Corpocaldas
NIT: 890803005-2

Corpocaldas

OFICINA DE CONTROL INTERNO DE GESTIÓN

INFORME DE SEGUIMIENTO POLITICA DE GOBIERNO DIGITAL

JUNIO DE 2025

TABLA DE CONTENIDO

Corpocaldas
NIT: 890803005-2

INFORME DE SEGUIMIENTO POLÍTICA DE GOBIERNO DIGITAL CORPOCALDAS

1. INTRODUCCION

Este informe busca hacer seguimiento al estado de avance de la implementación de la "Política de Gobierno Digital" de Corpocaldas, tomando como referente los lineamientos establecidos por MinTIC y por el manual operativo de MIPG, con el fin de dar cumplimiento al Plan Anual de Auditorías y Seguimientos de la Oficina de Control Interno de la vigencia 2025, el cual fue aprobado en el Comité Institucional de Coordinación de Control Interno (CICCI) del 28 de enero del 2025.

Adicionalmente, con este seguimiento se da cumplimiento a uno de los roles de la Oficina de Control Interno establecidos en el Decreto 1083 de 2015 en su artículo 2.2.21.5.3. De las Oficinas de Control Interno, el cual establece:
…

"*En relación con el rol de Evaluación y Seguimiento le corresponde a la Oficina de Control Interno evaluar y determinar la idoneidad de los controles que se han establecido a lo largo de la entidad, los cuales permiten garantizar de manera razonable que se alcanzarán los objetivos y metas trazadas*".

De igual forma, es importante resaltar lo indicado en el Manual Operativo MIPG (DAFP)

(…)

"Evaluaciones Independientes

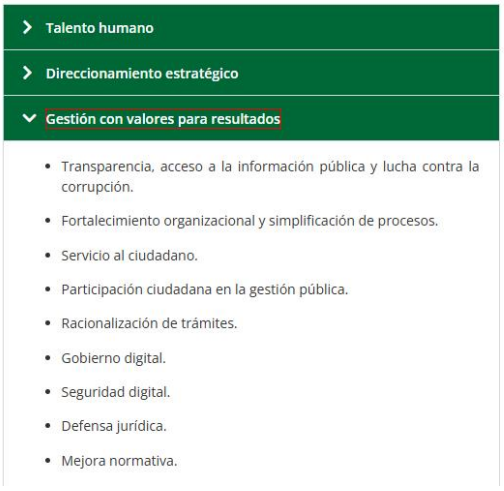
Las evaluaciones independientes se llevan a cabo de forma periódica, por parte de la oficina de control interno o quien haga sus veces a través de la auditoría interna de gestión. Estas evaluaciones permiten determinar si se han definido, puesto en marcha y aplicado los controles establecidos por la entidad de manera efectiva. Las evaluaciones, independientes a los componentes varían en alcance y frecuencia, dependiendo de la importancia del riesgo, de la respuesta al riesgo y de los resultados de las evaluaciones continuas o autoevaluación".

En el mundo, las Tecnologías de la Información y las Comunicaciones, son consideradas críticas porque son vistas como un motor clave para el desarrollo económico y social, la innovación y la competitividad de los países. En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) como líder de la Política de Gobierno Digital, las impulsa para consolidar un Estado y ciudadanos más competitivos, proactivos e innovadores.

Por lo anterior y en vista a lo que representan las tecnologías de la información y las comunicaciones -TIC, para todas las entidades, como áreas que apalancan el desarrollo de los planes, programas y proyectos, la gestión interna de los procesos y la información, la prestación de trámites y servicios a los ciudadanos y en general, la implementación de todas las políticas de gestión y desempeño, como aspecto fundamental para determinar desde el direccionamiento estratégico y la planeación, el desarrollo de todo el componente tecnológico de la entidad, a partir de los lineamientos y estándares que establece la Política de Gobierno Digital, es que se lleva a cabo el presente seguimiento.

2. OBJETIVO

Realizar el seguimiento al estado de avance de la implementación de la Política de Gobierno Digital, como parte de la dimensión Gestión con Valores para Resultados que hace parte del Modelo Integrado de Planeación y Gestión – MIPG (Decreto 1499 de 2017)



Fuente: Función Pública

3. ALCANCE

El presente informe se realiza a partir de las actividades desarrolladas para la implementación de la Política de Gobierno Digital desde el 1 de enero de 2024 y hasta el mes de mayo de 2025.

4. CRITERIOS NORMATIVOS

- Decreto 767 de mayo 16 de 2022: "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"
- Decreto 1078 de 2015. "Por medio del cual se expide el decreto único reglamentario del sector de Tecnologías de la Información y las comunicaciones".
- 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 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", en su artículo: 2.2.9.1.2.2. Manual de Gobierno Digital. Para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de esta Política de Gobierno Digital, el cual será elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con el Departamento Nacional de Planeación".
- Decreto 088 de enero 2022. "Por el cual se adiciona el Titulo 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentar los artículos 3, 5 y 6 de la Ley 2052 de 2020, estableciendo los conceptos, lineamientos, plazos y condiciones para la digitalización y automatización de trámites y su realización en línea"
- Manual Operativo del MIPG versión 5 (marzo de 2023- DAFP)
- Manual de Gobierno Digital (MinTIC)

5. METODOLOGIA

Para el desarrollo del presente seguimiento, se solicitó a la Oficina de Tecnologías de la Información y las Comunicaciones (TIC) de la Entidad, mediante el memorando No. 2025-II-00017896, la información necesaria para evidenciar el estado de avance en la implementación de la política objeto de análisis. La respuesta correspondiente fue recibida el 3 de junio de 2025.

Complementariamente, se realizó una revisión de la información disponible en la página web institucional, en el Sistema de Gestión Integrado (SGI), así como de los lineamientos normativos aplicables que la Entidad debe cumplir en el marco de dicha política.

6. RESULTADOS

Lo primero que debemos saber es que la “Política de Gobierno Digital”, es el instrumento gubernamental que propende por la transformación digital pública, buscando fortalecer la relación Estado-Ciudadano, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública; a través del uso y aprovechamiento de las TIC.

Los elementos que componen la estructura de la Política de Gobierno Digital son Gobernanza e Innovación Pública Digital, que son habilitados por cuatro elementos transversales: Arquitectura, Cultura y apropiación, Seguridad y privacidad de la Información, y Servicios Ciudadanos Digitales. Estos elementos se desarrollan a través de lineamientos y estándares, que son los requerimientos mínimos que todos los sujetos obligados deben cumplir para alcanzar la implementación de la política como se muestra a continuación:

El Decreto 767 de mayo 16 de 2022 en su artículo 2.2.9.1.2.2, establece la **obligatoriedad** de aplicar el Manual para la Implementación de la Política de Gobierno Digital, el cual define los lineamientos, estándares, y guías a ejecutar por parte de los sujetos obligados de esta política. Se procedió a revisar su aplicación en Corpocaldas, de acuerdo con lo señalado, evidenciando los siguientes resultados:

6.1 VERIFICACIÓN DE LA PARTICIPACIÓN DE LOS EJECUTORES DE LA POLÍTICA DE GOBIERNO DIGITAL EN CORPOCALDAS:

A continuación, se presentan las instancias y responsables de la implementación de la política de acuerdo con lo estipulado en el Manual de Gobierno Digital y a la información remitida por el líder de la oficina TIC de la Corporación:

6.1.1 Líder de la Política de Gobierno Digital.

Es el Ministerio de Tecnologías de la Información y las Comunicaciones, quién a través de la Dirección de Gobierno Digital, se encarga de emitir las normas, manuales, guías y la metodología de seguimiento y evaluación para la implementación de la política de Gobierno Digital, en las entidades públicas del orden nacional y territorial.

En la información aportada por el líder de la OTIC, se observa que Corpocaldas, a través del MinTIC ha recibido asesoría y acompañamiento vía correo electrónico y virtual en la vigencia 2025 para la revisión del tema de datos abiertos.

6.1.2 Responsable Institucional de la Política.

El Director de la Entidad coordina, hace seguimiento y verifica la implementación de la Política de Gobierno Digital. Esta función fue delegada en el Subdirector de Planificación, pudiéndose evidenciar en la resolución 2020-0538 del 24 de marzo por medio de la cual se modifica y reglamenta el Comité Institucional de Coordinación de Control Interno de la Corporación Autónoma Regional de Caldas, Artículo segundo, Conformación del Comité Institucional de Coordinación de Control Interno ítem 2 el cual indica: *"Subdirector Planificación Ambiental del Territorio, como representante de la Alta Dirección para la implementación del Modelo de Control Interno MECI"*

6.1.3 Comité Institucional de Gestión y Desempeño.

El Comité Institucional de Gestión y Desempeño es el responsable de orientar la implementación de la Política de Gobierno Digital, de acuerdo con lo indicado en el artículo 2.2.22.3.8 del Decreto 1083 de 2015; el cual en el numeral 6, señala: "*Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información*". Este Comité, será el responsable de orientar la implementación de la Política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

Teniendo en cuenta que la principal función de este comité se encuentra orientada hacia la implementación y operación de todas las políticas del Modelo Integrado de Planeación y Gestión -MIPG (entre las que se encuentra la de Gobierno Digital); le corresponde articular todos los esfuerzos institucionales, recursos, metodologías y estrategias para el desarrollo de estas políticas y en esta medida, lograr que la Política de Gobierno Digital, se desarrolle enlazándola con las demás políticas, en el marco del Sistema de Gestión de la Entidad.

Mediante la resolución No. 2019-3246 de diciembre de 2019, se crea el Comité Institucional de Gestión y Desempeño de Corpocaldas, la cual ha sido modificada mediante las resoluciones 1092-2022 de Julio del 2022 y 1908-2023 de diciembre del 2023. Se indica en la resolución 1092-2022 de Julio del 2022 que dentro de sus funciones se encuentran: "*Artículo 4. Funciones del Comité Institucional de Gestión y Desempeño*", *numeral 1. Aprobar y hacer seguimiento, por lo menos una vez cada tres meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión MIPG. numeral 2. Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del Modelo Integrado de Planeación y Gestión MIPG, numeral 3. Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión, numeral 4. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información, numeral 5. Aprobar y hacer seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de gestión.*

Se evidenciaron las siguientes actas de reuniones realizadas por el Comité Institucional de Gestión y Desempeño en las vigencias 2024 y 2025 donde se tratan temas relacionados con la Política de Gobierno Digital:

Vigencia 2024:

- **Acta No.1 del 24 y 26 de enero del 2024:** Revisión y aprobación del PETI, del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y del Plan de Seguridad y Privacidad de la Información vigencia 2024.
- **Acta No.2 del 25 de abril del 2024:** Estado de implementación de MIPG y Estado de implementación del MSPI (socialización de la matriz de riesgos y políticas de seguridad para revisión y posterior aprobación)
- **Acta No.4 del 25 de septiembre del 2024:** Informe de seguimiento a planes institucionales.
- **Acta No.5 del 4 de noviembre del 2024:** Socialización para aprobación de la política de seguridad de la información.

Vigencia 2025:

- **Acta No. 1 del 27 y 29 de enero del 2025:** Revisión y aprobación del PETI, del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y del Plan de Seguridad y Privacidad de la Información vigencia 2025.
- **Acta No.2 del 27 de febrero del 2025 (acta enviada sin firmas de aprobación):** Seguimiento a los compromisos de Gestionar la contratación del profesional en seguridad y del plan de implementación de la política

6.1.4 Responsable de liderar la implementación la Política de Gobierno Digital.

El responsable de liderar la implementación la Política de Gobierno Digital: es el director, jefe de oficina o coordinador de tecnologías y sistemas de la información y las comunicaciones o G-CIO (sigla en inglés de Government Chief Information Officer), o quien haga sus veces en la entidad, de acuerdo con lo indicado en el artículo 2.2.35.5. del Decreto 1083 de 2015. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

Se pudo evidenciar en el acta del CGD No. 3 del 21 de junio del 2022 en el ítem 9 de proposiciones y varios “Definición de líderes de las políticas de MIPG” la designación del Profesional Especializado de TIC de Corpocaldas como el responsable de las políticas 7 y 8 de MIPG “Gobierno Digital y Seguridad Digital”.

Gestión Tecnológica es un proceso de apoyo de acuerdo con el modelo de operación por procesos (MOP) de la entidad, el Profesional Especializado de TIC depende directamente de la Subdirección Administrativa y Financiera de acuerdo con la estructura organizacional y forma parte del Comité Institucional de Gestión y Desempeño. Lo anterior se aparta de lo establecido en el Decreto 1083 de 2015 en su artículo 2.2.35.4, por lo que se recomienda realizar una revisión jurídica para determinar las acciones de ajuste que correspondan, salvaguardando la autonomía institucional.

6.1.5 Otros Roles e instancias importantes.

6.1.5.1 Grupo de trabajo de Arquitectura empresarial.

Este grupo actúa como un comité técnico de arquitectura empresarial, que evalúa los impactos de cualquier decisión de inversión, adquisición o modernización de sistemas de información e infraestructura tecnológica en la Entidad. Así mismo, tiene funciones de gobierno sobre la arquitectura empresarial de la entidad y debe remitirse al Comité Institucional de Gestión y Desempeño cuando se requieran tomar decisiones de alto nivel.

Este grupo debe estar conformado por el Director de Tecnologías de la Información y las Comunicaciones (CIO) o quien haga sus veces, el Director de Planeación, Profesionales encargados de las arquitecturas de sistemas de información y arquitectura de infraestructura tecnológica, el líder de gestión o información o arquitecto de información de la entidad y líderes de las áreas funcionales y de procesos cuando se requiera.

Aunque este grupo según indica el Manual de Gobierno digital es deseable más no obligatorio, el líder de la Oficina TIC indicó que "*el grupo no está creado en la Entidad, dado que no se cuenta con los profesionales requeridos para su conformación ya que actualmente el área TIC está conformado por: 1 profesional especializado, 2 técnicos y 2 contratistas".*

Según lo indicado por el Líder de la OTIC se asignaron recursos en la vigencia 2025 para iniciar la primera etapa de implementación de arquitectura empresarial, se recomienda validar la conformación de un grupo de arquitectura con la participación del subdirector de planificación y los líderes de las áreas funcionales y de procesos cuando se requiera, con el fin de evaluar los impactos de las decisiones a tomar y realizar un plan de acción pertinente y apropiado para los intereses de la Entidad.

6.1.5.2 Responsable de Seguridad de la Información.

Se debe designar un responsable de Seguridad de la Información que a su vez responderá por la Seguridad Digital en la entidad, el cual debe pertenecer a un área que haga parte del direccionamiento estratégico o Alta Dirección.

Se evidenció que no se cuenta con un profesional responsable de la seguridad de la información desde el año 2024, situación que ha sido tratada en el Comité Institucional de Gestión y Desempeño.

6.1.5.3 Oficina de Control Interno.

Ejecuta acciones de seguimiento y control con enfoque en gestión de riesgos para validar el nivel de implementación de la Política de Gobierno Digital en conjunto con la alta dirección, los líderes de proceso y los funcionarios que hacen parte de la oficina TIC. Este seguimiento es fundamental para garantizar la efectividad, transparencia y cumplimiento normativo de los procesos, al identificar oportunamente desviaciones y riesgos que puedan afectar la gestión institucional. Además, la Oficina de Control Interno juega un rol clave en fortalecer la cultura de autocontrol y responsabilidad, promoviendo la mejora continua y asegurando que los planes y estrategias digitales se implementen de manera coherente y alineada con los objetivos estratégicos de la entidad.

6.2 AUTODIAGNÓSTICO POLÍTICA DE GOBIERNO DIGITAL.

Se validó el autodiagnóstico de MIPG para la Política de Gobierno Digital de las vigencias 2023, 2024 y 2025 observando unas calificaciones de **81,3%** (para la vigencia 2024) y de **88.3%** (para la vigencia 2025).

De acuerdo con la información recibida por parte del líder de la OTIC, se evidencian como meses de realización de los autodiagnósticos los siguientes: vigencia 2023 (marzo), vigencia 2024 (junio) y vigencia 2025 (abril) con lo que podría concluirse que los resultados no son tenidos en cuenta como punto de partida para la elaboración de los PETI de cada vigencia, ya que estos deben ser aprobados y publicados finalizando el mes de enero de cada año.

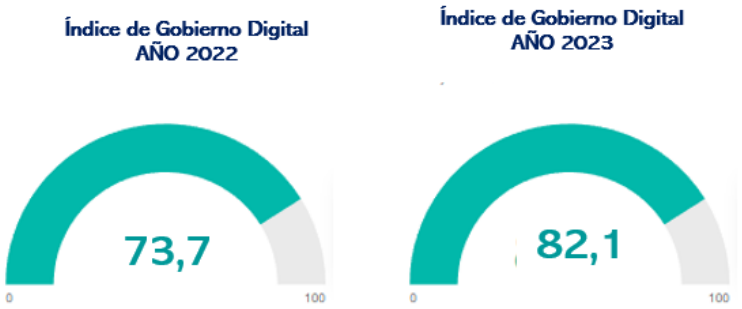
También se evidenció en el autodiagnóstico que para las vigencias 2024 y 2025 la calificación del habilitador "Uso y apropiación de los Servicios Ciudadanos Digitales" fue del 37,1% y 85,7%, respectivamente. Al consultar al líder de la OTIC sobre el Plan de Implementación de Servicios Ciudadanos Digitales correspondiente a dichas vigencias, este indicó: *"No se cuenta con un plan de implementación de servicios ciudadanos".* Esta situación dificulta el seguimiento, ya que no es posible evidenciar un plan con acciones y metas específicas que permitan verificar el avance reportado en el autodiagnóstico.

Además, en la vigencia 2025 se evidenció un resultado de cumplimiento dentro del habilitador "Fortalecimiento de la Arquitectura Empresarial y de la Gestión de TI" del 125% que altera el resultado general del diagnóstico por lo que se sugiere revisar el archivo para garantizar la confiabilidad de los datos.

Adicionalmente, se encontró que las gráficas de los resultados de las vigencias 2024 y 2025 no se están generando en el archivo del autodiagnóstico, lo que podría dificultar la realización de análisis comparativos que permitan contribuir en la toma de decisiones y en la formulación de acciones pertinentes para la Entidad en materia de Gobierno Digital.

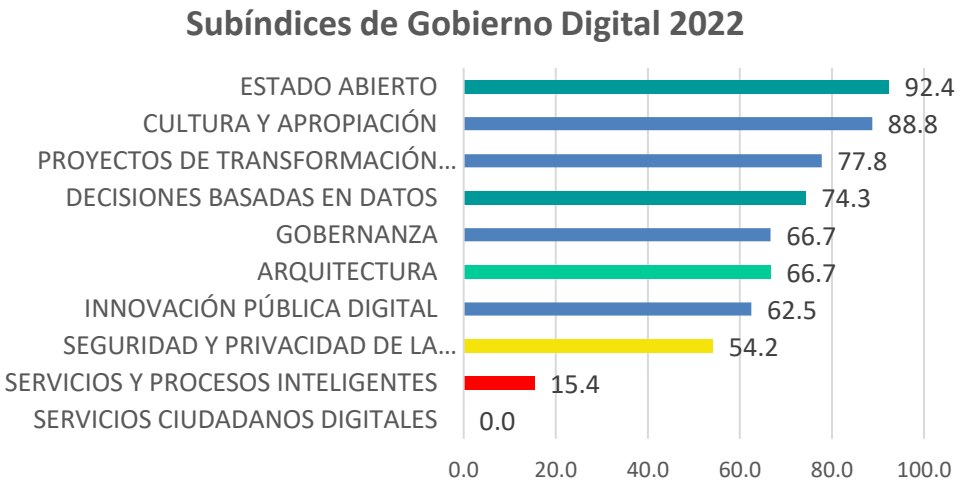
6.3 VERIFICACIÓN DE LOS RESULTADOS DE LA EVALUACIÓN DE LA POLÍTICA DE GOBIERNO DIGITAL REALIZADA A TRAVÉS DEL FORMULARIO ÚNICO REPORTE DE AVANCES DE LA GESTIÓN – FURAG, VIGENCIA 2022 Y 2023.

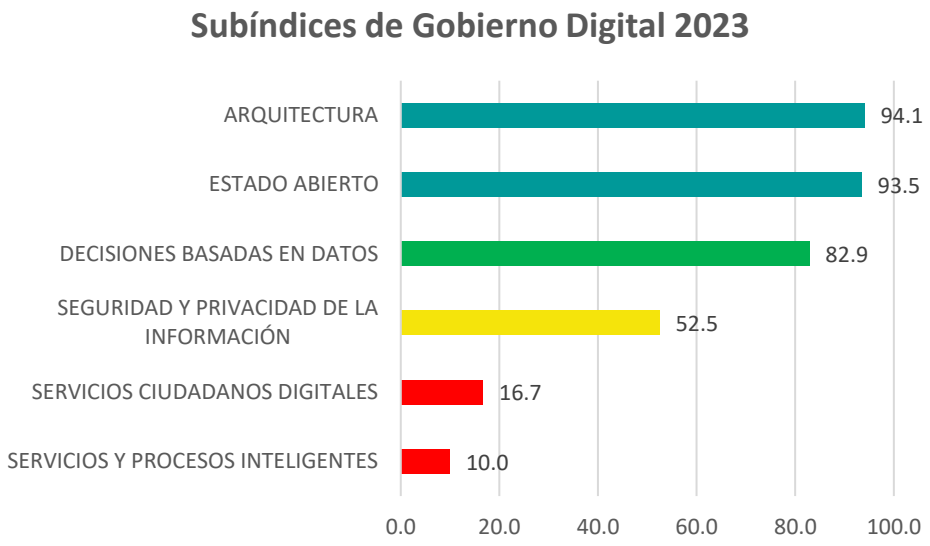
Teniendo en cuenta que el FURAG, es el instrumento que permite medir anualmente a las entidades públicas en el ejercicio de la gestión y desempeño de su labor, a continuación, se presentan los principales resultados alcanzados por la Oficina TIC en la Política de Gobierno Digital vigencias 2022 y 2023, de acuerdo con los resultados publicados por el DAFP:



Fuente: DAFP

A continuación, se muestran los resultados de los subíndices de Gobierno Digital de las vigencias 2022 y 2023:





Se observa en los subíndices de la vigencia 2023 que los componentes con mayor fortaleza son Arquitectura y Estado Abierto con calificaciones de 94,1 y 93,5 respectivamente.

En los subíndices de la vigencia 2023 en los que se identifican debilidades son: Servicios y Procesos Inteligentes, Servicios Ciudadanos Digitales y Seguridad y Privacidad de la información donde se obtuvieron los menores puntajes 10, 16,7 y 52,5 respectivamente, los cuales coinciden con los menor calificados en la vigencia 2022.

6.4 SEGUIMIENTO A LOS PLANES QUE FORMAN PARTE DE LA POLÍTICA

6.4.1 Plan Estratégico de Tecnologías de la Información – PETI.

Dentro de la Política de Gobierno Digital (PGD), se establece el Habilitador de Arquitectura, el cual agrupa las temáticas, lineamientos y productos que deben desarrollar las entidades públicas para fortalecer sus capacidades internas de gestión de tecnologías de la información. Este habilitador se fundamenta en el Marco de Referencia de Arquitectura Empresarial (MRAE), un conjunto de instrumentos que orienta a las entidades en la implementación del enfoque de Arquitectura Empresarial (AE), facilitando la gestión y el gobierno de TI, así como el desarrollo de proyectos estratégicos con componentes tecnológicos.

La Arquitectura Empresarial es una práctica estratégica que permite a las entidades públicas transformar su gestión de manera disciplinada, estructurada y sostenible, con el fin de alcanzar sus objetivos institucionales, responder a las necesidades de los grupos de interés y generar mayor valor público. Este enfoque no solo contempla el diseño y la

planeación, sino también la implementación de soluciones y el fortalecimiento de capacidades clave, promoviendo así organizaciones públicas de alto desempeño.

El Marco de Referencia de Arquitectura Empresarial (MRAE) proporciona una estructura conceptual, principios, lineamientos y mejores prácticas que permiten a las entidades articular su orientación estratégica, su modelo de gestión y su estrategia de tecnologías de información. En este contexto, **el Plan Estratégico de Tecnologías de la Información (PETI)** se convierte en una herramienta fundamental para expresar la Estrategia de TI de la entidad, alineada con los objetivos institucionales y los lineamientos del Gobierno Digital.

Se evidencian los PETI de las vigencias 2024 y 2025 publicados en la página web de la Entidad en el menú de “Transparencia y Acceso a la Información Pública” los cuales fueron aprobados en las actas del CGD No.1 del 24 y 26 de enero del 2024 y No. 1 del 27 y 29 de enero del 2025.

Se realiza validación del PETI de la vigencia 2025, confirmando cumplimiento del diseño de acuerdo con la guía MGGTI.GE.ES.03 - Guía para la Construcción del PETI, de noviembre del 2023 que se encuentra publicada en la página de MinTIC, con lo que se estaría cumpliendo la acción propuesta por el auditado en el plan de mejoramiento definido para subsanar el hallazgo #3 declarado en el informe final de auditoría realizado en la vigencia 2024 de fecha 23 de diciembre del 2024.

6.4.2 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

De conformidad con el documento Maestro del Modelo de Seguridad y Privacidad de la Información, del Ministerio de Tecnologías de la Información y las Comunicaciones de Octubre del 2021, **en el numeral 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información** la entidad debe:

Lineamiento: Definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita:

- Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos.
- Elaborar una declaración de aplicabilidad que contenga: los controles necesarios, su estado de implementación y la justificación de posible exclusión.
- Definir un plan de tratamiento de riesgos que contenga, fechas y responsables con el objetivo de realizar trazabilidad.
- Los dueños de los riesgos deben realizar la aprobación formal del plan de tratamiento de riesgos y esta aceptación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.

Propósito: Estructurar una metodología que permita definir las acciones que debe seguir la Entidad para poder gestionar los riesgos de seguridad y privacidad de la información.

Entradas recomendadas: Inventario de activos de información de la Entidad y valoración de los riesgos de seguridad de la información.

Se evidencian Planes de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de las vigencias 2024 y 2025 publicados en la página web de la Entidad en el menú de "Transparencia y Acceso a la Información Pública" los cuales fueron aprobados en las actas del CGD No.1 del 24 y 26 de enero del 2024 y No. 1 del 27 y 29 de enero del 2025.

Sin embargo, es necesario que la OTIC tenga presente el cumplimiento de todos los lineamientos emitidos en el documento Maestro del Modelo de Seguridad y Privacidad de la Información para la implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información ya que algunos de ellos no pudieron evidenciarse, con el fin de contar con:

- ✓ Plan de tratamiento de riesgos **aprobado por los dueños de los riesgos y el Comité Institucional de Gestión y Desempeño** (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia).

- ✓ **Declaración de aplicabilidad, aceptada y aprobadas en el Comité de Gestión Institucional.** No tener un Plan de Tratamiento de Riesgos aprobado por los dueños de los riesgos significa que no existe un documento formal que describa cómo se abordarán los riesgos identificados, y que esta gestión no ha sido revisada ni aprobada por las instancias responsables. Esto implica que no hay un lineamiento o instrumento aprobado, claro y socializado a todos los funcionarios de la Entidad, sobre las acciones a tomar para mitigar o controlar esos riesgos, lo que puede llevar a una gestión poco certera de los mismos y aumentar la probabilidad de que ocurran o tengan un impacto negativo.

6.4.3 Plan de Seguridad y Privacidad de la información.

El Plan de Seguridad y Privacidad de la Información, según la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), busca garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos, a través de la gestión de riesgos y la implementación de controles. Se basa en el Modelo de Seguridad y Privacidad de la Información (MSPI) y busca que las entidades incorporen la seguridad en todos sus procesos y activos.

La Corporación Autónoma Regional de Caldas establece el Plan de Seguridad y Privacidad de la Información con el fin de dar cumplimiento al Decreto 1008 de 2018 que establece los lineamientos generales de la Política de Gobierno Digital que deberán adoptar las entidades pertenecientes a la administración pública, encaminados hacia la transformación digital y el mejoramiento de las capacidades TIC, para el desarrollo del habilitador transversal "Seguridad y privacidad de la Información" de la Política de Gobierno Digital; al Decreto 1499 de 2017 que determina el cumplimiento institucional de las Políticas de Gobierno y Seguridad Digital en relación con el habilitador "Seguridad y privacidad de la Información"; a la Resolución 500 de 2021 de MinTIC que establece los lineamientos para implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) y la resolución interna No. 2019-3246 de diciembre de 2019, por la cual se constituye el Comité Institucional de Gestión y Desempeño de Corpocaldas, en donde se establece en una de sus funciones "*Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información*".

Para Corpocaldas, se evidencian Planes de Seguridad y Privacidad de la Información de las vigencias 2024 y 2025 publicados en la página web de la Entidad en el menú de "Transparencia y Acceso a la Información Pública" los cuales fueron aprobados en las actas del CGD No.1 del 24 y 26 de enero del 2024 y No. 1 del 27 y 29 de enero del 2025.

6.4.4 Plan de Implementación de Servicios Ciudadanos Digitales.

Según la Política de Gobierno Digital del MinTIC, las entidades públicas deben contar con un Plan de Implementación de Servicios Ciudadanos Digitales con el fin de fortalecer la relación entre el Estado y los Ciudadanos, mediante el uso estratégico de tecnologías digitales. Este plan permite a las entidades ofrecer servicios más accesibles, eficientes y seguros, facilitando la autenticación digital, la interoperabilidad entre sistemas y el acceso a la Carpeta Ciudadana Digital. Además, responde a la necesidad de cumplir con los lineamientos establecidos en el Manual de Gobierno Digital, que exige planear, implementar, medir y mejorar continuamente el uso de los habilitadores digitales, entre ellos los Servicios Ciudadanos Digitales, como parte esencial de la transformación digital.

Para este seguimiento, la Oficina de Control Interno solicitó al líder de la OTIC el Plan de Implementación de Servicios Ciudadanos Digitales de las vigencias 2024 y 2025 evidenciando que no se encuentran disponibles, lo cual representa una oportunidad de mejora prioritaria en pro del cumplimiento de los lineamientos establecidos en los Decretos 1078 del 2015 y 088 del 2022.

6.4.5 Plan de Transformación Digital con Horizonte a cinco (5) años.

Según la Política de Gobierno Digital del MinTIC, las entidades públicas en Colombia **deben formular un Plan de Transformación Digital con horizonte a cinco (5) años** como una herramienta estratégica para guiar su evolución hacia un modelo de gestión más eficiente, transparente e innovador. Este plan permite a las entidades alinear sus procesos, servicios y cultura organizacional con el uso de tecnologías emergentes y disruptivas, asegurando la generación de valor público y una mejor relación con la ciudadanía. La visión a cinco años garantiza una planificación estructurada, sostenible y con impacto a largo plazo, permitiendo a las entidades adaptarse a los nuevos retos y mejorar la calidad de vida de los ciudadanos mediante servicios más ágiles, accesibles y centrados en sus necesidades.

Para este seguimiento, la Oficina de Control Interno solicitó al líder de la OTIC el Plan de Transformación Digital con Horizonte a cinco (5) años para lo cual indicó *"**No se cuenta con un plan de transformación digital**"*.

El objetivo de un **plan de transformación digital con el uso de tecnologías emergentes y disruptivas** es contar con una hoja de ruta estratégica que guíe a la Entidad en la adopción de tecnologías digitales con el objetivo de **cambiar radicalmente** su forma de operar, relacionarse con los usuarios y generar valor. La clave está en la **disrupción**, que implica no solo mejorar lo existente, sino **reinventar procesos, modelos de servicio y estructuras organizativas** a través de la tecnología.

Contar con un plan de transformación digital representa una oportunidad estratégica para mejorar la eficiencia operativa, fortalecer la transparencia y aumentar la capacidad de respuesta frente a los retos tecnológicos y ambientales. Su desarrollo permitiría a la entidad anticiparse a los cambios, adaptarse con agilidad y ofrecer servicios más eficaces y alineados con las necesidades actuales.

6.5 SEGUIMIENTO Y EVALUACION DEL AVANCE DE LA POLÍTICA.

Se evidenció que la entidad hace seguimiento al estado de avance de la implementación de la política, a través de las siguientes acciones:

6.5.1 Medición del cumplimiento de los planes: El líder de la OTIC remitió archivo donde se evidencia el porcentaje de cumplimiento de los planes para la vigencia 2024 así:

PLAN	% CUMPLIMIENTO A SEPTIEMBRE DEL 2024	% DE CUMPLIMIENTO A DICIEMBRE DEL 2024
Plan Estratégico de Tecnologías de la Información – PETI	63%	91%
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	28%	28%
Plan de Seguridad y Privacidad de la Información	59%	59%

Fuente: Oficina TIC

Los resultados **al cierre de septiembre del 2024** fueron socializados en Comité de Gestión y Desempeño (CGD), pudiéndose evidenciar en el acta No. 4 del 25 de septiembre del 2024 en el ítem "*Informe de seguimiento a planes institucionales*".

Los resultados de cumplimiento de los planes **al cierre de la vigencia 2024** no fueron socializados oficialmente al CGD pues se evidenció en el acta No.1 del 27 y 29 de enero del 2025 que al tratar el punto 2 del orden del día "*seguimiento cierre a los planes y estrategias vigencia 2024*" se indicó en el desarrollo de este punto lo siguiente: "*se informa al comité que el área de Planeación Institucional realizó seguimiento a los indicadores de cumplimiento de los planes institucionales y estrategias de la vigencia 2024. Estos resultados no son presentados en el comité por motivo de tiempo, con la claridad de que si el comité lo requiere solicitará dicha información durante la revisión y aprobación de los nuevos planes y estrategias*".

Lo anterior, puede limitar la capacidad del comité para ejercer su función de orientación estratégica, articulación de políticas y toma de decisiones por lo que se recomienda desde esta oficina que en el CGD se dediquen espacios para revisar los resultados de los planes y estrategias de cada vigencia, con el fin de identificar oportunidades de mejora y asegurar la alineación de las nuevas estrategias con los aprendizajes y retos que se presenten para de esta manera fortalecer la gobernanza institucional, la transparencia y la efectividad en la implementación de la Política de Gobierno Digital y demás políticas del MIPG.

En el acta No.2 del 27 de febrero del 2025 (acta enviada a la OCI sin firmas de aprobación) se evidencia el seguimiento a los compromisos de la OTIC de gestionar la contratación del profesional en seguridad y del plan de implementación de la política para lo cual el Líder de la OTIC informa "*el CDP está listo, pero hace falta la hoja de vida del profesional experto en seguridad de la información. Manifiesta que la falta de este profesional en seguridad afecta el cumplimiento del plan de mejoramiento de la auditoria del proceso TIC, de igual forma afecta el cumplimiento de los dos planes institucionales: el de seguridad de la información y el plan de riesgos de seguridad.*" Respecto al compromiso relacionado con el plan de implementación de la política, el líder de la OTIC, informa que "*no se puede cumplir este compromiso sin que se haya*

cumplido el compromiso de gestionar la contratación del profesional en seguridad".

Dado lo anterior, se hace evidente la necesidad urgente de una intervención por parte del Comité de Gestión y Desempeño (CGD) para movilizar y agilizar el proceso de contratación del profesional responsable de la Seguridad de la Información en la Entidad. La ausencia de este recurso humano pone en riesgo el cumplimiento del Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos aprobados para la vigencia 2025, así como del plan de mejoramiento derivado de la auditoría al proceso TIC realizada en 2024, según lo señalado por el líder de la OTIC. Adicionalmente, los bajos niveles de cumplimiento de estos planes reportados en la vigencia 2024, reflejan que la entidad no cuenta con una gestión integral ni actualizada de los riesgos de seguridad de la información y de sus controles conforme a una matriz de riesgos aprobada, no dispone de políticas plenamente aprobadas ni socializadas y presenta discontinuidad en la ejecución de acciones estratégicas en materia de seguridad y privacidad de la información. Esta situación puede comprometer la protección de los activos de información, la capacidad institucional de respuesta ante incidentes, la eficiencia operativa, el cumplimiento normativo, la exposición de información sensible o crítica y el debilitamiento del sistema de control interno.

Adicionalmente, se observa que los indicadores de los planes se calculan conforme a lo establecido en el SGI y en los respectivos planes institucionales, considerando el número de proyectos o actividades ejecutadas frente al total programado. Sin embargo, esta metodología presenta una inconsistencia con la forma real de cálculo, ya que actualmente se asigna un porcentaje de avance a cada actividad y luego se obtiene un promedio general. Por lo tanto, se recomienda revisar esta metodología y realizar los ajustes necesarios para garantizar coherencia entre lo planificado y lo reportado. Así mismo, se sugiere evaluar la posibilidad de estructurar los indicadores con base en proyectos que cuenten con metas específicas, lo cual permitiría mejorar la capacidad de la Entidad para medir el impacto real de sus acciones y obtener una visión más integral del avance institucional. De igual manera se sugiere considerar para la definición de los indicadores de seguridad y privacidad de la información la Guía - Indicadores Gestión de Seguridad de la Información del MinTIC.

6.5.2 Seguimiento al uso y aprovechamiento de las TIC tanto en la gestión interna como en la entrega de servicios digitales a usuarios, ciudadanos y grupos de interés.

Se solicitó al líder de la OTIC las mediciones realizadas que permitieran evaluar el nivel de satisfacción de usuarios internos y externos y las tasas de uso de procesos, trámites y servicios digitales vs. presenciales para lo cual indicó: *"No se cuenta con indicadores para*

medir el nivel de satisfacción de usuarios internos y externos y tampoco con indicadores que permitan medir las tasas de uso de procesos, trámites y servicios digitales vs. presenciales"

La ausencia de indicadores que permitan medir la satisfacción de los usuarios internos y externos, así como el nivel de uso de los servicios digitales en comparación con los presenciales, representa una oportunidad de mejora para la Entidad ya que esto puede restringir la medición integral del impacto de los servicios prestados por lo que se sugiere su incorporación para fortalecer la evaluación institucional. Contar con estos indicadores facilitaría también un seguimiento más preciso del avance en la transformación digital y permitiría una mejor alineación de los servicios con las necesidades y expectativas de la ciudadanía.

6.5.3 Autodiagnóstico de la Política de Gobierno Digital.

El autodiagnóstico de la Política de Gobierno Digital permite a las entidades públicas evaluar el grado de avance en la implementación de sus habilitadores y propósitos, estableciendo una línea base que facilita la identificación de fortalezas y oportunidades de mejora. Esta herramienta contribuye a promover una gestión pública más eficiente, transparente y centrada en el ciudadano, al tiempo que impulsa la mejora continua en la calidad de los servicios ofrecidos.

Corpocaldas realiza anualmente el autodiagnóstico general de la "Política de Gobierno Digital" a través de la herramienta dispuesta en el sitio web del Modelo Integrado de Planeación y Gestión (MIPG). No obstante, se evidenció que los autodiagnósticos correspondientes a las vigencias 2023, 2024 y 2025 se realizaron en los meses de marzo, junio y abril, respectivamente. Esta situación sugiere que los resultados del autodiagnóstico no están siendo utilizados como insumo inicial para la elaboración de los Planes Estratégicos de Tecnologías de la Información (PETI) de cada vigencia, los cuales deben ser aprobados y publicados a más tardar en enero de cada año; o en caso de que dichos resultados se estén considerando para la formulación del PETI de la vigencia siguiente, la información utilizada no reflejaría con precisión el desempeño actual de la política, debido a la distancia temporal entre la recolección de datos y la construcción del nuevo plan.

En consecuencia de lo anterior, se hace indispensable ajustar los tiempos de ejecución del autodiagnóstico, de manera que se convierta en un verdadero motor de gestión y planificación, que fortalezca la formulación oportuna de los planes estratégicos y contribuya a una implementación efectiva de la Política de Gobierno Digital.

6.5.4 Autodiagnóstico de Seguridad y Privacidad de la Información

El autodiagnóstico de Seguridad y Privacidad de la Información, exigido por la Política de Gobierno Digital del MinTIC, es una herramienta que permite a las entidades públicas evaluar su nivel de madurez en la gestión de la seguridad y privacidad de la información. Su objetivo principal es identificar fortalezas, debilidades y brechas en estos aspectos, con el fin de planificar acciones de mejora, cumplir con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), y fomentar una cultura organizacional orientada a la protección de los datos.

Se evidenciaron autodiagnósticos del MSPI realizados en Corpocaldas en las vigencias 2023 y 2024 con los siguientes resultados:

Efectividad de Controles:

VIGENCIA	RESULTADO
2023	29
2024	64

Calificación frente a mejores prácticas de ciberseguridad

Vigencia 2023

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	31	100
DETECTAR	23	100
RESPONDER	20	100
RECUPERAR	20	100
PROTEGER	31	100

Vigencia 2024

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	65	100
DETECTAR	56	100
RESPONDER	59	100
RECUPERAR	47	100
PROTEGER	63	100

Obteniendo como resultado un nivel de madurez del modelo del **12% (nivel crítico)** para la vigencia 2023 y del **53% (nivel intermedio)** para la vigencia 2024.

6.5.5 Reporte de implementación de la política a través del FURAG.

La entidad realiza el reporte de la implementación de la política de Gobierno Digital a través del FURAG en los tiempos determinados por el DAFP, pudiéndose evidenciar los resultados de las vigencias 2022 y 2023.

7. RECOMENDACIONES

- ✓ Garantizar que el cargo asignado al líder TIC cumpla con lo establecido en el artículo 2.2.35.4 del Decreto 1083 de 2015, el cual señala que el director, jefe de oficina o coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, debe responder directamente al representante legal de la entidad. Esta adecuación es fundamental para asegurar el cumplimiento normativo, fortalecer el liderazgo estratégico de la política y garantizar su articulación con los objetivos institucionales.

- ✓ Formalizar la conformación de un grupo de trabajo de Arquitectura Empresarial integrando al subdirector de Planificación y a los líderes de las áreas funcionales y de procesos. Este grupo permitirá evaluar de manera técnica y estratégica los impactos de las decisiones relacionadas con la modernización tecnológica, y facilitará la formulación de un plan de acción estructurado que responda a los intereses institucionales y a los lineamientos del Marco de Referencia de Arquitectura Empresarial (MRAE) del MinTIC.

- ✓ Programar y realizar el autodiagnóstico de la Política de Gobierno Digital con la debida anticipación, de manera que sus resultados puedan ser utilizados como insumo técnico para la formulación del Plan Estratégico de Tecnologías de la Información (PETI) de cada vigencia. Esto permitirá que el PETI refleje de forma oportuna las necesidades, brechas y oportunidades identificadas en el diagnóstico, asegurando su alineación con los lineamientos del MinTIC y fortaleciendo la planeación estratégica en materia de transformación digital.

  Se recomienda designar con carácter prioritario al profesional responsable de la Seguridad de la Información, garantizando que este cargo pertenezca a un área de direccionamiento estratégico o de la Alta Dirección, conforme a lo indicado por MinTIC, ya que normas como la ISO 27001 y el Modelo de Seguridad y Privacidad

de la Información del MinTIC (MSPI) promueven la separación de funciones como un principio de control interno, por lo tanto, podría existir un potencial conflicto de interés si quien diseña o implementa los sistemas (Oficina TIC) también es quien se audita o evalúa a sí mismo. A pesar de contar con aprobación del Comité Institucional de Gestión y Desempeño y con disponibilidad presupuestal respaldada por CDP, la falta de esta designación ha limitado el avance de los planes institucionales de seguridad y privacidad de la información y del plan de tratamiento de riesgos de seguridad y privacidad de la información, pudiendo impactar en el cumplimiento del plan de mejoramiento derivado de la auditoría TIC de la vigencia 2024, por lo que se recomienda priorizar esta designación considerando que es un tema crítico con efectos estratégicos para la entidad.

- ✓ Formular y adoptar un **Plan de Implementación de Servicios Ciudadanos Digitales** que incluya acciones, metas, responsables y cronogramas específicos, con el fin de dar cumplimiento a los lineamientos establecidos en el Manual de Gobierno Digital y facilitar el seguimiento y evaluación del avance institucional. La ausencia de este plan impide verificar la coherencia entre los resultados reportados en el autodiagnóstico y las acciones realmente ejecutadas, lo que puede afectar la trazabilidad, la toma de decisiones y el cumplimiento normativo en materia de transformación digital orientada al ciudadano.

- ✓ Se recomienda revisar el archivo del autodiagnóstico de la vigencia 2025, dado que se evidenció un resultado de cumplimiento del 125%, lo cual podría afectar la confiabilidad del resultado general.

- ✓ Se recomienda garantizar la generación de gráficas en los archivos de autodiagnóstico para facilitar el análisis comparativo entre vigencias y apoyar la toma de decisiones estratégicas.

- ✓ Priorizar acciones de mejora en los componentes de **Servicios y Procesos Inteligentes**, **Servicios Ciudadanos Digitales** y **Seguridad y Privacidad de la Información**, dado que han presentado los puntajes más bajos de forma reiterada en los subíndices del FURAG durante las vigencias 2022 y 2023. Esta situación evidencia la necesidad de formular planes de acción por componente y de realizar seguimientos rigurosos a su implementación, con el fin de elevar el nivel de madurez digital de la entidad y cumplir con los estándares establecidos por el MinTIC.

- ✓ Cumplir con todos los lineamientos emitidos en el documento Maestro del Modelo de Seguridad y Privacidad de la Información para la implementación del Plan de

Tratamiento de Riesgos de Seguridad y Privacidad de la Información con el fin de poder demostrar la aprobación por parte de los dueños de los riesgos, adicional a la del CGD y de contar con una declaración de aplicabilidad, aceptada y aprobada también por el CGD.

- ✓ Formular y adoptar un Plan de Transformación Digital con horizonte a cinco (5) años, en cumplimiento a los lineamientos establecidos por el MinTIC. Este plan debe servir como hoja de ruta estratégica para orientar la evolución institucional hacia un modelo de gestión más eficiente, transparente e innovador, alineando los procesos, servicios y cultura organizacional con el uso de tecnologías emergentes. La ausencia de este instrumento limita la capacidad de planificación a largo plazo, dificulta la articulación de iniciativas digitales y reduce el impacto de las acciones orientadas a generar valor público y mejorar la experiencia del ciudadano.

- ✓ Establecer espacios formales y periódicos para la revisión y análisis de los resultados de cumplimiento de los planes y estrategias institucionales por parte del Comité de Gestión y Desempeño (CGD). Esta práctica permitirá fortalecer su rol de orientación estratégica, facilitar la identificación de oportunidades de mejora y asegurar que las decisiones sobre nuevos planes y estrategias se fundamenten en los aprendizajes y retos evidenciados. La socialización oportuna de estos resultados también contribuye a la transparencia, la trazabilidad de la gestión institucional y la efectividad en la implementación de la Política de Gobierno Digital y demás políticas del MIPG.

- ✓ Revisar y ajustar la metodología utilizada para el cálculo de los indicadores de cumplimiento de los planes institucionales, con el fin de garantizar coherencia entre lo planificado y lo reportado. Específicamente, se sugiere evitar promedios generales que puedan distorsionar el avance real, y en su lugar, estructurar indicadores basados en proyectos con metas específicas y medibles. Esta mejora permitirá una evaluación más precisa del impacto de las acciones institucionales. Adicionalmente, para los indicadores relacionados con seguridad y privacidad de la información, se recomienda adoptar como referencia la “Guía de Indicadores de Gestión de Seguridad de la Información” del MinTIC.

- ✓ Diseñar e implementar indicadores que permitan medir el nivel de satisfacción de los usuarios internos y externos, así como las tasas de uso de procesos, trámites y servicios digitales frente a los presenciales. Estos indicadores son fundamentales para evaluar el impacto del uso de las TIC en la gestión institucional y en la calidad del servicio ofrecido a la ciudadanía. Contar con esta información permitirá identificar oportunidades de mejora, orientar decisiones estratégicas y fortalecer el enfoque de Gobierno Digital

centrado en el usuario, en línea con los principios de eficiencia, transparencia y accesibilidad.

- ✓ Se recomienda priorizar la intervención de las brechas identificadas en los autodiagnósticos realizados en el marco del MSPI, fortaleciendo paralelamente la cultura organizacional en torno a la seguridad de la información. Para ello, es fundamental implementar procesos continuos de capacitación, sensibilización y apropiación institucional. Asimismo, se deben establecer mecanismos efectivos de seguimiento y mejora continua que permitan avanzar progresivamente hacia niveles superiores de madurez, en concordancia con los estándares del MSPI y los lineamientos establecidos por la Política de Gobierno Digital del MinTIC.

- ✓ Revisar e implementar un plan de acción con las recomendaciones emitidas por el DAFP de acuerdo con los últimos resultados del FURAG.

Manizales, 24 de junio de 2025.

Atentamente,

Lina María Daza Gallego
Jefe Oficina de Control Interno

Elaboró: Paula Andrea Rabelly P. Profesional OCI
Revisó: Lina María Daza G.