PLAN 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 gestión administrativa y el relacionamiento con la ciudadanía y las organizaciones comunales. En este sentido, el IDACCC establece el presente Plan de Seguridad y Privacidad de la Información como instrumento de planeación que orienta las acciones, lineamientos y proyectos para fortalecer la confidencialidad, integridad y disponibilidad de la información, así como la adecuada protección de datos personales.

El Plan se formula en concordancia con la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los lineamientos y estándares de la estrategia de seguridad digital adoptados por el Ministerio TIC, constituyéndose en la hoja de ruta para la implementación progresiva de controles, la gestión de incidentes, la concientización institucional y la mejora continua.

1.2. ALCANCE

El presente Plan aplica a todos los servidores públicos, contratistas y terceros que, para el cumplimiento de sus funciones u obligaciones, recolecten, utilicen, consulten, administren, transmitan o almacenen información del IDACCC. Igualmente, aplica a los activos de información físicos y digitales, sistemas de información, bases de datos, infraestructura tecnológica, plataformas institucionales y servicios TIC que soportan los procesos estratégicos, misionales, de apoyo y de evaluación de la entidad.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

Fortalecer la confidencialidad, integridad y disponibilidad de los activos de información del IDACCC, mitigando los riesgos de seguridad digital hasta niveles aceptables, mediante la implementación progresiva de la estrategia de seguridad digital y del Modelo de Seguridad y Privacidad de la Información (MSPI), promoviendo además el cumplimiento normativo y la protección de datos personales.

1.3.2. OBJETIVOS ESPECÍFICOS

- Definir y ejecutar las acciones estratégicas de seguridad y privacidad de la información del IDACCC para la vigencia 2026.
- Establecer y consolidar los elementos requeridos para la implementación del MSPI (políticas, roles, procedimientos, inventarios, gestión de incidentes y riesgos).
- Priorizar proyectos y actividades para implementar controles y cerrar brechas identificadas.
- Realizar seguimiento y evaluación al desempeño de los controles y lineamientos implementados.
- Fortalecer la cultura institucional de seguridad y privacidad de la información en servidores, contratistas y actores que interactúan con la entidad.

2. CONTEXTO ESTRATÉGICO

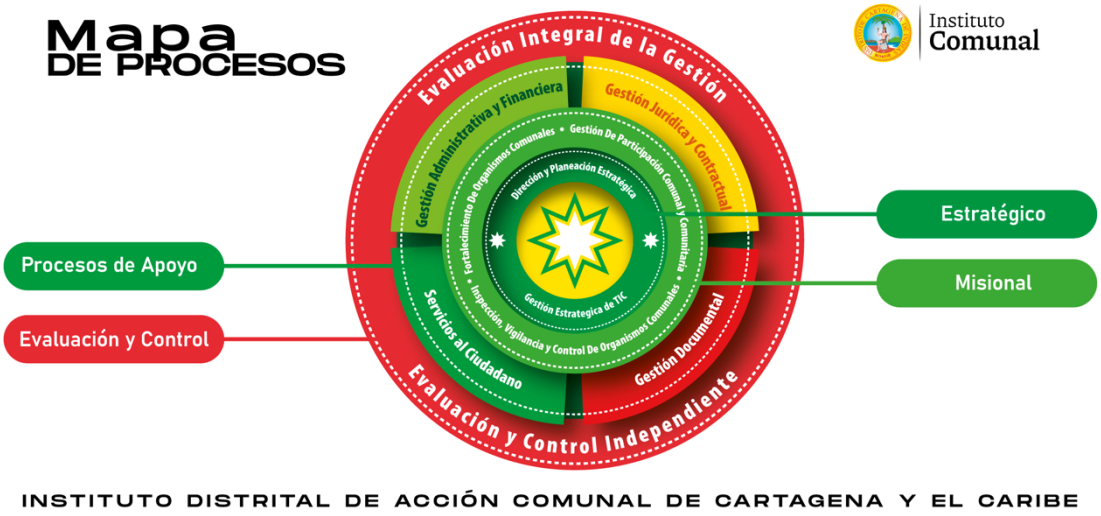
En el marco de la puesta en marcha y fortalecimiento institucional del IDACCC, se hace necesario establecer una línea base de seguridad y privacidad de la información que permita identificar brechas, riesgos y capacidades actuales, con el fin de priorizar acciones de mejora. En esta línea, la entidad desarrollará la autoevaluación del MSPI y consolidará instrumentos institucionales (políticas, procedimientos, inventarios, gestión de incidentes y tratamiento de riesgos) que permitan avanzar en el nivel de madurez de seguridad digital y garantizar confianza en el uso de los servicios y plataformas institucionales.

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.

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

- 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 612 de 2018 – Integración de planes institucionales (incluye el Plan de Seguridad y Privacidad de la Información como instrumento de planeación).

- Resolución MinTIC 500 de 2021 – Lineamientos y estándares de la estrategia 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 documentos del MSPI – MinTIC.
- Actos administrativos internos del IDACCC (Comité Institucional de Gestión y Desempeño, políticas y procedimientos que se adopten).

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.

En el marco del MSPI, el IDACCC estructura su enfoque de implementación a partir de una Estrategia de Seguridad Digital organizada en cinco ejes: (i) liderazgo de seguridad de la información, (ii) gestión de riesgos, (iii) implementación de controles, (iv) gestión de incidentes y (v) concientización, los cuales orientan el portafolio de actividades y proyectos definidos para la vigencia 2026.

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.

El Plan de Acción del Plan de Seguridad y Privacidad de la Información del Instituto Distrital de Acción Comunal de Cartagena y el Caribe – IDACCC define las actividades, responsables, metas, evidencias y tiempos necesarios para la implementación progresiva de los lineamientos, controles y buenas prácticas orientadas a fortalecer la seguridad digital y la protección de la información institucional. Este plan constituye la hoja de ruta operativa para la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), permitiendo priorizar acciones, realizar seguimiento al avance de la estrategia de seguridad digital y asegurar su articulación con el Modelo Integrado de Planeación y Gestión (MIPG), el sistema de control interno y los procesos institucionales.

COMPONENTE / ACTIVIDAD PRINCIPAL	ACTIVIDADES RELACIONADAS	META	UNIDAD DE MEDIDA (EVIDENCIA)	BENEFICIARIOS	PERSONA RESPONSABLE	OBSERVACIONES	FECHA
Plan de Seguridad y Privacidad de la Información	Fortalecer el liderazgo institucional en seguridad de la información	Consolidar el liderazgo institucional y el compromiso de la alta dirección en la implementación del Plan de Seguridad y Privacidad de la Información del IDACCC.	Actas del Comité Institucional de Gestión y Desempeño, lineamientos internos	IDACCC	Líder TI	Actividad transversal a todo el plan.	Enero – Diciembre 2026
	Definir y adoptar políticas de seguridad y privacidad	Definir, documentar y adoptar las políticas de seguridad y privacidad de la información conforme al MSPI y la normatividad vigente.	Políticas de seguridad y privacidad aprobadas	IDACCC	Líder TI	Insumo base para la gestión de la seguridad de la información.	Enero – Marzo 2026
	Identificar y gestionar riesgos de seguridad	Identificar, valorar y actualizar los riesgos de seguridad y privacidad de la información institucional.	Matriz de riesgos de seguridad actualizada	IDACCC	Líder TI	Articulado con el mapa de riesgos institucional.	Marzo – Junio 2026

COMPONENTE / ACTIVIDAD PRINCIPAL	ACTIVIDADES RELACIONADAS	META	UNIDAD DE MEDIDA (EVIDENCIA)	BENEFICIARIOS	PERSONA RESPONSABLE	OBSERVACIONES	FECHA
	Definir el plan de tratamiento de riesgos	Establecer acciones y controles para mitigar, aceptar o transferir los riesgos priorizados.	Plan de Tratamiento de Riesgos aprobado	IDACCC	Líder TI	Documento complementario al presente plan.	Abril – Junio 2026
	Implementar controles de seguridad	Implementar controles administrativos, técnicos y procedimentales para proteger los activos de información.	Evidencias de controles implementados	IDACCC y ciudadanía usuaria	Líder TI	Implementación progresiva según nivel de riesgo.	Julio – Octubre 2026
	Gestionar incidentes de seguridad	Implementar y operar mecanismos para la gestión y atención de incidentes de seguridad de la información.	Registros de incidentes en la mesa de ayuda	IDACCC	Líder TI	Mesa de ayuda institucional en implementación.	Agosto – Diciembre 2026
	Sensibilizar y capacitar al personal	Fortalecer la cultura institucional en seguridad y privacidad de la información.	Registros de capacitaciones y asistencia	Servidores y contratistas	Líder TI	Jornadas presenciales y/o virtuales.	Enero – Diciembre 2026

COMPONENTE / ACTIVIDAD PRINCIPAL	ACTIVIDADES RELACIONADAS	META	UNIDAD DE MEDIDA (EVIDENCIA)	BENEFICIARIOS	PERSONA RESPONSABLE	OBSERVACIONES	FECHA
	Realizar seguimiento y evaluación	Realizar seguimiento periódico al cumplimiento del plan y a la efectividad de los controles implementados.	Informes de seguimiento y actas	Dirección IDACCC	Líder TI	Insumo para control interno y mejora continua.	Octubre – Diciembre 2026
	Reportar resultados y actualizar el plan	Presentar resultados al Comité Institucional de Gestión y Desempeño y actualizar el plan para la siguiente vigencia.	Informe final y plan actualizado	IDACCC	Líder TI	Cierre de la vigencia 2026.	Diciembre

7.2. BATERÍA DE INDICADORES

Con el fin de realizar el seguimiento y evaluación al cumplimiento del Plan de Seguridad y Privacidad de la Información del Instituto Distrital de Acción Comunal de Cartagena y el Caribe – IDACCC, se establece la presente batería de indicadores, orientada a medir el avance en la implementación de políticas, la gestión de riesgos, la aplicación de controles de seguridad, la atención de incidentes y el fortalecimiento de la cultura institucional en seguridad y privacidad de la información. Estos indicadores constituyen un insumo clave para la toma de decisiones, el control interno, la mejora continua y los reportes asociados al Modelo Integrado de Planeación y Gestión (MIPG).

No.	Indicador	Descripción	Fórmula de Cálculo	Frecuencia	Responsable
1	Nivel de implementación del Plan de Seguridad y Privacidad	Mide el avance general en la ejecución de las actividades definidas en el Plan.	(Actividades ejecutadas / Actividades programadas) × 100	Trimestral	Líder TI
2	Porcentaje de políticas de seguridad adoptadas	Evalúa el grado de adopción de las políticas de seguridad y privacidad de la información.	(Políticas adoptadas / Políticas definidas) × 100	Trimestral	Líder TI
3	Porcentaje de riesgos de seguridad gestionados	Mide el avance en la gestión de los riesgos de seguridad y privacidad de la información.	(Riesgos gestionados / Riesgos identificados) × 100	Trimestral	Líder TI
4	Porcentaje de controles de seguridad implementados	Evalúa el nivel de implementación de los controles administrativos, técnicos y procedimentales.	(Controles implementados / Controles definidos) × 100	Trimestral	Líder TI
5	Incidentes de seguridad gestionados	Mide la cantidad de incidentes de seguridad de la información atendidos mediante la mesa de ayuda institucional.	Número total de incidentes gestionados en el periodo	Trimestral	Líder TI

No.	Indicador	Descripción	Fórmula de Cálculo	Frecuencia	Responsable
6	Porcentaje de servidores y contratistas sensibilizados	Evalúa el nivel de cobertura de las acciones de sensibilización en seguridad y privacidad de la información.	(Personas sensibilizadas / Total de personas vinculadas) × 100	Semestral	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 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-IDACCC-2026	Julio Barcos	Javier Gaona	Geverson Ortiz	Creación del documento.