizar una descripción de los riesgos.
11. Se debe revisar la probabilidad y el impacto de ocurrencia de los riesgos.
12. Se debe calcular el riesgo inherente.
13. Se deben aplicar los controles a los riesgos identificados.
14. Los controles deben tener una frecuencia de aplicación.
15. La tolerancia es el nivel del riesgo que la entidad puede o está dispuesta a soportar, que corresponden a los riesgos que se encuentren en zona residual Baja y los que se encuentran en otra zona se trataran de acuerdo a los lineamientos establecidos en el procedimiento de Gestión de Riesgos de la entidad.
16. La entidad revisará y actualizará la política de Gestión de Riesgos de acuerdo con los cambios del entorno, las nuevas metodologías y los resultados de los indicadores de gestión asociados a la materialización de riesgos definidos.
17. Los riesgos identificados en la entidad deberán ser monitoreados permanentemente, para asegurar que los controles sean eficaces y eficientes, y obtener información para mejorar la evaluación y gestión de los mismos.
18. Los niveles de responsabilidad sobre periodicidad de seguimiento y evaluación de los riesgos se llevarán a cabo de acuerdo con el procedimiento de Gestión de Riesgos de la entidad.

Las opciones del tratamiento a los riesgos que se evalúan en la entidad son:

a. Evitar el riesgo: Se logra cuando al interior de los procesos se generan cambios sustanciales por rediseño, eliminación o cancelación de una actividad o conjunto de actividades que causan el riesgo, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.
b. Reducir el riesgo: Implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.

c. Compartir el riesgo: Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones o dependencias, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar y esto equivale a la tercerización.
d. Asumir el riesgo: Después de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el líder del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo. No aplica para los riesgos de corrupción, estos siempre deben conducir a un plan de acción o de tratamiento para mitigarlo.

## 7. SEGUIMIENTO Y MEDICIÓN DEL PLAN

| Ítem | Actividad | Fecha de inicio | Fecha final | Responsable | Producto o resultado |
|---|---|---|---|---|---|
| Riesgos de seguridad y privacidad de la información | | | | | |
| 1 | Actualización del plan de tratamiento de riesgos de seguridad y privacidad de la información | Enero | Febrero | Profesional de seguridad de la información | Plan de tratamiento de riesgos de seguridad y privacidad de la información |
| 2 | Revisión de la matriz de activos de información junto con las dependencias de la CVP | Marzo | Abril | Profesional de seguridad de la información | Matriz de activos de información actualizada |
| 3 | Identificación de riesgos de seguridad digital | Marzo | Mayo | Profesional de seguridad de la información | Matriz de riesgos de seguridad digital |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Tratamiento de riesgos de seguridad digital | Junio | Agosto | Profesional de seguridad de la información | Matriz de riesgos de seguridad digital |
| 5 | Oficialización de la matriz de riesgos de Seguridad digital | Agosto | Septiembre | Profesional de seguridad de la información | Matriz de riesgos de seguridad digital |

## 8. DOCUMENTOS RELACIONADOS

n/a

### 8.1 Normatividad

Ver normograma Gestión TIC: calidad\SGC\14. PROCESO GESTIÓN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES\1. CARACTERIZACION\1.2 NORMATIVIDAD.

208-TIC-Nr-01 NORMOGRAMA GESTION TIC.xlsx

### 8.2 Formatos Asociados

- n/a

### 8.3 Documentos Externos

| Nombre del Documento | Fecha de publicación o versión del documento | Entidad que lo emite | Ubicación |
|---|---|---|---|
| N/A | N/A | N/A | N/A |

## 9. REFERENCIAS

La Caja de la Vivienda Popular ha elaborado el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, tomando como referencia Norma NTC-ISO-IEC 27001, que es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013.

Metodología de la función pública Guía para la administración del riesgo y el diseño de controles en entidades públicas, riesgos de gestión, corrupción y seguridad digital.

Adicionalmente, tiene en cuenta lo establecido en el 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.

En particular la Guía No. 7, MINTIC, Guía de gestión de riesgos, Seguridad y privacidad de la información.

## 10. CONTROL DE CAMBIOS

| Versión | Fecha Aprobación (dd-mm-aaaa) | Cambios | Revisó Nombre y Cargo Líder del Proceso |
|---|---|---|---|
| 1 | 27-07-2018 | Creación del documento | Diana Carolina Donoso Casas Jefe Oficina TIC |
| 2 | 30-01-2020 | Actualización del documento | Andrés Orlando Briceño Díaz Jefe Oficina TIC |

| Versión | Fecha Aprobación (dd-mm-aaaa) | Cambios | Revisó Nombre y Cargo Líder del Proceso |
|---|---|---|---|
| 3 | 28-01-2021 | Actualización del documento | Liliana Morales Jefe Oficina TIC |
| 4 | 19-01-2023 | Actualización de la plantilla del documento de acuerdo con lo establecido en el SGC de la CVP, bajo codificación *208-GE-Ft-107 PLAN V1.docx* | Luz Yamile Reyes Bonilla Jefe Oficina TIC |

## 11. APROBACIÓN

| ELABORADO | REVISADO | APROBADO |
|---|---|---|
| **Nombre:** Fabián David Rojas Castiblanco<br>**Cargo:** Contratista<br>**Fecha:** 19-01-2023 | **Nombre:** Camilo Augusto Ramos Beltrán<br>**Cargo:** Profesional Universitario<br>**Fecha:** 19-01-2023 | **Nombre:** Luz Yamile Reyes Bonilla<br>**Cargo:** Jefe Oficina TIC<br>**Fecha:** 19-01-2023 |

## 12. PUBLICACIÓN

| | |
|---|---|
| **RESPONSABLE DEL SISTEMA DE GESTIÓN** | **Nombre:** Catalina Nagy Patiño |
| **CARGO:** | **Cargo:** Jefe Oficina Asesora de Planeación |
| **FECHA DE APROBACIÓN DE PUBLICACIÓN EN EL SISTEMA DE GESTIÓN** | **Fecha:** 31-01-2023 |