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

2026

DIRECCIÓN GENERAL

VERSIÓN 1.0

Instituto Distrital de Acción Comunal de Cartagena y el Caribe
IDACCC
Cartagena de Indias
2026

Contenido

1. GENERALIDADES DEL PLAN INSTITUCIONAL

1.1. INTRODUCCIÓN

La información constituye un activo estratégico para el Instituto Distrital de Acción Comunal de Cartagena y el Caribe – IDACCC, por cuanto soporta la operación institucional, la prestación de servicios, la gestión administrativa y el relacionamiento con la ciudadanía y las organizaciones comunales. En este sentido, la entidad requiere fortalecer de manera sistemática la identificación, valoración y tratamiento de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información durante todo su ciclo de vida.

En concordancia con el Modelo Integrado de Planeación y Gestión (MIPG), la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI), el IDACCC adopta el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para establecer la hoja de ruta institucional que permita prevenir incidentes, reducir vulnerabilidades, implementar controles y asegurar el cumplimiento de las disposiciones legales y regulatorias aplicables, especialmente las relacionadas con la protección de datos personales.

1.2. ALCANCE

El presente Plan aplica a los procesos misionales, estratégicos, de apoyo y de evaluación del IDACCC, y cubre los activos de información (físicos y digitales), plataformas, sistemas de información, servicios tecnológicos, infraestructura, comunicaciones, bases de datos, documentos y demás recursos que sean utilizados para el cumplimiento de las funciones institucionales.

El alcance comprende la identificación y valoración de riesgos de seguridad y privacidad de la información, la definición e implementación de controles, el seguimiento al tratamiento de riesgos, la gestión de incidentes asociados y la actualización periódica del plan conforme a cambios en procesos, tecnología, normatividad o contexto institucional.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Implementar y mantener el tratamiento de los riesgos de seguridad y privacidad de la información del IDACCC, mediante la identificación, valoración, priorización y aplicación de controles, con el fin de minimizar, mitigar, transferir o aceptar los riesgos dentro de niveles tolerables, garantizando el cumplimiento normativo y la continuidad de los servicios institucionales.

1.3.2.OBJETIVOS ESPECÍFICOS

- Identificar y actualizar el inventario de activos de información y sus responsables, como base para la gestión del riesgo.
- Valorar los riesgos de seguridad y privacidad de la información, considerando amenazas, vulnerabilidades, probabilidad e impacto.
- Definir e implementar controles básicos y acciones de tratamiento priorizadas según el nivel de riesgo.
- Establecer mecanismos de seguimiento (indicadores, reportes y evidencias) para verificar la efectividad de los controles y el avance del plan.
- Promover la apropiación institucional mediante sensibilización y responsabilidades claras para la gestión del riesgo.

2. CONTEXTO ESTRATÉGICO

El contexto estratégico del IDACCC en materia de seguridad y privacidad de la información se orienta a fortalecer la confianza digital, la continuidad operativa y el cumplimiento del marco de Gobierno Digital y MIPG, en un entorno donde la entidad gestiona información institucional, administrativa y datos personales de usuarios, líderes comunales y actores del ecosistema de participación ciudadana.

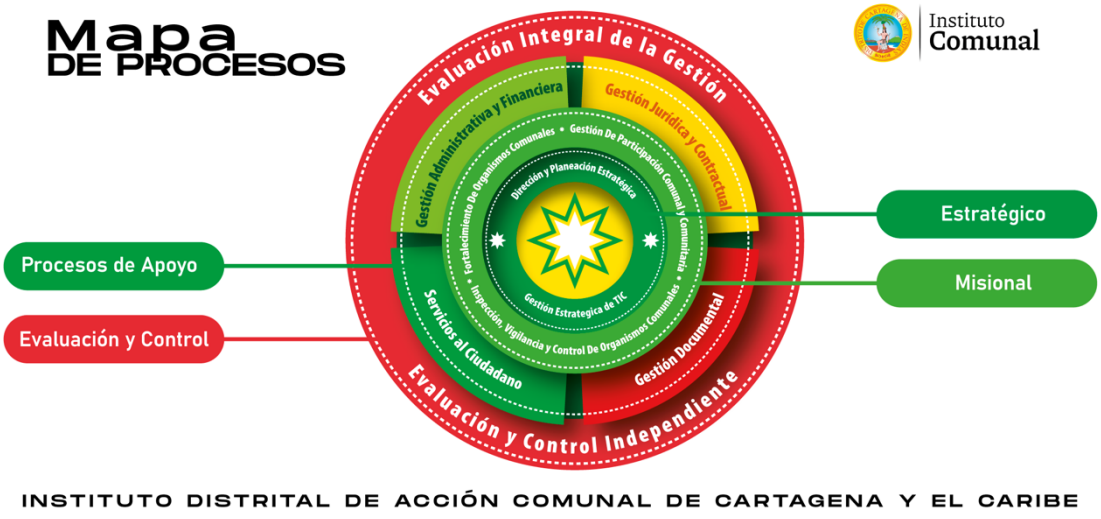
La implementación del MSPI requiere la identificación permanente de brechas, la priorización de riesgos y la ejecución progresiva de controles organizacionales, procedimentales y técnicos. Por ello, el presente Plan se integra a la planeación institucional y se articula con el mapa de riesgos, el control interno y los mecanismos de seguimiento definidos por la entidad.

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 6, 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 Instituto Distrital de Acción Comunal de Cartagena y el Caribe IDACCC, a través del Acta No. 01 - 2025 del Comité Institucional de Gestión y Desempeño, aprobó 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 DEL INSTITUTO COMUNAL IDACCC



Fuente: Acta No. 01-2025 del Comité Institucional de Gestión y Desempeño IDACCC

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 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.

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.

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

5. MARCO NORMATIVO

- Constitución Política de Colombia.
- Ley 1581 de 2012 – Protección de datos personales.
- Ley 1712 de 2014 – Transparencia y acceso a la información pública.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del sector TIC (y sus modificaciones).
- Decreto 1083 de 2015 – Decreto Único Reglamentario del sector Función Pública (MIPG / políticas de gestión).
- Decreto 612 de 2018 – Integración de planes institucionales (incluye componentes relacionados con seguridad de la información).
- Resolución MinTIC 500 de 2021 – Lineamientos/estándares de seguridad digital y adopción del MSPI como habilitador de Gobierno Digital.
- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital.
- CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital.
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (DAFP).
- Manual de Gobierno Digital y lineamientos del MSPI – MinTIC.
- Actos administrativos internos del IDACCC (Comité Institucional de Gestión y Desempeño, roles de TI, políticas de seguridad, etc.)

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 MSPI:

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

La priorización de acciones en el IDACCC se realizará con base en la criticidad de los activos de información, el nivel de riesgo residual y la capacidad institucional para implementar controles. El Plan se ejecutará mediante un Plan de Acción anual con responsables definidos, evidencias verificables e indicadores de seguimiento, y será revisado como mínimo de manera trimestral en el marco de los ejercicios de control interno y comités institucionales.

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.

El Plan de Acción del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Instituto Distrital de Acción Comunal de Cartagena y el Caribe – IDACCC establece las actividades, responsables, productos, beneficiarios y tiempos requeridos para la implementación progresiva de las medidas orientadas a mitigar, controlar, aceptar o transferir los riesgos identificados. Este plan se constituye en la hoja de ruta operativa para la ejecución del Modelo de Seguridad y Privacidad de la Información (MSPI), articulándose con el Modelo Integrado de Planeación y Gestión (MIPG), el sistema de control interno y los instrumentos de planeación institucional, y permite realizar el seguimiento sistemático al avance, efectividad y mejora continua de los controles definidos durante la vigencia correspondiente.

COMPONENTE / ACTIVIDAD PRINCIPAL	ACTIVIDADES RELACIONADAS	META	UNIDAD DE MEDIDA (EVIDENCIA)	BENEFICIARIOS	PERSONA RESPONSABLE	OBSERVACIONES	FECHA
Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)	Convocar al Comité Institucional de Gestión y Desempeño	Dar inicio formal al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del IDACCC, garantizando el respaldo institucional.	Acta de convocatoria y acta de sesión del Comité	IDACCC	Líder TI	Actividad inicial obligatoria para la ejecución del plan.	Febrero
Implementación del MSPI	Sensibilizar a servidores y contratistas	Fortalecer la cultura institucional en seguridad de la información y protección de datos personales.	Registro de asistencia, material de sensibilización, actas	Servidores y contratistas del IDACCC	Líder TI	Puede realizarse de forma presencial o virtual.	Febrero – Marzo 2026
Implementación del MSPI	Identificar activos de información	Identificar y documentar los activos de información institucionales como base para la gestión del riesgo.	Inventario de activos de información	IDACCC	Líder TI	Debe incluir activos físicos y digitales.	Febrero – Marzo 2026

COMPONENTE / ACTIVIDAD PRINCIPAL	ACTIVIDADES RELACIONADAS	META	UNIDAD DE MEDIDA (EVIDENCIA)	BENEFICIARIOS	PERSONA RESPONSABLE	OBSERVACIONES	FECHA
Implementación del MSPI	Clasificar activos de información	Clasificar los activos según su criticidad, confidencialidad, integridad y disponibilidad.	Matriz de clasificación de activos	IDACCC	Líder TI	Insumo clave para la valoración del riesgo.	Marzo
Implementación del MSPI	Identificar amenazas y vulnerabilidades	Identificar amenazas y vulnerabilidades que puedan afectar los activos de información.	Documento de identificación de amenazas y vulnerabilidades	IDACCC	Líder TI	Se articula con el mapa de riesgos institucional.	Marzo – Abril 2026
Implementación del MSPI	Valorar riesgos de seguridad	Analizar y valorar los riesgos de seguridad y privacidad de la información.	Matriz de riesgos valorada	IDACCC	Líder TI	Metodología alineada con MSPI y DAFP.	Abril – Mayo 2026
Implementación del MSPI	Priorizar riesgos	Priorizar los riesgos identificados de acuerdo con su nivel de impacto y probabilidad.	Matriz de priorización de riesgos	IDACCC	Líder TI	Define el orden de intervención.	Mayo – Junio 2026
Implementación del MSPI	Definir controles de seguridad	Definir controles administrativos, técnicos y procedimentales para el tratamiento de riesgos.	Documento de controles definidos	IDACCC	Líder TI	Controles proporcionales al nivel de riesgo.	Junio – Julio 2026

COMPONENTE / ACTIVIDAD PRINCIPAL	ACTIVIDADES RELACIONADAS	META	UNIDAD DE MEDIDA (EVIDENCIA)	BENEFICIARIOS	PERSONA RESPONSABLE	OBSERVACIONES	FECHA
Implementación del MSPI	Implementar controles básicos	Implementar los controles de seguridad y protección de datos priorizados.	Evidencias de implementación de controles	IDACCC y ciudadanía usuaria	Líder TI	Puede ejecutarse de manera progresiva.	Julio – Octubre 2026
Implementación del MSPI	Articular controles con la mesa de ayuda	Integrar la gestión de incidentes de seguridad al sistema de mesa de ayuda institucional.	Registros del sistema de mesa de ayuda	IDACCC	Líder TI	Mesa de ayuda en proceso de implementación.	Agosto – Octubre 2026
Implementación del MSPI	Realizar seguimiento y monitoreo	Verificar la efectividad de los controles y el avance del plan de tratamiento de riesgos.	Informes de seguimiento y reportes periódicos	Dirección IDACCC	Líder TI	Insumo para control interno y mejora continua.	Octubre – Diciembre 2026
Implementación del MSPI	Reportar resultados al Comité	Presentar los avances y resultados del plan al Comité Institucional de Gestión y Desempeño.	Acta e informe de presentación	Dirección IDACCC	Líder TI	Cierre del ciclo anual de gestión del riesgo.	Diciembre
Implementación del MSPI	Ajustar y actualizar el plan	Ajustar el Plan de Tratamiento de Riesgos conforme a resultados y cambios institucionales.	Plan actualizado	IDACCC	Líder TI	Actividad recurrente anual.	Diciembre

7.2. BATERÍA DE INDICADORES

No.	Indicador	Descripción	Fórmula de Cálculo	Frecuencia	Responsable
1	Porcentaje de activos de información identificados	Mide el nivel de identificación de los activos de información del IDACCC.	(Número de activos identificados / Número total de activos estimados) × 100	Trimestral	Líder TI
2	Porcentaje de riesgos de seguridad valorados	Evalúa el avance en la valoración de los riesgos de seguridad y privacidad de la información.	(Riesgos valorados / Riesgos identificados) × 100	Trimestral	Líder TI
3	Porcentaje de riesgos con controles definidos	Mide el grado de definición de controles para los riesgos priorizados.	(Riesgos con controles definidos / Riesgos priorizados) × 100	Trimestral	Líder TI
4	Porcentaje de controles implementados	Evalúa el nivel de implementación de los controles de seguridad definidos en el plan.	(Controles implementados / Controles definidos) × 100	Trimestral	Líder TI
5	Incidentes de seguridad atendidos	Mide la cantidad de incidentes de seguridad de la información gestionados a través de la mesa de ayuda institucional.	Número total de incidentes atendidos en el periodo	Trimestral	Líder TI
6	Nivel de cumplimiento del Plan de Acción	Evalúa el cumplimiento general del Plan de Tratamiento de Riesgos frente a las actividades programadas.	(Actividades ejecutadas / Actividades programadas) × 100	Trimestral	Líder TI

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	30.03.2026	06.04.2026
II Trimestre	30.06.2026	06.07.2026
III Trimestre	30.09.2026	05.10.2026
IV Trimestre	23.12.2026	29.12.2026

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 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-IDACCC-2026	Julio Barcos	Javier Gaona	Geverson Ortiz	Creación del documento.