

	FORMATO PLANES INSTITUCIONALES	Código: ES-DEPL-11
		Fecha: 20/01/2023
		Página 1 de 13
		Versión: 1

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

2026



OFICINA ASESORA DE PLANEACIÓN

**Fondo de Vivienda de Interés Social y Reforma Urbana Distrital
CORVIVIENDA
Cartagena de Indias 2026**

Contenido

1.	GENERALIDADES DEL PLAN INSTITUCIONAL.....	3
1.1.	INTRODUCCIÓN	3
1.2.	ALCANCE.....	3
1.3.	OBJETIVOS.....	4
1.3.1.	OBJETIVO GENERAL	4
1.3.2.	OBJETIVOS ESPECÍFICOS	4
2.	CONTEXTO ESTRATÉGICO	4
3.	CONTEXTO ORGANIZACIONAL	5
4.	MARCO CONCEPTUAL	6
5.	MARCO NORMATIVO	9
6.	DESCRIPCIÓN DEL PLAN	9
7.	METODOLOGÍA DE SEGUIMIENTO.....	10
7.1.	PLAN DE ACCIÓN.....	10
7.2.	BATERÍA DE INDICADORES.....	11
7.3.	CRONOGRAMA DE SEGUIMIENTO Y EVALUACIÓN	12
7.4.	MEDICIÓN TRIMESTRAL DE METAS	12
8.	CONTROL DE CAMBIOS	13

	FORMATO PLANES INSTITUCIONALES	Código: ES-DEPL-11
		Fecha: 20/01/2023
		Página 3 de 13
		Versión: 1

1. GENERALIDADES DEL PLAN INSTITUCIONAL

1.1. INTRODUCCIÓN

Teniendo en cuenta lo establecido en el Modelo Integrado de Gestión y Desempeño, en lo relacionado con la gestión del riesgo institucional, se hace necesario que en la entidad se realice una debida gestión del riesgo siguiendo los lineamientos establecidos por el Departamento Administrativo de la Función Pública, con un enfoque preventivo que permita la protección de la información.

Tomamos como base el Manual de la política de Gobierno Digital expedido por el Ministerio de Tecnologías de información y de las Comunicaciones que establece que la política tiene como propósito promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones, para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital, disminuyendo los riesgos en la generación de la información.

1.2. ALCANCE

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Corvivienda tiene como alcance establecer las estrategias, controles y acciones necesarias para gestionar de manera efectiva los riesgos que puedan afectar la seguridad digital, la integridad de los sistemas de información, la infraestructura tecnológica y la protección de los datos institucionales. Este plan se orienta a garantizar que los riesgos identificados sean tratados con medidas adecuadas que mitiguen su impacto sobre el modelo de operación por procesos adoptado en la entidad.

Su alcance contempla:

- Gestión integral de los riesgos de seguridad y privacidad
- Definición y selección de estrategias de tratamiento
- Implementación de controles de seguridad
- Alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Política de Gobierno Digital
- Cobertura de todos los procesos institucionales
- Seguimiento, evaluación y mejora continua

	FORMATO PLANES INSTITUCIONALES	Código: ES-DEPL-11
		Fecha: 20/01/2023
		Página 4 de 13
		Versión: 1

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar el Sistema de Gestión de Riesgos de Seguridad y Privacidad de la Información, con el fin de minimizar, mitigar o transferir los riesgos a los cuales se expone la información, además de velar por el cumplimiento de los requerimientos legales, regulatorios y contractuales de la Entidad.

1.3.2. OBJETIVOS ESPECÍFICOS

1. Establecer los principios básicos y el marco general de actuación para el control y la gestión de los riesgos de seguridad y privacidad de la información a los que se enfrenta la entidad.
2. Realizar seguimiento permanente a los riesgos identificados de seguridad y privacidad de la información en la Entidad mediante la aplicación de herramientas (mapa de Riesgos de Gestión TIC) que permitan la valoración e implementación de acciones para mitigar, minimizar o transferirlos.

2. CONTEXTO ESTRATÉGICO

El contexto estratégico del Plan de Tratamiento de Riesgos de la Privacidad y Seguridad de la información se refiere a cómo la organización identifica y da tratamiento a los riesgos potenciales en el manejo y protección de la información confidencial y privada de sus funcionarios, contratistas y otros grupos de interés. 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, la entidad debe cumplir con las leyes y regulaciones aplicables en materia de privacidad y seguridad de la información.

Durante la vigencia 2025 a través del acto administrativo No. 8 de 20 de enero de 2025 y Acta No. 11 - 2024 del Comité Institucional de Gestión y Desempeño CORVIVIENDA se actualizaron los Procedimientos de Backup de Hosting, Desarrollo de Sistemas de Información, Publicación de Contenidos web y Soporte Técnico TI, Solicitud de acceso a sistemas de Información y Gestión de incidentes de seguridad de la información, con los cuales se buscar robustecer el Proceso de Gestión TIC.

Por esto se hace necesario la ejecución de la herramienta de autoevaluación del MSPI para medir el nivel de madurez de la seguridad de la información en la entidad, identificar 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. 11 - 2024 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. 11 - 2024 del Comité Institucional de Gestión y Desempeño CORVIVIENDA

	FORMATO PLANES INSTITUCIONALES	Código: ES-DEPL-11
		Fecha: 20/01/2023
		Página 6 de 13
		Versión: 1

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.

APETITO DE RIESGO: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

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.

CAPACIDAD DE RIESGO: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

CAUSA: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

CAUSA INMEDIATA: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

CAUSA RAÍZ: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

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

	FORMATO PLANES INSTITUCIONALES	Código: ES-DEPL-11
		Fecha: 20/01/2023
		Página 7 de 13
		Versión: 1

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.

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - Versión 1
Fecha: 31-1-2024

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

	FORMATO PLANES INSTITUCIONALES	Código: ES-DEPL-11
		Fecha: 20/01/2023
		Página 8 de 13
		Versión: 1

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.

RIESGO DE CORRUPCIÓN: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

RIESGO DE SEGURIDAD DE LA INFORMACIÓN: 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).

RIESGO INHERENTE: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

RIESGO RESIDUAL: El resultado de aplicar la efectividad de los controles al riesgo inherente.

TOLERANCIA DEL RIESGO: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

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.

	FORMATO PLANES INSTITUCIONALES	Código: ES-DEPL-11 Fecha: 20/01/2023 Página 9 de 13 Versión: 1
---	---	---

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

5. MARCO NORMATIVO

- Constitución Política de Colombia
- Acuerdo 37 del 19 de Junio de 1991 “Por medio del cual se crea el Fondo de Vivienda de Interés Social y Reforma Urbana Distrital CORVIVIENDA”.
- Decreto 612 del 4 de Abril 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”.
- Ley 1581 de 2012: “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Ley 1712 de 2014: “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”.
- Decreto Ministerial 1078 de 2015: “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- Decreto Presidencial 1083 de 2015: “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.
- ISO/IEC 27001:2013: Tecnología de la información-Técnicas de seguridad-Sistemas de Gestión de la Seguridad de la Información (SGSI)- Requisitos.

6. DESCRIPCIÓN DEL PLAN

El tratamiento de riesgos de la información es el proceso de identificar, evaluar y mitigar los riesgos potenciales para la privacidad y seguridad de la información de una organización. El tratamiento de riesgos es esencial para proteger la información confidencial y cumplir con las 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 Modelo de Seguridad y Privacidad de la Información MSPI:

- Identificación de riesgos: Se buscan y se identifican los riesgos potenciales para la privacidad y seguridad de la información de la organización. Esto

	FORMATO PLANES INSTITUCIONALES	Código: ES-DEPL-11
		Fecha: 20/01/2023
		Página 10 de 13
		Versión: 1

incluye riesgos internos y externos, tales como el robo de dispositivos móviles, el espionaje industrial, y el hacking.

- Evaluación de riesgos: Se determina la probabilidad y el impacto de cada riesgo identificado. Esto ayuda a priorizar los riesgos y a tomar decisiones sobre cómo tratarlos.
- Mitigación de riesgos: Se implementan medidas para reducir la probabilidad o el impacto de los riesgos identificados. Esto puede incluir medidas de seguridad física y digital, políticas y procedimientos, educación y concientización de los empleados, y la contratación de un equipo de seguridad de la información.
- Monitoreo y revisión: Se realizan auditorías y se monitorea continuamente el plan de seguridad para detectar y responder a incidentes de privacidad y seguridad de la información. Esto también ayuda a identificar posibles cambios en el entorno de seguridad que puedan requerir una actualización del plan.

Es importante destacar que el tratamiento de riesgos debe ser un proceso continuo y adaptativo, ya que los riesgos cambian con el tiempo y las regulaciones aplicables también pueden cambiar.

7. METODOLOGÍA DE SEGUIMIENTO

Para el correcto seguimiento del Plan de Tratamiento de Riesgos de la Seguridad y Privacidad de la Información al interior de la entidad, se construirán 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.

	FORMATO PLANES INSTITUCIONALES	Código: ES-DEPL-11
		Fecha: 20/01/2023
		Página 11 de 13
		Versión: 1

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.

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.

- 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 planificados²

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

EFFECTIVIDAD: 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 Tratamiento de Riesgos de la Seguridad y Privacidad de la Información son los siguientes:

¹ (DNP, 2017, pág. 5)

² Glosario- Servicio al Ciudadano – Función Pública.

³ Glosario- Servicio al Ciudadano – Función Pública.

⁴ Glosario- Servicio al Ciudadano – Función Pública.

- 1. Nombre del Indicador:** Grado de implementación de normativas y controles de acuerdo con la política de seguridad digital en materia de tratamiento de riesgos de la información

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 en materia de tratamiento de riesgos de la información

Formula de Calculo:

$$\text{Eficacia} = \frac{\text{No de Actividades realizadas}}{\text{No de Actividades Programadas}} \times 100$$

- 2. Nombre del Indicador:** Grado de satisfacción y apropiación del proceso gestión tic en materia de tratamiento de riesgos de la información.

Tipo de indicador: Eficiencia

Objetivo del Indicador: Determinar el porcentaje de satisfacción y apropiación del proceso gestión TIC en materia de tratamiento de riesgos de la información.

Formula de Calculo:

$$\text{Eficiencia} = \frac{\text{No de solicitudes a satisfechas}}{\text{No de solicitudes atendidas}} \times 100$$

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	15 de diciembre

7.4. MEDICIÓN TRIMESTRAL DE METAS

Con el fin de medir la **EFICACIA** del Plan de Tratamiento de Riesgos de la Seguridad y Privacidad de la Información, se definieron rangos de seguimiento

	FORMATO PLANES INSTITUCIONALES	Código: ES-DEPL-11
		Fecha: 20/01/2023
		Página 13 de 13
		Versión: 1

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. ENTIDADES DE APOYO

- Ministerio de Tecnología de la Información y las Comunicaciones (MINTIC)
- Departamento de la Función Pública
- Proveedores de servicios de Tecnología
- Alcaldía de Cartagena de Indias

9. CONTROL DE CAMBIOS

Versión	Fecha y número de Acta y/o Acto Administrativo aprobación	Elaborado por:	Revisado por:	Aprobado por:	Descripción del Cambio