PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2023

OFICINA ASESORA DE PLANEACIÓN

VERSIÓN 1.0

Fondo de Vivienda de Interés Social y Reforma Urbana Distrital
CORVIVIENDA
Cartagena de Indias 2023

Contenido

Si este documento se encuentra impreso no se garantiza su vigencia
La versión vigente reposa en el Sistema Integrado de Planeación y Gestión www.corvivienda.gov.co

1. GENERALIDADES DEL PLAN INSTITUCIONAL

1.1. INTRODUCCIÓN

En consecuencia a lo establecido en el decreto 1008 del 14 de junio 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 1078 de 2015, decreto único reglamentario del sector de Tecnologías de la Información y las Comunicaciones, el Fondo de Vivienda de Interés Social y Reforma Urbana – Corvivienda, procede a definir normativas y buenas prácticas para el tratamiento de la información dentro de la entidad.

Mediante este plan se indicarán las medidas que se implementará que pretende garantizar la seguridad y privacidad de la información que maneja la institución.

1.2. ALCANCE

El Plan de seguridad y privacidad de la información está orientado a gestionar las buenas prácticas en uso de las plataformas tecnológicas y servicios de tecnologías de información y comunicaciones, que apoyan el desarrollo de las diferentes actividades relacionadas con el modelo de operación por procesos adoptados en la entidad.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar un marco normativo de buenas prácticas en el buen uso de la información dando cumplimiento a lo planteado en el decreto 1008 del 14 de junio de 2018 (Gobierno Digital)

1.3.2. OBJETIVOS ESPECÍFICOS

1. Diagnosticar la situación actual del Sistema de Gestión de Seguridad y Privacidad de la Información al interior de la entidad, así como detectar posibles riesgos.
2. Establecer alcance, roles, responsabilidades, políticas, procedimientos y demás elementos que permitan construir un marco normativo al interior de la institución.
3. Determinar el estado de los activos de información, identificación, valoración y tratamiento de riesgos dentro de la Entidad.

4. Diseñar e implementar controles para mitigar, minimizar o transferir los riesgos de Seguridad y Protección de la información en cada una de las áreas.
5. Evaluar el desempeño de las herramientas, políticas y controles implementados en el Sistema de Gestión de Seguridad y Privacidad de la Información.

2. CONTEXTO ESTRATÉGICO

El contexto estratégico del Plan de Privacidad y Seguridad de la información se refiere a cómo la organización maneja y protegen la información confidencial y privada de sus clientes, empleados y otros intereses. Esto incluye la implementación de medidas de seguridad físicas y digitales, la creación de políticas y procedimientos para el manejo de la información, y la educación y concientización de los empleados sobre los riesgos de privacidad y seguridad. Además, las organizaciones deben cumplir con las leyes y regulaciones aplicables en materia de privacidad y seguridad de la información.

Durante la vigencia 2022 se elaboraron la política de Seguridad Digital y los Procedimientos de Backup de Hosting, Desarrollo de Sistemas de Información, Publicación de Contenidos y Soporte Técnico, con los cuales se buscar robustecer el Proceso de Gestión TIC.

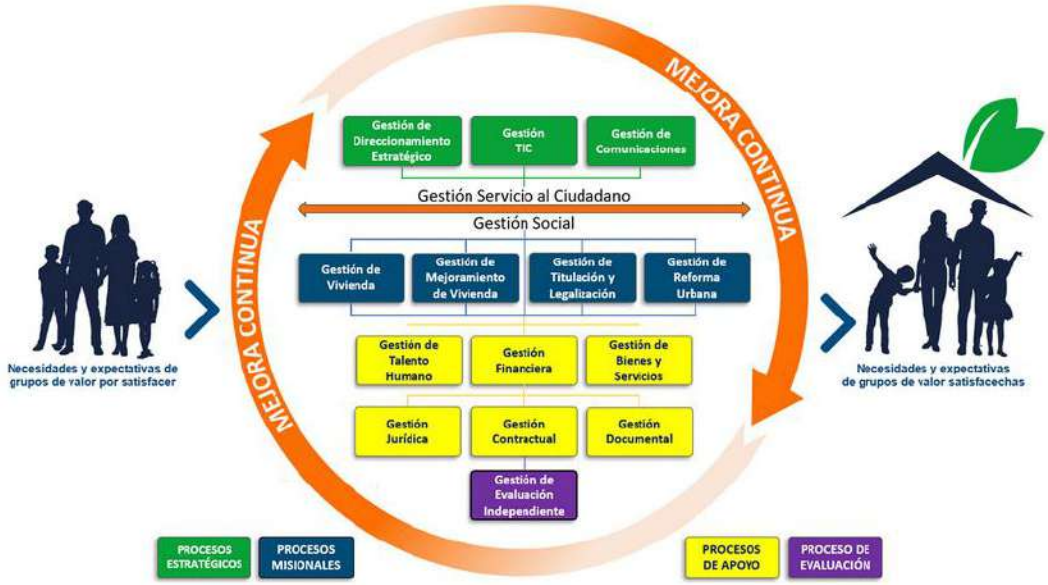
En esta misma línea se pretende seguir robusteciendo este Proceso, mediante la elaboración de otros Procedimientos, formatos y guías que aborden la totalidad de los servicios TI, prestados por la entidad. Por esto se hace necesario la ejecución de la herramienta de autoevaluación MSPI para establecer las brechas y establecer planes acción correspondientes.

3. CONTEXTO ORGANIZACIONAL

Para el desarrollo de las organizaciones, en términos de calidad de acuerdo a los lineamientos del Departamento Administrativo de Función Pública DAFP, según la Guía para la Gestión por Procesos en el Marco del Modelo Integrado de Planeación y Gestión MIPG versión 1, es la adopción de una gestión por procesos, permitiendo la mejora sustancial de las actividades al interior de las Entidades Públicas, orientando sus esfuerzos al servicio de los grupos de interés y de valor, permitiendo dar resultados acordes a las necesidades de estos.

El Fondo de Vivienda de Interés Social y Reforma Urbana Distrital de Cartagena CORVIVIENDA, a través del Acta No. 8 - 2022 del Comité Institucional de Gestión y Desempeño, actualizó su Mapa de Procesos, permitiendo con esto lograr aunar esfuerzos en procura de generar valor a través de la gestión por procesos, impactando al ciudadano como eje fundamental de la Gestión Pública.

MAPA DE PROCESOS DE CORVIVIENDA



Fuente: Acta No. 8 - 2022 del Comité Institucional de Gestión y Desempeño CORVIVIENDA

4. MARCO CONCEPTUAL

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ALCANCE: Ámbito de la organización que queda sometido al SGSI.

ATAQUE: Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN: Procesos y procedimientos para garantizar una operativa continuada de la seguridad de la información.

CONTROL: Medida por la que se modifica el riesgo. Los controles incluyen procesos, políticas, dispositivos, prácticas, entre otras acciones que modifican el

riesgo. Es posible que los controles no siempre ejerzan el efecto de modificación previsto o supuesto. Los términos salvaguardan o contramedida son utilizados frecuentemente como sinónimos de control.

CRITERIO DEL RIESGO: Los criterios del riesgo se basan en los objetivos de la organización y el contexto externo y el contexto interno. Los criterios de riesgo pueden derivarse de estándares, leyes, políticas y otros requisitos.

DISPONIBILIDAD: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

FIABILIDAD: Propiedad del comportamiento y de unos resultados consistentes previstos.

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.

INTEGRIDAD: Propiedad de la información relativa a su exactitud y completitud.

ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ORGANIZACIÓN: Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para lograr sus objetivos.

PROFESIONAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI): Persona que establece, implementa, mantiene y mejora continuamente uno o más procesos del sistema de gestión de seguridad de la información.

RECURSOS DE TRATAMIENTO DE INFORMACIÓN: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

RENDIMIENTO: El rendimiento puede relacionarse con hallazgos cuantitativos o cualitativos. El rendimiento puede relacionarse con la gestión de actividades, procesos, productos (incluidos servicios), sistemas u organizaciones.

REQUISITO: Necesidad o expectativa que es establecida, generalmente de forma implícita u obligatoria.

RIESGO: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad.

SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información.

SISTEMA DE INFORMACIÓN: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan información.

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.

VULNERABILIDAD: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. MARCO NORMATIVO

- **En materia de derechos de autor:**
  Decisión 351 de la C.A.N, Ley 23 de 1982, Decreto 1360 de 1989, Ley 44 de 1993, Decreto 460 de 1995, Decreto 162 de 1996, Ley 545 de 1999, Ley 565 de 2000, Ley 603 de 2000 y Ley 719 de 2001.
- **En materia de propiedad industrial e intelectual:**
  Decisión 486 de la C.A.N, Decreto 2591 de 2000, Ley 463 de 1998, Ley 170 de 1994, Ley 178 de 1994, Decisión 345 de la C.A.N, Decisión 391 de la C.A.N y Decisión 523 de la C.A.N.
- **En materia de Seguridad Informática:**

ISO 27001:2013, Política de Seguridad Digital – MIPG, Modelo de Seguridad MSPI - MINTIC

6. DESCRIPCIÓN DEL PLAN

Un plan de privacidad y seguridad de la información es un conjunto de medidas y procedimientos diseñados para proteger la privacidad y seguridad de la información confidencial de una organización. El plan debe incluir medidas para prevenir, detectar y responder a incidentes de privacidad y seguridad de la información, así como cumplir con las leyes y regulaciones aplicables en materia de privacidad y seguridad de la información.

Para la gestión de este plan se tienen en cuenta actividades que impacten en los siguientes aspectos del MSPI:

- Identificación y evaluación de riesgos: Un análisis de los riesgos potenciales para la privacidad y seguridad de la información, incluyendo los riesgos internos y externos.
- Políticas y procedimientos: Un conjunto de políticas y procedimientos para garantizar que la información se maneja de manera segura y cumpliendo con las regulaciones aplicables
- Medidas de seguridad física y digital: medidas de seguridad para proteger la información física y digital, tales como protección de la infraestructura, firewalls, encriptación, autenticación de usuarios, etc
- Educación y concientización: Capacitaciones a los empleados sobre la privacidad y seguridad de la información, incluyendo temas como el manejo seguro de contraseñas, el uso seguro de dispositivos móviles, y cómo identificar y responder a incidentes de seguridad.
- Monitoreo y auditorías: Monitoreo y auditorías regulares para detectar y responder a incidentes de privacidad y seguridad de la información.
- Plan de respuesta a incidentes: Un plan detallado para responder a incidentes de privacidad y seguridad de la información, incluyendo un plan de comunicación con los interesados afectados.

7. METODOLOGÍA DE SEGUIMIENTO

Para el correcto seguimiento del Plan de Seguridad y Privacidad de la Información al interior de la entidad, se construirán unos indicadores de gestión que permitirán establecer el avance de cumplimiento a partir de actividades planeadas para cada uno de los componentes que conforman el presente plan institucional.

Es de precisar que las actividades a desarrollar son apuestas al mejoramiento de los procesos dentro de la entidad en términos de transparencia, acceso a la información y lucha contra la corrupción.

7.1. PLAN DE ACCIÓN.

Se estableció la herramienta Plan de Acción como criterio documental para la gestión del Plan de Seguridad y Privacidad de la Información, ya que enmarca la hoja de ruta a seguir en la ejecución del plan.

Esta herramienta administrativa establece la ruta a implementar para gestionar los productos o metas necesarias para el cumplimiento de los objetivos en el marco de la misionalidad de la entidad.

El Plan de Acción está conformado por tres (3) componentes, un **Planteamiento Estratégico** alineado con el objetivo del Plan Institucional, una **Articulación con la Metodología Integral de Planeación y Gestión MIPG** con los procesos institucionales y una **Política de Administración de Riesgos** donde se identifican los riesgos asociados y controles.

FORMATO PLAN DE ACCIÓN PLANES INSTITUCIONALES

PLANTEAMIENTO ESTRATÉGICO PLAN INSTITUCIONAL													ARTICULACIÓN MIPG				POLÍTICA DE ADMINISTRACIÓN DE RIESGOS	
No	INDICADOR	UNIDAD DE MEDIDA INDICADOR	DESCRIPCIÓN DEL INDICADOR	PESO	ACTIVIDADES	META ACTIVIDAD	UNIDAD DE MEDIDA META	PROGRAMACIÓN META			DEPENDENCIA RESPONSABLE	OBSERVACION O RELACIÓN DE EVIDENCIA	DIMENSIONES DE MIPG	POLÍTICAS DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL	PROCESO ASOCIADO	OBJETIVO INSTITUCIONAL	RIESGOS ASOCIADOS AL PROCESO	CONTROLES ESTABLECIDOS PARA LOS RIESGOS
								DESDE	HASTA	FRECUENCIA								
1	XXXXX	XXXXX	xxxxx	0%	1	0	xxxxx					xxxxx	xxxxx	xxxxx	xxxxx	xxxxx	xxxxx	xxxxx
						0	VISITAS					xxxxx					xxxxx	xxxxx
						0	INSPECCIONES					xxxxx					xxxxx	xxxxx
						0	EXPEDIENTES					xxxxx					xxxxx	xxxxx
2	XXXXX	XXXXX	xxxxx	0%	xxxxx	0	xxxxx					xxxxx	xxxxx	xxxxx	xxxxx	xxxxx	xxxxx	xxxxx
						0	VISITAS					xxxxx					xxxxx	xxxxx
						0	INSPECCIONES					xxxxx					xxxxx	xxxxx
						0	EXPEDIENTES					xxxxx					xxxxx	xxxxx

Fuente: Oficina Asesora de Planeación

7.2. BATERÍA DE INDICADORES

En el marco de la **Guía para la Construcción y Análisis de Indicadores 2018** del Departamento Nacional de Planeación DNP, que orienta en la construcción y análisis de los indicadores a partir de la **CADENA DE VALOR** (relación secuencial y lógica entre insumos, actividades, productos y resultados en la que se añade valor a lo largo del proceso de transformación total)[1] de la entidad.

Con relación a la Cadena de Valor de la entidad, los indicadores a utilizar son los **INDICADORES DE GESTIÓN**, cuyo objetivo principal es cuantificar y medir dos elementos.

[1] (DNP, 2017, pág. 5)

- La cantidad de insumos utilizados.
- Las acciones de gestión realizadas.

Teniendo en cuenta los tipos de indicadores de gestión, se establecen indicadores de eficacia, eficiencia y efectividad, con relación al desarrollo de las actividades dentro del Plan de Acción del Plan Institucional.

EFICACIA: Grado en el que se realizan las actividades planificadas y se alcanzan los resultados planificados.[2]

EFICIENCIA: Medida en que el uso de los insumos (recursos financieros, humanos, técnicos y materiales) se ha hecho en forma económica u óptima para generar productos. Relación entre el resultado alcanzado y los recursos utilizados.[3]

EFECTIVIDAD: Medida del impacto de la gestión tanto en el logro de los resultados planificados, como en el manejo de los recursos utilizados y disponibles.[4]

Los Indicadores de gestión del Plan de Seguridad y Privacidad de la Información son los siguientes:

1. **Nombre del Indicador:** Grado de implementación de normativas y controles de acuerdo con la política de Seguridad Digital

   Tipo de indicador: Eficacia

   Objetivo del Indicador: Determinar el porcentaje de cumplimiento de implementación de normativas y controles de acuerdo a la política de Seguridad Digital.

   Formula de Calculo:

$$Eficacia = \frac{No\ de\ Actividades\ realizadas}{No\ de\ Actividades\ Programadas} x100$$

2. **Nombre del Indicador:** Grado de satisfacción y apropiación del proceso Gestión TIC

   Tipo de indicador: Eficiencia

   Objetivo del Indicador: Determinar el porcentaje de satisfacción y apropiación del proceso Gestión TIC en materia de Seguridad Digital.

   Formula de Calculo:

[2] Glosario- Servicio al Ciudadano – Función Pública.
[3] Glosario- Servicio al Ciudadano – Función Pública.
[4] Glosario- Servicio al Ciudadano – Función Pública.

$$Eficiencia = \frac{No\ de\ solicitudes\ a\ satisfechas}{No\ de\ solicitudes\ atendidas} x100$$

7.3. CRONOGRAMA DE SEGUIMIENTO Y EVALUACIÓN

Para el seguimiento y evaluación del Plan de Acción, se debe realizar una evaluación trimestral y las fechas programadas para la entrega de informes, con el fin de dar cumplimiento a los compromisos normativos, son:

SEGUIMIENTO	Entrega Informe de Gestión Plan Institucional	Reporte Avance Trimestral Plan Institucional (2da línea de defensa)
I Trimestre	31 de Marzo	7 de Abril
II Trimestre	7 de Julio	7 Julio
III Trimestre	29 de Septiembre	6 de Octubre
IV Trimestre	8 de Diciembre	13 de Diciembre

7.4. MEDICIÓN TRIMESTRAL DE METAS

Con el fin de medir la **EFICACIA** del Plan Institucional de Seguridad y Privacidad de la Información, se definieron rangos de seguimiento para medir la gestión del Plan de Acción, y establecer alertas y planes de choque que permitan el cumplimiento de lo planeado.

MATRIZ DE RANGOS PORCENTUALES DE GESTIÓN

Nivel de EFICACIA	Estado del Indicado	Marzo	Junio	Septiembre	Diciembre
ALTO		25% o más	50% o más	75% o más	95% o más
MEDIO		15% a 24,9%	40% a 49,9%	65% a 74,9%	85% a 94,9%
BAJO		Menos de 15%	Menos de 40%	Menos de 65%	Menos de 85%

8. CONTROL DE CAMBIOS

Versión	Fecha y número de Acta y/o Acto Administrativo aprobación	Elaborado por:	Revisado por:	Aprobado por:	Descripción del Cambio
1	Acta de Comité Institucional de Gestión y Desempeño No. 01-2023	Fabio Pérez Márquez	María Elena Gutiérrez / Laura Meza Espinosa	Javier Gaona Solano Oficina Asesora de Planeación	Creación del documento.