Cartagena de Indias D. T., y C;
DC- OF- EX 088 06-12-2023

Doctor (es)
WILLIAM DAU CHAMAT
Alcalde Mayor
INGRID PAOLA SOLANO BENITEZ
Jefe Oficina Asesora Informática
Alcaldía Mayor de Cartagena de indias
Ciudad

Asunto: Informe Definitivo Auditoria de Cumplimiento vigencia 2022

Cordial saludo

La Contraloría Distrital de Cartagena de Indias, en cumplimiento del Plan de Vigilancia y Control Fiscal Territorial – PVCFT vigencia 2023, practicó Auditoria de Cumplimiento a la Política de Gobierno Digital del Distrito de Cartagena de Indias, con el fin de efectuar el análisis, evaluación y coherencia de los resultados de la contratación, la legalidad y los avances en la implementación de la Política de Gobierno Digital.

Cabe anotar que, durante el proceso auditor no se dieron a conocer observaciones que fueran elevadas a hallazgos administrativos, por lo que la entidad no suscribirá Plan de Mejoramiento.

Atentamente,

ANGELA MARIA CUBIDES GONZALEZ
Contralora Distrital de Cartagena de Indias

Revisó: Hernando Pertuz Corcho
Director Técnico de Auditoría Fiscal

Anexos: treinta y nueve (39) folios

Elaboró: Gladis Ávila Marengo
Auxiliar Administrativo

CONTRALORIA
DISTRITAL DE CARTAGENA DE INDIAS
CONTROL FISCAL AUTÓNOMO Y COMPROMETIDO CON LA CIUDADANÍA

INFORME DEFINITIVO AUDITORÍA DE CUMPLIMIENTO GOBIERNO DIGITAL

ALCALDIA MAYOR DE CARTAGENA DE INDIAS
VIGENCIA 2022

CONTRALORÍA DISTRITAL DE CARTAGENA DE INDIAS
Cartagena, diciembre de 2023

INFORME DEFINITIVO

AUDITORÍA DE CUMPLIMIENTO
GOBIERNO DIGITAL
VIGENCIA 2022

Contralor Distrital	**ANGELA MARÍA CUBIDES GONZÁLEZ**
Director Técnico de Auditoria Fiscal	**HERNANDO PERTUZ CORCHO**
Supervisor	**ANTONIO SANCHEZ BALLESTEROS**
Líder de auditoría	**MANUEL CASSIANI CAÑATE**

TABLA DE CONTENDO

1. CARTA DE CONCLUSIONES

Doctor (es)
WILLIAM DAU CHAMAT
Alcalde Mayor
INGRID PAOLA SOLANO BENITEZ
Jefe Oficina Asesora Informática
Alcaldía Mayor de Cartagena de indias
Ciudad

Cordial saludo

Con fundamento en las facultades otorgadas por el Artículos 267 y 272 de la Constitución Política y de conformidad con lo estipulado en la Resolución Administrativa 056 del 01 de junio de 2021, la Contraloría Distrital de Cartagena realizó **Auditoria de cumplimiento a la Política de Gobierno Digital del Distrito de Cartagena de Indias, correspondiente a la Vigencia Fiscal 2022.**

Es responsabilidad de la Administración, el contenido en calidad y cantidad de la información suministrada, así como con el cumplimiento de las normas que le son aplicables a su actividad institucional en relación con el asunto auditado.

Es obligación de la Contraloría Distrital expresar con independencia una conclusión sobre el cumplimiento de las disposiciones aplicables al Alcalde Mayor del Distrito de Cartagena de Indias, conclusión que debe estar fundamentada en los resultados obtenidos en la auditoría realizada.

Este trabajo se ajustó a lo dispuesto en los Principios fundamentales de auditoría y las Directrices impartidas para la auditoría de cumplimiento, conforme a lo establecido en la Resolución Administrativa 056 del 1º de junio de 2021, proferida por la Contraloría Distrital de Cartagena, en concordancia con las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI[1]), desarrolladas por la Organización Internacional de las Entidades Fiscalizadoras Superiores (INTOSAI[2]) para las Entidades Fiscalizadoras Superiores.

Estos principios requieren de parte de la Contraloría Territorial la observancia de las exigencias profesionales y éticas que requieren de una planificación y

[1] ISSAI: The International Standards of Supreme Audit Institutions.

[2] INTOSAI: International Organisation of Supreme Audit Institutions.

ejecución de la auditoría destinadas a obtener garantía limitada, de que los procesos consultaron la normatividad que le es aplicable.

La auditoría incluyó el examen de las evidencias y documentos que soportan el proceso auditado y el cumplimiento de las disposiciones legales y que fueron remitidos por las entidades consultadas.

Los análisis y conclusiones se encuentran debidamente documentados en papeles de trabajo.

La auditoría se adelantó en la vigencia 2023. El período auditado tuvo como fecha de corte 31 de diciembre de 2022 y abarcó el período comprendido entre el 01 de enero de 2022 y 31 de diciembre de 2022.

1.1 INTRODUCCIÓN

Con las modificaciones experimentadas en la transición de la Estrategia de Gobierno en Línea a la Política Digital, se instaura un enfoque renovado en el cual no solo el Estado, sino también diversos actores de la sociedad, se erigen como elementos fundamentales para el desarrollo integral del Gobierno Digital en Colombia. En este marco, las necesidades y problemáticas del contexto determinan la aplicación de la tecnología y su contribución a la generación de valor público. En consonancia con las normas ISSAI, se busca fortalecer la transparencia y eficacia en la gestión gubernamental digital.

En este contexto, el nuevo objetivo de la Política de Gobierno Digital se articula de la siguiente manera: "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".

Para dar cumplimiento a esta política, resulta imperativo que el ente de control aplique el Manual de Gobierno Digital, el cual establece los lineamientos y estándares de los componentes de la política. La implementación se desglosa en dos componentes principales: TIC para el Estado y TIC para la Sociedad. Estos se ven potenciados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, los cuales, bajo los preceptos de las normas ISSAI, se traducen en requisitos mínimos que deben cumplir todos los sujetos obligados para alcanzar los objetivos de la política.

La evolución constante del gobierno electrónico en Colombia ha destacado la importancia de las TIC para optimizar la gestión en las entidades públicas y los

servicios que el Estado brinda a los ciudadanos. Sin embargo, emerge una nueva realidad donde la política de Gobierno Digital no solo mejora procesos y servicios existentes, sino que también posibilita la transformación digital, alterando la relación tradicional entre el Estado y el ciudadano.

En este nuevo contexto, el Gobierno Digital se erige como el motor de la transformación digital del Estado, propiciando la eficiencia en la atención a las necesidades y problemáticas de los ciudadanos. Bajo el enfoque de las normas ISSAI, se promueve la participación activa de los ciudadanos en los procesos de cambio mediante el uso y apropiación de las tecnologías digitales.

Así, la Política de Gobierno Digital, alineada con las normas ISSAI, establece lineamientos, estándares y proyectos estratégicos que facilitan la transformación digital del Estado. El propósito es lograr una interacción más efectiva con ciudadanos, usuarios y grupos de interés, permitiendo la resolución satisfactoria de necesidades, el abordaje de problemáticas públicas, el impulso del desarrollo sostenible y, en última instancia, la creación de valor público.

1.2 OBJETIVO POLÍTICA

Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital

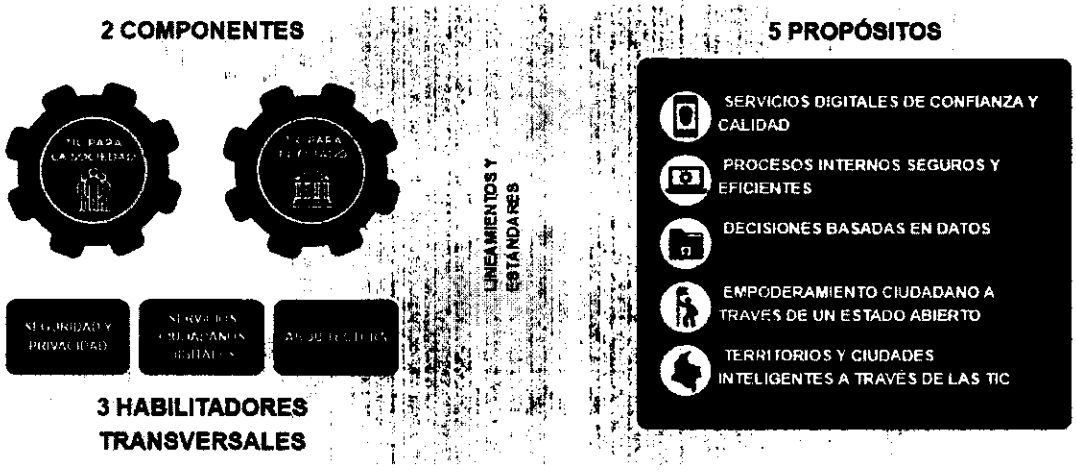
Propósitos:

- Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad
- Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información
- Tomar decisiones basadas en datos a partir del aumento en el uso y aprovechamiento de la información
- Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto
- Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales, a través del aprovechamiento de las TIC

1.3 ELEMENTOS DE LA POLÍTICA

Para la implementación de la Política de Gobierno Digital, se han definido dos componentes y tres habilitadores transversales que definen lineamientos y estándares para el desarrollo de servicios digitales de confianza y calidad, procesos digitales seguros y eficientes, contar con datos e información de calidad para tomar decisiones, promover la la apropiación de la tecnología para empoderar al ciudadano y contar con ciudades y territorios inteligentes.

Ilustración 1 - Elementos de la política de Gobierno Digital



2 OBJETIVO DE LA AUDITORÍA

Auditoria de Cumplimiento a la Política de Gobierno Digital del Distrito de Cartagena de Indias, correspondiente a la Vigencia Fiscal 2022.

El Objetivo de la auditoría fue:

2.1 OBJETIVO GENERAL

Realizar la auditoría de Cumplimiento para efectuar el análisis, evaluación y coherencia de los resultados de la contratación, la legalidad y los avances en la implementación de la Política de Gobierno Digital, teniendo en cuenta lo definido en la Constitución Política de Colombia especialmente el Art. 209, el Decreto Único Reglamentario 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones, los manuales de contratación y los procedimientos de la entidad, con la finalidad de conceptuar sobre la gestión de las Tecnologías de la Información y las Comunicaciones de la misma, durante la vigencia 2022.

2.2 FUENTES DE CRITERIO

2.3 De acuerdo con el objeto de la evaluación, el marco legal sujeto a verificación fue:

Gestión Contractual:

- Constitución Política de Colombia Artículos 209 y 211
- Ley 80 de 1993, sus decretos reglamentarios y todas las normas que lo
- adicionen, modifiquen o deroguen y a lo consagrado en el Estatuto General
- de contratación
- Ley 1150 de 2007.
- Decreto 1082 de 2015.
- Decreto Ley 019 de 2012.
- Ley 1474 de 2011.
- Ley 42 de 1993.
- Decreto 2641 de 2012.
- Decreto 092 de 2017.
- Decreto 403 de 2020
- Ley 1712 de 2014.
- Ley 87 de 1993, reglamentada por los Decretos 2145 de 1999 y 1537 de 2001
- Decreto 1499 de 2017.
- Decreto 111 de 1996, compilatorio de las Leyes 38 de 1989 y 179 de 1994.
- Decreto 1737 de 1998.
- Circular Externa No. 1 de junio 21 de 2013 emitida por la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, respecto a la publicación de los contratos.
- Manual y Estatuto de contratación de la Entidad.

Política de Gobierno Digital:

- Resolución 500 de 2021.
- Resolución 2893 de 2020 - Anexo 1 - Anexo 2 - Anexo 2.1 - Anexo 3 - Anexo 3.1 - Anexo 4 - Anexo 4.1 - Anexo 5 - Anexo 5.1
- Resolución 2893 de 2020
- Resolución 2160 de 2020
- Resolución 1519 de 2020
- Decreto 620 de 2020
- Ley 2052 de 2020
- Resolución 2160 de 2020 - Anexo 1 - Anexo 2

- Ley 2052 de 2020
- Resolución 1519 de 2020 - Anexo1 - Anexo 2 - Anexo 3 - Anexo 4
- Decreto 620 de 2020 - Servicios Ciudadanos Digitales
- Decreto 2106 de 2019 - Simplificación, supresión y reforma de trámites, procesos y procedimientos innecesarios existentes en la administración pública
- Decreto 2106 de 2019
- Ley 1955 de 2019
- Ley 1978 de 2019
- Resolución 1443 de 2018 - Por el cual se sustituyen los artículos 15 y 19 y se modifica el artículo 17 de la Resolución 2405 de 2016
- Resolución 1443 de 2018
- Resolución 2405 de 2016
- Decreto 1166 de 2016
- Decreto 415 de 2016
- Resolución 2405 de 2016 - Por el cual se adopta el modelo del Sello de Excelencia Gobierno en Línea
- Decreto 415 de 2016 - Lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones
- Acuerdo 03 de 2015
- Decreto 1083 de 2015
- Decreto 1069 de 2015
- Decreto 1078 de 2015
- Resolución 3564 de 2015 - Reglamentaciones asociadas a la Ley de Transparencia y Acceso a la Información Pública
- Decreto Reglamentario Único 1081 de 2015 Decreto 103 de 2015 - Reglamento sobre la gestión de la información pública
- Decreto 1078 de 2015 Decreto Único Sectorial - Lineamientos generales de la Estrategia de Gobierno en Línea
- Ley 1712 de 2014 - Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional
- Ley Estatutaria 1581 de 2012 - Protección de datos personales
- Decreto 235 de 2010 - Intercambio de información entre entidades para el cumplimiento de funciones públicas

2.3 ALCANCE DE LA AUDITORÍA

Durante este proceso auditor se evaluarán los criterios identificados en los objetivos específicos, y el control fiscal interno.

2.4 RESULTADOS EVALUACIÓN CONTROL INTERNO

Con base en el PT-24 y en el análisis previo a este documento, específicamente en la fase de planeación y ejecución, se registra la evaluación de la entidad en diversos componentes:

1. Ambiente de Control: La entidad cuenta con controles establecidos para detectar, identificar, prevenir o disminuir los riesgos de fraude. Esto se respalda mediante procedimientos y manuales legalizados.
2. Gestión del Riesgo: La alta dirección demuestra conciencia sobre la probabilidad de ocurrencia del riesgo de fraude en los procesos y actividades relacionadas con la materia auditada. La Política de Gobierno Digital se actualiza periódicamente, respaldada por manuales internos, guías y planes.
3. Actividades de Control: La entidad ha implementado mecanismos como planes de contingencia, continuidad del negocio, tratamiento del riesgo y seguridad de la información. Estos mecanismos permiten mitigar y tratar los riesgos identificados, como la pérdida de confidencialidad, integridad y disponibilidad de los activos, evitando situaciones que obstaculicen el logro de los objetivos del sujeto de control.
4. Información y Comunicación: El sujeto de control comunica las prácticas y controles diseñados para prevenir y detectar riesgos a través de diferentes comités institucionales.
5. Supervisión y Monitoreo: La entidad realiza un monitoreo efectivo de la ejecución de planes, acciones y controles para mitigar o detectar riesgos. Las auditorías internas realizadas por Control Interno y otros entes competentes del Nivel Nacional contribuyen a este proceso. Además, la entidad cuenta con procedimientos y manuales que mitigan los riesgos de fraude.

De acuerdo con el PT-24, la evaluación resultante en el componente de control interno es "ADECUADO". La calificación general sobre la calidad y eficiencia del control fiscal interno del asunto o materia es "EFICIENTE", como se refleja en el desarrollo del PT-24-AC.

EVALUACIÓN CONTROL INTERNO

					CALIFICACIÓN SOBRE LA EFICIENCIA Y EFICACIA DEL CONTROL FISCAL INTERNO (RANGO DE ADECUADO O INADECUADO)
1,30		PARCIALMENTE ADECUADO	MEDIO	CON DEFICIENCIAS	1,2

De > 1,5 a 2,0	Con deficiencias

2.6 RELACIÓN DE OBSERVACIONES

Como resultado de la auditoría, el equipo auditor de la Contraloría Distrital de Cartagena no constituyó observaciones, para los cinco (5) criterios auditados.

OBSERVACIONES	CANTIDAD	VALOR (en pesos)
1. ADMINISTRATIVOS	0	
2. DISCIPLINARIOS	0	
3. PENALES	0	
4. FISCALES	0	
TOTALES (1,2,3,4 y 5)	0	

ANGELA MARIA CUBIDES GONZALEZ
Contralora Distrital de Cartagena de Indias

Equipo de Auditoría

HERNANDO PERTUZ CORCHO
Director Técnico de Auditoría Fiscal

ANTONIO SANCHEZ BALLESTEROS
Supervisor

MANUEL CASSIANI CAÑATE
Profesional Universitario – Lider

3. OBJETIVOS Y CRITERIOS

Los objetivos específicos y los criterios de auditoría aplicados en la evaluación de la Política de Gobierno Digital del Distrito de Cartagena de Indias para la Vigencia Fiscal 2022 fueron los siguientes:

3.1 OBJETIVOS ESPECÍFICOS

1. Emitir concepto sobre la gestión fiscal, administrativa y contractual adelantada para la contratación y ejecución de los proyectos de tecnología del PETI, verificando la recepción de los bienes y servicios de conformidad con las especificaciones técnicas establecidas y la cobertura a la población beneficiaria.
2. Evaluar el estado de implementación de la Política de Gobierno Digital en el Distrito de Cartagena.

3.2 CRITERIOS DE AUDITORÍA

1. Criterio de Revisión del Componente TIC para la Sociedad y del Componente TIC para el Estado:
   1.1. Evaluación de la alineación de las iniciativas y proyectos del Componente TIC para la Sociedad con los objetivos y necesidades de los ciudadanos.
   1.2. de la efectividad y eficiencia en la implementación del Componente TIC para el Estado, considerando la mejora de los procesos internos gubernamentales.
2. Criterio de Revisión de Habilitadores Transversales:
   2.1. Evaluación de la implementación y efectividad de los habilitadores transversales de seguridad y privacidad, servicios ciudadanos digitales y arquitectura.
   2.2. De la coherencia y sinergia entre estos habilitadores para garantizar una implementación integral y eficaz.
3. Criterio de Revisión de Servicios Digitales:

3.1. Evaluación de la confianza y calidad de los servicios digitales ofrecidos, considerando la experiencia del usuario, la disponibilidad, y la capacidad de respuesta.
3.2. Análisis de la seguridad de los procesos internos digitales, tomando en cuenta la protección de la información y la eficiencia operativa.

4. Criterio de Evaluación de Riesgos y Controles:
   4.1. Identificación y evaluación de los riesgos asociados a la implementación de la Política de Gobierno Digital, tanto en el Componente TIC para la Sociedad como en el Componente TIC para el Estado.
   4.2. Revisión de la efectividad de los controles establecidos para mitigar los riesgos identificados.
5. Criterio de Reporte de Beneficios de Control Fiscal:
   5.1. Identificación y documentación de los beneficios derivados del control fiscal durante el proceso de auditoría.
   5.2. Presentación de los resultados positivos obtenidos, destacando mejoras en eficiencia, transparencia, y eficacia en la gestión gubernamental.

Estos criterios proporcionan una base estructurada para evaluar diferentes aspectos de la Política de Gobierno Digital, desde la implementación de componentes específicos hasta la evaluación de riesgos y controles, y finalmente, la documentación y comunicación de los beneficios obtenidos durante el proceso auditor.

4. RESULTADOS DE LA AUDITORÍA

4.1 RESULTADOS GENERALES SOBRE EL ASUNTO O MATERIA AUDITADA

En el transcurso de la presente auditoría, se procedió a evaluar la implementación de la Política de Gobierno Digital llevada a cabo por la Alcaldía Mayor de Cartagena de Indias durante la vigencia fiscal 2022. El análisis de dicha política se refleja en las conclusiones derivadas de cada uno de los objetivos específicos abordados en el informe.

La auditoría se enfocó en examinar la efectividad y el cumplimiento de los objetivos establecidos en la Política de Gobierno Digital, abarcando distintos aspectos, desde la alineación con normativas hasta la eficiencia en la implementación de componentes específicos como TIC para la Sociedad y TIC para el Estado, así como los habilitadores transversales de seguridad y privacidad, servicios ciudadanos digitales y arquitectura.

Además, se evaluaron criterios relacionados con la calidad de los servicios digitales ofrecidos, la seguridad de los procesos internos, la toma de decisiones basada en datos, el empoderamiento ciudadano a través de un estado abierto y el fomento de territorios y ciudades inteligentes mediante las TIC.

El cuerpo del informe presenta las conclusiones derivadas de este análisis detallado, proporcionando una visión integral de la efectividad y el impacto de la Política de Gobierno Digital durante la vigencia fiscal 2022, en la Alcaldía Mayor de Cartagena de Indias. Estas conclusiones ofrecen una base para la toma de decisiones y la formulación de recomendaciones que contribuyan a fortalecer y mejorar la implementación de la política en el futuro.

Seguimiento Mapa de Riesgo

#	Riesgo	
R1	Riesgo de Pérdida de Reputación y Consecuencias Económicas debido al No Cumplimiento de Normativas Legales de Seguridad y Privacidad de la Información, causado por la Falta de Actualización en Asuntos Legales o Políticos en las Operaciones de la Entidad.	
R2	Riesgo de Pérdida Económica y Reputacional debido a Retrasos en el Cumplimiento de las Etapas del Ciclo de Desarrollo de Nuevas Funcionalidades o Ajustes en Aplicaciones o Software, derivado de la Ausencia de Protocolos y Metodologías Adecuadas para el Desarrollo de Software.	60%
R3	Riesgo de Pérdida Económica y Reputacional por la Inadecuada Formulación de Proyectos de Tecnologías de la Información (TI), Resultante de la Desarticulación con el Plan de Desarrollo Vigente.	
R4	Riesgo de Pérdida Económica y Reputacional debido a Sanciones por Incumplimiento de Metas Establecidas en el Plan de Desarrollo Vigente, Causado por la Insuficiente Asignación de Recursos.	
R5	Riesgo de Pérdida Reputacional debido a Interrupciones en la Prestación de Servicios de Tecnologías de la Información (TI), sin considerar los Niveles de Servicio (ANS) establecidos en el Catálogo de Servicios, ocasionado por la Carencia de Mantenimiento Preventivo y Correctivo en Equipos y Software de la Infraestructura Tecnológica.	60%

R6	Riesgo de Pérdida Económica y Reputacional debido a Retrasos en los Procesos del Distrito, ocasionados por la Insuficiencia de Capacidad en la Infraestructura de Tecnologías de la Información (TI).	60%	60%
R7	Riesgo de Pérdida Económica y Reputacional debido a la Pérdida Total o Parcial de la Información Contenida en las Bases de Datos, como resultado del Incumplimiento de las Políticas de Seguridad Digital.		
R8	Riesgo de Pérdida Económica y Reputacional debido a la Ocurrencia de Eventos que Afecten la Totalidad o Parte de la Infraestructura Tecnológica (hardware, software, redes, etc.) del Distrito, como Consecuencia del Incumplimiento de las Políticas de Seguridad Digital.		60%
R9	Riesgo de Pérdida Económica y Reputacional debido a la Pérdida de Integridad de la Base de Datos, originada por la Ausencia de Políticas de Control de Acceso, Contraseñas sin Protección y Mecanismos de Autenticación Débil.		
R10	Riesgo de Pérdida Económica y Reputacional debido a la Afectación de la Integridad de la Información Contenida en las Bases de Datos, como resultado del Incumplimiento de los Procedimientos Establecidos.		
R11	Riesgo de Pérdida Reputacional debido a la Afectación de la Integridad y Disponibilidad de la Página Web de la Alcaldía Distrital de Cartagena de Indias, Causada por la Ausencia de Certificados de Navegación Segura, ya sea por Vencimiento de las Licencias o por la Falta de Presupuesto para Renovarlos.		
R12	Riesgo de Pérdida Reputacional debido al Incumplimiento de Uno o Más de los Criterios de Usabilidad Establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic), Originado por el No Cumplimiento de la Política de Gobierno Digital.	60%	60%
R13	Riesgo de Pérdida Económica y Reputacional debido a la Falta o Escasa Autorización para el Tratamiento de Datos Personales, como Resultado del Incumplimiento de la Política de Tratamiento de Datos Personales.		
R14	Riesgo de Pérdida Económica y Reputacional derivado del Incumplimiento de Uno o más de los Criterios Establecidos para que una Entidad Pública Cumpla con los Requerimientos de Gobierno Digital, como Consecuencia de la Inobservancia de la Política de Gobierno Digital.	60%	60%
R15	Riesgo de Pérdida Económica y Reputacional debido a Vulnerabilidades No Detectadas en los Sistemas	60%	60%

	Informáticos, Originado por un Escaso o Nulo Escaneo de Vulnerabilidades en la Página Web.		
R16	Riesgo de Pérdida Económica y Reputacional debido a Fallos en los Mecanismos de Autenticación, Ocasionados por la Falta o Insuficiente Control de Autenticación en los Sistemas Informáticos.	60%	60%
R17	Riesgo de Pérdida Reputacional y Económica debido a Sistemas de Información Obsoletos, Incapaces de Actualizarse, Parcharse o Integrarse, Originado por su Creación en Lenguajes de Programación Obsoletos y Sin Compatibilidad.		
R18	Riesgo de Pérdida Económica y Reputacional debido a Equipos Tecnológicos Obsoletos o Tecnología Desactualizada, Resultante de que su Vida Útil ha Llegado a su Término.		

Exploracion de aspectos asociados a los riesgos

R1. La posibilidad de pérdida reputacional y económica debido al incumplimiento de la normatividad legal vigente en materia de seguridad y privacidad de la información, causado por la desactualización en temas legales o políticos en las operaciones de la entidad, es un riesgo significativo y multifacético.
A continuación, se exploran los aspectos clave asociados con esta situación:

1) **Reputación Institucional:**
   a) Descripción del Riesgo: La falta de actualización en temas legales y políticos podría resultar en decisiones o prácticas que no se alinean con los estándares actuales de seguridad y privacidad de la información.
   b) Impacto Potencial: Esto podría dañar la reputación de la entidad, ya que la sociedad y los stakeholders pueden percibir el incumplimiento como una negligencia en la protección de la información sensible.
2) **Sanciones y Multas:**
   a) Descripción del Riesgo: La desactualización podría llevar a la falta de cumplimiento de leyes y regulaciones, lo que podría resultar en sanciones legales y multas.
   b) Impacto Potencial: Las penalizaciones económicas y las sanciones podrían tener un impacto directo en los recursos financieros de la entidad, generando pérdidas económicas sustanciales.
3) **Pérdida de Confianza:**
   a) Descripción del Riesgo: La falta de cumplimiento puede erosionar la confianza de los ciudadanos, usuarios y otras partes interesadas en la capacidad de la entidad para gestionar y proteger adecuadamente la información.

b) Impacto Potencial: La pérdida de confianza puede tener consecuencias a largo plazo en las relaciones con los stakeholders, lo que puede afectar la colaboración y la participación ciudadana.

4) **Daño a la Imagen Gubernamental:**
   a) Descripción del Riesgo: El incumplimiento podría afectar la imagen del gobierno, ya que se espera que las entidades gubernamentales lideren en el cumplimiento de las normas y regulaciones.
   b) Impacto Potencial: El daño a la imagen gubernamental puede tener consecuencias negativas en la percepción de la efectividad y transparencia del gobierno.
5) **Costos de Remediación:**
   a) Descripción del Riesgo: La necesidad de remediar el incumplimiento puede generar costos adicionales, tanto en términos de recursos financieros como de tiempo.
   b) Impacto Potencial: Los costos asociados con la corrección de las deficiencias y la implementación de medidas correctivas pueden ser significativos.

R2. El riesgo de pérdida económica y reputacional derivado de retrasos en el cumplimiento de las etapas del ciclo de desarrollo de nuevas funcionalidades o ajustes en aplicaciones o software, a causa de la ausencia de protocolos y metodologías adecuadas para el desarrollo de software, es un desafío crítico para cualquier entidad que dependa de soluciones tecnológicas. Aquí se detallan los aspectos clave relacionados con este riesgo:

1) **Pérdida de Oportunidades de Mercado:**
   a) Descripción del Riesgo: La falta de protocolos y metodologías adecuadas puede conducir a retrasos en la entrega de nuevas funcionalidades, lo que podría resultar en la pérdida de oportunidades para adaptarse rápidamente a las demandas del mercado.
   b) Potencial: La entidad podría perder ventaja competitiva y oportunidades de negocio frente a competidores que logran implementar cambios más ágilmente.
2) **Percepción de Ineficiencia:**
   a) Descripción Riesgo: Los retrasos continuos pueden llevar a la percepción de que la entidad es ineficiente en la gestión de sus desarrollos de software.
   b) Impacto Potencial: Esto podría afectar la reputación de la entidad, generando desconfianza entre los usuarios y stakeholders, lo que a su vez podría afectar la participación y colaboración.
3) **Costos Adicionales:**
   a) Descripción del Riesgo: Los retrasos en el ciclo de desarrollo pueden resultar en costos adicionales, ya sea por recursos extra necesarios para

acelerar el proceso o por pérdida de ingresos debido a la demora en la implementación.
   b) Impacto Potencial: Los costos adicionales pueden afectar negativamente los recursos económicos de la entidad y comprometer la rentabilidad de los proyectos.
4) **Insatisfacción del Ciudadano:**
   a) Descripción del Riesgo: La ausencia de protocolos eficientes puede llevar a la entrega de productos que no cumplen con las expectativas de la ciudadanía.
   b) Impacto Potencial: La insatisfacción del usuario puede generar retroalimentación negativa, disminuyendo la aceptación de las soluciones tecnológicas y afectando la percepción de calidad.
5) **Incumplimiento de Plazos Regulatorios:**
   a) Descripción del Riesgo: Los retrasos pueden ocasionar incumplimientos en plazos regulatorios, especialmente en entornos donde existen requisitos normativos específicos.
   b) Impacto Potencial: El incumplimiento de plazos regulatorios puede resultar en sanciones, multas u otras consecuencias legales y reputacionales.

R3. La posibilidad de pérdida económica y reputacional debido a la inadecuada formulación de proyectos de Tecnologías de la Información (TI), derivada de la desarticulación con el plan de desarrollo vigente, es un riesgo significativo que puede afectar negativamente a la entidad. Aquí se destacan los aspectos claves asociados con este riesgo:

1) **Desalineación con Objetivos Estratégicos:**
   a) Descripción del Riesgo: La inadecuada formulación de proyectos de TI puede resultar en iniciativas que no están alineadas con los objetivos estratégicos y metas delineadas en el plan de desarrollo vigente.
   b) Potencial: La desalineación puede generar una pérdida de recursos económicos en proyectos que no contribuyen de manera efectiva a los objetivos más amplios de la entidad.
2) **Pérdida de Eficiencia y Efectividad**
   a) Descripción del Riesgo: La falta de integración con el plan de desarrollo puede dar lugar a proyectos de TI que no optimizan los recursos disponibles, disminuyendo la eficiencia y efectividad de la implementación.
   b) Impacto Potencial: La entidad podría enfrentar desafíos en la consecución de resultados esperados, lo que afectaría su capacidad para cumplir con sus funciones y metas.
3) **Costos Adicionales y Desviaciones Presupuestarias:**
   a) Descripción del Riesgo: La desarticulación con el plan de desarrollo puede conducir a desviaciones presupuestarias y costos adicionales, ya que los proyectos pueden requerir ajustes y correcciones durante su ejecución.

b) Impacto Potencial: Los costos adicionales pueden impactar negativamente en los recursos económicos disponibles, generando presiones financieras en la entidad.

4) **Reputación Afectada:**
   a) Descripción del Riesgo: La falta de alineación puede llevar a la percepción de que la entidad no gestiona adecuadamente sus recursos y proyectos de TI, afectando su reputación.
   b) Impacto Potencial: La reputación de la entidad puede deteriorarse, generando desconfianza entre los stakeholders y la comunidad.
5) **Incumplimiento de Plazos y Entregables:**
   a) Descripción del Riesgo: La falta de coordinación con el plan de desarrollo puede resultar en demoras y dificultades en el cumplimiento de plazos y entregables establecidos para los proyectos de TI.
   b) Impacto Potencial: El incumplimiento de plazos puede afectar la implementación oportuna de soluciones tecnológicas críticas.

R4. La posibilidad de pérdida económica y reputacional debido a sanciones por el incumplimiento con las metas establecidas en el plan de desarrollo vigente, derivada de la falta de asignación de recursos, es un riesgo que puede tener consecuencias significativas para una entidad. A continuación, se exploran los aspectos claves asociados con este riesgo:

1) **Incumplimiento de Metas Estratégicas:**
   a) Descripción del Riesgo: La falta de asignación de recursos puede conducir al incumplimiento de las metas estratégicas y objetivos delineados en el plan de desarrollo.
   b) Impacto Potencial: El no logro de metas estratégicas puede tener consecuencias directas en la capacidad de la entidad para cumplir con su misión y funciones.
2) **Sanciones y Penalizaciones:**
   a) Descripción del Riesgo: El incumplimiento con las metas establecidas en el plan de desarrollo puede resultar en sanciones y penalizaciones, especialmente si hay obligaciones legales o normativas asociadas.
   b) Potencial: Las sanciones y penalizaciones pueden generar pérdidas económicas significativas y afectar la situación financiera de la entidad.
3) **Reputación Afectada:**
   a) Descripción del Riesgo: La incapacidad para cumplir con las metas estratégicas puede afectar la reputación de la entidad, especialmente si se percibe como una falta de compromiso o gestión ineficiente.
   b) Impacto Potencial: La reputación de la entidad puede sufrir daños, generando desconfianza entre los stakeholders y la comunidad.

4) **Desconfianza de Stakeholders:**
   a) Descripción del Riesgo: La falta de asignación de recursos y el consecuente incumplimiento de metas pueden generar desconfianza entre los stakeholders, incluyendo ciudadanos, colaboradores y financiadores.
   b) Potencial: La desconfianza puede dificultar la colaboración futura, el respaldo financiero y la participación de stakeholders clave.
5) **Impacto en Finanzas y Presupuesto:**
   a) Descripción del Riesgo: La pérdida de recursos debido al incumplimiento puede afectar las finanzas y presupuesto de la entidad, generando presiones económicas y limitando su capacidad para abordar otras prioridades.
   b) Impacto Potencial: La entidad puede enfrentar dificultades financieras que afectan su capacidad de operación y ejecución de proyectos.

R5. La posibilidad de pérdida reputacional debido a interrupciones en la prestación de los servicios de Tecnologías de la Información (TI), sin tener en cuenta los Acuerdos de Niveles de Servicio (ANS) establecidos en el catálogo de servicios, debido a la falta de mantenimiento preventivo y correctivo de los equipos y software de la infraestructura tecnológica, es un riesgo crítico que puede impactar negativamente en la percepción de la entidad. Aquí se exploran los aspectos clave relacionados con este riesgo:

1) **Interrupciones en la Prestación de Servicios:**
   a) Descripción del Riesgo: La falta de mantenimiento preventivo y correctivo puede aumentar la probabilidad de fallas y, por ende, de interrupciones en la prestación de servicios de TI.
   b) Impacto Potencial: Las interrupciones pueden afectar la continuidad de los servicios, generando insatisfacción entre los usuarios y stakeholders.
2) **Incumplimiento de ANS Establecidos:**
   a) Descripción del Riesgo: La falta de mantenimiento puede llevar al incumplimiento de los ANS establecidos en el catálogo de servicios, afectando la calidad y disponibilidad de los servicios tecnológicos.
   b) Impacto Potencial: El incumplimiento de los ANS puede generar desconfianza entre los usuarios y stakeholders, impactando negativamente la percepción de la calidad del servicio.
3) **Pérdida de Productividad:**
   a) Descripción del Riesgo: Las interrupciones y la falta de mantenimiento pueden provocar una pérdida de productividad para los usuarios que dependen de los servicios de TI.
   b) Impacto Potencial: La pérdida de productividad puede generar frustración y afectar la eficiencia operativa de la entidad.

4) **Reputación Afectada:**
   a) Descripción del Riesgo: Las interrupciones frecuentes y la percepción de falta de mantenimiento pueden afectar la reputación de la entidad, generando una imagen de falta de fiabilidad en sus servicios.
   b) Impacto Potencial: La reputación puede sufrir daños, afectando la confianza y la percepción pública de la entidad.
5) **Costos Asociados a Incidentes no Planificados:**
   a) Descripción del Riesgo: La falta de mantenimiento puede resultar en incidentes no planificados, generando costos adicionales asociados a la resolución de problemas y recuperación de servicios.
   b) Impacto Potencial: Los costos adicionales pueden afectar el presupuesto de la entidad y comprometer recursos que podrían destinarse a otras iniciativas.

R6. La posibilidad de pérdida económica y reputacional por retrasos en los procesos del Distrito, debido a la falta de capacidad de infraestructura de Tecnologías de la Información (TI), es un riesgo crítico que puede impactar negativamente en la eficiencia operativa y en la percepción pública de la entidad. A continuación, se exploran los aspectos clave relacionados con este riesgo:

1) **Retrasos en Procesos Clave:**
   a) Descripción del Riesgo: La falta de capacidad de infraestructura TI puede conducir a retrasos en la ejecución de procesos clave, afectando la eficiencia y eficacia de las operaciones del Distrito.
   b) Impacto Potencial: Los retrasos en procesos críticos pueden tener consecuencias directas en la prestación de servicios, en la toma de decisiones y en el cumplimiento de plazos establecidos.
2) **Pérdida de Productividad:**
   a) Descripción del Riesgo: La falta de capacidad puede resultar en una disminución de la productividad de los usuarios y del personal que depende de la infraestructura TI para realizar sus tareas diarias.
   b) Impacto Potencial: La pérdida de productividad puede afectar la capacidad del Distrito para cumplir con sus responsabilidades y metas operativas.
3) **Impacto en la Atención Ciudadana:**
   a) Descripción del Riesgo: La falta de capacidad puede afectar la capacidad de la entidad para atender las necesidades y consultas de la ciudadanía de manera oportuna.
   b) Impacto Potencial: La insatisfacción ciudadana puede generar una pérdida de confianza y afectar la reputación del distrito.
4) **Costos Asociados a Correcciones Urgentes:**
   a) Descripción del Riesgo: La falta de capacidad puede requerir correcciones urgentes, generando costos adicionales para abordar la infraestructura insuficiente.

b) Impacto Potencial: Los costos adicionales pueden afectar el presupuesto del Distrito y limitar recursos que podrían destinarse a otras prioridades.

5) **Reputación Institucional Afectada:**
   a) Descripción del Riesgo: Los retrasos y la falta de capacidad pueden afectar la reputación del Distrito, generando percepciones negativas sobre su capacidad para gestionar eficientemente los recursos tecnológicos.
   b) Impacto Potencial: La reputación de la entidad puede sufrir daños, afectando la confianza de los stakeholders y la percepción pública.

R7. La posibilidad de pérdida económica y reputacional por la pérdida total o parcial de la información contenida en las bases de datos, debido al incumplimiento de las políticas de seguridad digital, es un riesgo crítico que puede tener consecuencias graves para una entidad. A continuación, se exploran los aspectos clave relacionados con este riesgo:

1) **Pérdida de Información Sensible:**
   a) Descripción del Riesgo: El incumplimiento de políticas de seguridad digital puede abrir la puerta a la pérdida de información sensible almacenada en las bases de datos.
   b) Potencial: La pérdida de información sensible puede tener consecuencias financieras y legales, afectando la confidencialidad de datos críticos.
2) **Impacto en la Continuidad del Negocio:**
   a) Descripción del Riesgo: La pérdida total o parcial de información puede afectar la continuidad del negocio al interrumpir procesos críticos dependientes de la información almacenada.
   b) Potencial: La interrupción en la operación normal puede resultar en pérdidas económicas significativas y en la incapacidad para cumplir con obligaciones contractuales.
3) **Costos de Recuperación y Restauración:**
   a) Descripción del Riesgo: La recuperación y restauración de datos perdidos pueden generar costos sustanciales, especialmente si no se cuentan con sistemas de respaldo adecuados.
   b) Impacto Potencial: Los costos asociados con la recuperación pueden afectar el presupuesto de la entidad y comprometer recursos que podrían destinarse a otras iniciativas.
4) **Violaciones a la Privacidad:**
   a) Descripción del Riesgo: La pérdida de información puede resultar en violaciones a la privacidad de individuos cuyos datos se encuentran en las bases de datos.
   b) Impacto Potencial: Las violaciones a la privacidad pueden tener consecuencias legales y reputacionales, generando desconfianza en la entidad.

5) **Reputación Institucional Afectada:**
   a) Descripción del Riesgo: La pérdida de información sensible y los problemas de seguridad pueden afectar la reputación de la entidad.
   b) Impacto Potencial: La reputación dañada puede generar desconfianza entre los stakeholders, incluyendo ciudadanos, colaboradores y socios comerciales.

R8. La posibilidad de pérdida económica y reputacional por la ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) del Distrito, debido al incumplimiento de las políticas de seguridad digital, es un riesgo crítico que requiere una atención especial. A continuación, se detallan los aspectos clave relacionados con este riesgo:

1) **Paralización de Operaciones:**
   a) Descripción del Riesgo: Eventos que afecten la infraestructura tecnológica pueden resultar en la paralización total o parcial de las operaciones del Distrito.
   b) Impacto Potencial: La interrupción de operaciones puede generar pérdidas económicas directas y afectar la capacidad del Distrito para cumplir con sus funciones y responsabilidades.
2) **Pérdida de Datos Críticos:**
   a) Descripción del Riesgo: Incidentes de seguridad pueden conducir a la pérdida de datos críticos almacenados en la infraestructura tecnológica.
   b) Potencial: La pérdida de datos críticos puede tener consecuencias financieras y operativas, así como impactar la confidencialidad y la integridad de la información.
3) **Costos de Recuperación y Restauración:**
   a) Descripción del Riesgo: La recuperación y restauración de la infraestructura tecnológica después de un incidente de seguridad puede generar costos significativos.
   b) Impacto Potencial: Los costos asociados con la recuperación pueden afectar el presupuesto del Distrito y comprometer recursos que podrían destinarse a otras iniciativas.
4) **Tiempo de Inactividad Prolongado:**
   a) Descripción del Riesgo: La falta de cumplimiento de políticas de seguridad puede prolongar el tiempo necesario para recuperarse de un evento, aumentando el tiempo de inactividad.
   b) Impacto Potencial: El tiempo de inactividad prolongado puede generar mayores pérdidas económicas y afectar la percepción pública del distrito.
5) **Daño a la Reputación:**
   a) Descripción del Riesgo: Los eventos que afectan la infraestructura tecnológica pueden dañar la reputación del Distrito, generando

preocupaciones sobre la capacidad de gestionar adecuadamente los recursos tecnológicos.
   b) Impacto Potencial: La reputación dañada puede afectar la confianza de los stakeholders y la percepción pública del Distrito como entidad responsable.
6) **Posible Pérdida de Confianza Ciudadana:**
   a) Descripción del Riesgo: La ocurrencia de eventos de seguridad puede generar una pérdida de confianza por parte de la ciudadanía en la capacidad del Distrito para proteger la información y garantizar la continuidad de servicios.
   b) Impacto Potencial: La pérdida de confianza ciudadana puede afectar la colaboración y el respaldo público al Distrito.

R9. La posibilidad de pérdida económica y reputacional debido a la pérdida de la integridad de la base de datos, derivada de la ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, es un riesgo crítico que puede tener consecuencias significativas. Aquí se detallan los aspectos claves relacionados con este riesgo:

1) **Acceso No Autorizado:**
   a) Descripción del Riesgo: La falta de políticas de control de acceso y mecanismos de autenticación débil puede abrir la puerta a accesos no autorizados a la base de datos.
   b) Impacto Potencial: Accesos no autorizados pueden llevar a la manipulación, eliminación o alteración de datos, comprometiendo la integridad de la base de datos.
2) **Manipulación de Datos:**
   a) Descripción del Riesgo: Contraseñas sin protección y políticas de control de acceso deficientes facilitan la manipulación maliciosa de datos por parte de usuarios no autorizados.
   b) Impacto Potencial: La manipulación de datos puede afectar la validez y confiabilidad de la información almacenada, generando pérdidas económicas y operativas.
3) **Fugas de Información Confidencial:**
   a) Descripción del Riesgo: Accesos no autorizados pueden resultar en la pérdida de información confidencial almacenada en la base de datos.
   b) Impacto Potencial: La pérdida de información confidencial puede tener consecuencias legales y reputacionales, afectando la confianza de stakeholders y la percepción pública.
4) **Costos Asociados a Incidentes:**
   a) Descripción del Riesgo: Incidentes de seguridad derivados de contraseñas sin protección pueden generar costos significativos asociados con la gestión y resolución de incidentes.

b) Impacto Potencial: Los costos adicionales pueden afectar el presupuesto y comprometer recursos que podrían destinarse a otras iniciativas.

5) **Reputación Afectada:**
   a) Descripción del Riesgo: La pérdida de integridad de la base de datos puede afectar la reputación de la entidad, generando preocupaciones sobre la gestión de la seguridad de la información.
   b) Impacto Potencial: La reputación dañada puede afectar la confianza de los stakeholders y la percepción pública de la entidad.
6) **Incumplimiento de Normativas:**
   a) Descripción del Riesgo: La pérdida de integridad de datos puede resultar en el incumplimiento de normativas y regulaciones relacionadas con la protección de la información.
   b) Impacto Potencial: El incumplimiento puede generar sanciones legales y multas, además de afectar la relación con entidades reguladoras.

R10. La posibilidad de pérdida económica y reputacional por la afectación de la integridad de la información contenida en las bases de datos, debido al incumplimiento de los procedimientos establecidos, es un riesgo crítico que puede tener consecuencias significativas. A continuación, se exploran los aspectos clave relacionados con este riesgo:

1) **Manipulación No Autorizada de Datos:**
   a) Descripción del Riesgo: El incumplimiento de procedimientos establecidos puede facilitar la manipulación no autorizada de datos almacenados en las bases de datos.
   b) Impacto Potencial: La manipulación no autorizada puede comprometer la integridad de la información, afectando su confiabilidad y validez.
2) **Errores e Inconsistencias en la Información:**
   a) Descripción del Riesgo: La falta de cumplimiento de procedimientos puede dar lugar a errores y inconsistencias en la gestión de datos, afectando la integridad de la información.
   b) Impacto Potencial: Errores y datos inconsistentes pueden generar pérdidas económicas y afectar la toma de decisiones basada en información inexacta.
3) **Pérdida de Confianza:**
   a) Descripción del Riesgo: La afectación de la integridad de la información puede resultar en la pérdida de confianza por parte de stakeholders que dependen de la precisión de los datos.
   b) Impacto Potencial: La pérdida de confianza puede afectar la reputación de la entidad y generar desconfianza entre usuarios, clientes y otros stakeholders.

4) **Incumplimiento de Normativas y Regulaciones:**
   a) Descripción del Riesgo: La afectación de la integridad de datos puede llevar al incumplimiento de normativas y regulaciones relacionadas con la gestión y protección de la información.
   b) Impacto Potencial: El incumplimiento puede resultar en sanciones legales y multas, además de afectar la imagen pública de la entidad.
5) **Costos de Recuperación y Restauración:**
   a) Descripción del Riesgo: La restauración de la integridad de datos afectados puede generar costos significativos en términos de tiempo y recursos.
   b) Impacto Potencial: Los costos asociados con la recuperación pueden afectar el presupuesto y comprometer recursos destinados a otras iniciativas.
6) **Daño a la Reputación Institucional:**
   a) Descripción del Riesgo: Los incidentes que afectan la integridad de la información pueden dañar la reputación de la entidad, generando percepciones negativas sobre su capacidad de gestionar la información de manera segura.
   b) Impacto Potencial: La reputación dañada puede afectar la confianza de los stakeholders y la percepción pública de la entidad como responsable y competente.

R11. La posibilidad de pérdida reputacional por la afectación de la integridad y disponibilidad de la página web de la Alcaldía Distrital de Cartagena de Indias debido a la ausencia de certificados de navegación segura por vencimiento de las licencias o por falta de presupuesto para renovarlos es un riesgo crítico que puede impactar la confianza de los usuarios y la percepción pública de la entidad. A continuación, se detallan los aspectos claves relacionados con este riesgo:

1) **Riesgo de Ciberseguridad:**
   a) Descripción del Riesgo: La falta de certificados de navegación segura puede hacer que la página web sea vulnerable a amenazas cibernéticas, comprometiendo la integridad de la información y la disponibilidad del servicio.
   b) Impacto Potencial: Vulnerabilidades cibernéticas pueden resultar en accesos no autorizados, manipulación de información, o interrupción del servicio, afectando la confianza de los usuarios.
2) **Pérdida de Confianza del Usuario:**
   a) Descripción del Riesgo: La interrupción o compromiso de la página web debido a la falta de certificados puede generar pérdida de confianza por parte de los usuarios y stakeholders.
   b) Impacto Potencial: La pérdida de confianza puede afectar la reputación de la Alcaldía y la percepción pública de su capacidad para proporcionar servicios digitales seguros y confiables.

3) **Impacto en la Experiencia del Usuario:**
   a) Descripción del Riesgo: La falta de certificados de navegación segura puede generar advertencias de seguridad en los navegadores, afectando la experiencia del usuario.
   b) Impacto Potencial: Advertencias de seguridad pueden disuadir a los usuarios de acceder a la página web, afectando la visibilidad y utilidad de la plataforma digital.
4) **Cumplimiento Normativo:**
   a) Descripción del Riesgo: La falta de certificados puede resultar en incumplimiento de normativas y estándares de seguridad digital.
   b) Impacto Potencial: El incumplimiento puede generar sanciones legales y multas, además de afectar la relación con entidades reguladoras.
5) **Costos Asociados a Incidentes:**
   a) Descripción del Riesgo: Incidentes de ciberseguridad derivados de la falta de certificados pueden generar costos asociados a la gestión y resolución de incidentes.
   b) Impacto Potencial: Los costos adicionales pueden afectar el presupuesto de la entidad y comprometer recursos destinados a otras iniciativas.

R12. La posibilidad de pérdida reputacional por el incumplimiento de uno o más de los criterios de usabilidad establecidos por MinTic, debido a la falta de cumplimiento de la Política de Gobierno Digital, es un riesgo que puede afectar la percepción pública de la entidad. A continuación, se detallan los aspectos clave relacionados con este riesgo:

1) **Incumplimiento de Estándares de Usabilidad:**
   a) Descripción del Riesgo: La falta de cumplimiento de los criterios de usabilidad establecidos por MinTic puede resultar en una experiencia de usuario deficiente en los servicios digitales ofrecidos por la entidad.
   b) Impacto Potencial: Usuarios insatisfechos pueden percibir la plataforma como difícil de usar, generando frustración y afectando la reputación de la entidad.
2) **Descontento de los Usuarios:**
   a) Descripción del Riesgo: Criterios de usabilidad no cumplidos pueden llevar al descontento de los usuarios, especialmente si encuentran obstáculos al utilizar los servicios en línea.
   b) Impacto Potencial: El descontento de los usuarios puede propagarse a través de redes sociales y otras plataformas, afectando negativamente la imagen de la entidad.
3) **Impacto en la Adopción de Servicios Digitales:**
   a) Descripción del Riesgo: Una plataforma digital con baja usabilidad puede obstaculizar la adopción de servicios digitales por parte de la población, limitando el alcance y la eficacia de las iniciativas digitales.

b) Impacto Potencial: La baja adopción de servicios digitales puede afectar la percepción de la entidad como moderna y eficiente.

4) **Incumplimiento de Lineamientos Gubernamentales:**
   a) Descripción del Riesgo: El incumplimiento de criterios de usabilidad puede contravenir lineamientos gubernamentales y políticas establecidas para garantizar una experiencia positiva del usuario.
   b) Impacto Potencial: El incumplimiento de lineamientos puede generar críticas y cuestionamientos sobre la eficacia de la entidad para seguir las directrices gubernamentales.
5) **Repercusiones en la Imagen Institucional:**
   a) Descripción del Riesgo: La mala usabilidad puede ser interpretada como falta de compromiso con la calidad y la eficiencia, afectando la imagen general de la entidad.
   b) Impacto Potencial: La reputación de la entidad puede verse perjudicada, especialmente en un entorno digital donde la usabilidad es crucial.

R13. La posibilidad de pérdida económica y reputacional por la falta o escasa autorización para el tratamiento de datos personales, debido al incumplimiento de la Política de Tratamiento de Datos Personales, es un riesgo significativo que puede tener consecuencias importantes. A continuación, se detallan los aspectos claves relacionados con este riesgo:

1) **Incumplimiento Normativo:**
   a) Descripción del Riesgo: La falta de autorización adecuada para el tratamiento de datos personales puede resultar en incumplimiento de normativas y regulaciones de protección de datos.
   b) Impacto Potencial: El incumplimiento puede generar sanciones legales y multas, así como dañar la relación con las autoridades regulatorias.
2) **Violación de la Privacidad:**
   a) Descripción del Riesgo: El tratamiento no autorizado de datos personales puede violar la privacidad de los individuos afectados.
   b) Impacto Potencial: Violaciones de privacidad pueden resultar en demandas legales, pérdida de confianza y daño a la reputación de la entidad.
3) **Multas y Sanciones Financieras:**
   a) Descripción del Riesgo: La falta de autorización puede dar lugar a multas y sanciones financieras por parte de las autoridades de protección de datos.
   b) Impacto Potencial: Las multas y sanciones pueden generar pérdidas económicas significativas y afectar la estabilidad financiera de la entidad.
4) **Pérdida de Confianza del Usuario:**
   a) Descripción del Riesgo: Los usuarios afectados pueden perder la confianza en la entidad si sus datos personales se tratan sin la debida autorización.

b) Impacto Potencial: La pérdida de confianza puede afectar la reputación de la entidad y la disposición de los usuarios a proporcionar información personal en el futuro.

5) **Costos Asociados a Investigaciones y Auditorías:**
   a) Descripción del Riesgo: Incidentes de tratamiento no autorizado pueden llevar a investigaciones y auditorías, generando costos asociados a la gestión y resolución de estos eventos.
   b) Impacto Potencial: Los costos adicionales pueden afectar el presupuesto y comprometer recursos destinados a otras iniciativas.

R14. La posibilidad de pérdida económica y reputacional por el incumplimiento de uno o más de los criterios establecidos para que una entidad pública cumpla con los requerimientos de gobierno digital, debido al incumplimiento de la Política de Gobierno Digital, es un riesgo que puede afectar la eficiencia operativa y la percepción pública de la entidad. A continuación, se detallan los aspectos clave relacionados con este riesgo:

1) **Incumplimiento de Estándares de Gobierno Digital:**
   a) Descripción del Riesgo: El no cumplir con los criterios establecidos para el Gobierno Digital puede indicar deficiencias en la adopción de prácticas digitales eficientes y modernas.
   b) Impacto Potencial: El incumplimiento puede resultar en la pérdida de eficiencia operativa, afectar la calidad de los servicios digitales y generar descontento entre los usuarios.
2) **Sanciones o Multas:**
   a) Descripción del Riesgo: El incumplimiento de criterios de Gobierno Digital puede llevar a sanciones o multas por parte de entidades reguladoras o de control.
   b) Potencial: Las sanciones o multas pueden generar pérdidas económicas significativas y afectar la estabilidad financiera de la entidad.
3) **Repercusiones en la Imagen Institucional:**
   a) Descripción del Riesgo: La falta de cumplimiento en Gobierno Digital puede afectar la imagen pública de la entidad, percibiéndose como menos eficiente o moderna.
   b) Impacto Potencial: La reputación de la entidad puede verse perjudicada, especialmente en un entorno donde la adopción de tecnologías digitales es fundamental.
4) **Desconfianza de los Usuarios y Stakeholders:**
   a) Descripción del Riesgo: El incumplimiento puede generar desconfianza entre usuarios y stakeholders que esperan servicios digitales eficientes y seguros.

b) Impacto Potencial: La desconfianza puede afectar la percepción pública de la entidad y reducir la participación y colaboración por parte de los stakeholders.

5) **Pérdida de Oportunidades de Colaboración:**
   a) Descripción del Riesgo: Entidades que no cumplen con los estándares de Gobierno Digital pueden perder oportunidades de colaboración y asociación con otras entidades o actores del sector público y privado.
   b) Impacto Potencial: La pérdida de oportunidades puede limitar el alcance y la efectividad de las iniciativas de la entidad.
6) **Costos Asociados a Correcciones y Actualizaciones:**
   a) Descripción del Riesgo: Corregir y actualizar sistemas y procesos para cumplir con los criterios puede generar costos adicionales.
   b) Impacto Potencial: Los costos asociados pueden afectar el presupuesto y comprometer recursos destinados a otras iniciativas.

R15. La posibilidad de pérdida económica y reputacional por vulnerabilidades no detectadas en los sistemas informáticos, debido al escaso o nulo escaneo de vulnerabilidades de la página web, es un riesgo crítico que puede tener consecuencias graves en términos de seguridad y confianza. A continuación, se detallan los aspectos claves relacionados con este riesgo:

1) **Exposición a Amenazas Cibernéticas:**
   a) Descripción del Riesgo: La falta de escaneo de vulnerabilidades puede dejar a la página web expuesta a amenazas cibernéticas, como ataques de inyección de código, explotación de brechas de seguridad y otros ataques informáticos.
   b) Impacto Potencial: Las amenazas cibernéticas pueden comprometer la integridad, confidencialidad y disponibilidad de la información, generando pérdidas económicas y afectando la reputación.
2) **Pérdida de Datos Sensibles:**
   a) Descripción del Riesgo: Las vulnerabilidades no detectadas pueden facilitar el acceso no autorizado y la pérdida de datos sensibles almacenados en la página web.
   b) Potencial: La pérdida de datos sensibles puede tener consecuencias financieras significativas y afectar la confianza de los usuarios y stakeholders.
3) **Riesgo de Ataques Maliciosos:**
   a) Descripción del Riesgo: La presencia de vulnerabilidades no detectadas hace que la página web sea un objetivo atractivo para ataques maliciosos, como ransomware o robo de información.
   b) Impacto Potencial: Los ataques maliciosos pueden resultar en interrupciones del servicio, pérdida de ingresos y daño a la reputación.
4) **Incumplimiento Normativo:**

a) Descripción del Riesgo: La falta de escaneo de vulnerabilidades puede llevar al incumplimiento de normativas y regulaciones relacionadas con la seguridad cibernética.
b) Impacto Potencial: El incumplimiento normativo puede resultar en sanciones legales, multas y pérdida de confianza por parte de las autoridades reguladoras.

5) **Daño Reputacional:**
   a) Descripción del Riesgo: La explotación de vulnerabilidades puede dar lugar a incidentes de seguridad que afecten la reputación de la entidad.
   b) Potencial: El daño reputacional puede ser duradero y afectar la confianza de los usuarios y stakeholders en la capacidad de la entidad para proteger la información.
6) **Costos de Recuperación:**
   a) Descripción del Riesgo: La identificación y corrección de vulnerabilidades no detectadas puede generar costos significativos en términos de tiempo y recursos.
   b) Impacto Potencial: Los costos asociados a la recuperación pueden afectar el presupuesto y comprometer recursos destinados a otras iniciativas.

R16. La posibilidad de pérdida económica y reputacional por fallas en los mecanismos de autenticación, debido a la falta o escaso control de autenticación en los sistemas informáticos, es un riesgo significativo que puede tener consecuencias graves en términos de seguridad y confianza. A continuación, se detallan los aspectos clave relacionados con este riesgo:

1) **Acceso No Autorizado:**
   a) Descripción del Riesgo: La falta de control en los mecanismos de autenticación puede permitir accesos no autorizados a los sistemas informáticos.
   b) Impacto Potencial: Accesos no autorizados pueden resultar en la manipulación de datos, pérdida de confidencialidad y daño a la integridad de la información.
2) **Violación de la Privacidad:**
   a) Descripción del Riesgo: Las fallas en la autenticación pueden llevar a la violación de la privacidad al permitir a personas no autorizadas acceder a información sensible.
   b) Impacto Potencial: Violaciones de privacidad pueden generar pérdida de confianza, sanciones legales y daño a la reputación.
3) **Fraude y Suplantación de Identidad:**
   a) Descripción del Riesgo: La falta de control en la autenticación puede facilitar el fraude y la suplantación de identidad.
   b) Impacto Potencial: Actividades fraudulentas pueden generar pérdidas económicas y afectar la credibilidad de la entidad.

4) **Incumplimiento Normativo:**
   a) Descripción del Riesgo: La falta de control en los mecanismos de autenticación puede llevar al incumplimiento de normativas y regulaciones relacionadas con la seguridad de la información.
   b) Impacto Potencial: El incumplimiento normativo puede resultar en sanciones legales, multas y pérdida de confianza por parte de las autoridades reguladoras.
5) **Daño Reputacional:**
   a) Descripción del Riesgo: Incidentes relacionados con la falta de autenticación adecuada pueden dañar la reputación de la entidad.
   b) Impacto Potencial: El daño reputacional puede afectar la confianza de los usuarios y stakeholders en la capacidad de la entidad para proteger la información.
6) **Responsabilidad Legal:**
   a) Descripción del Riesgo: Fallos en los mecanismos de autenticación pueden dar lugar a responsabilidad legal por parte de la entidad.
   b) Impacto Potencial: La responsabilidad legal puede generar costos significativos y afectar la estabilidad financiera de la entidad.

R17. La posibilidad de pérdida reputacional y económica debido a sistemas de información obsoletos, sin posibilidad de actualizar, parchar o integrar, debido a que están creados en lenguajes de programación obsoletos sin compatibilidad, es un riesgo crítico que puede tener consecuencias significativas para la entidad. A continuación, se detallan los aspectos claves relacionados con este riesgo:

1) **Obsolescencia Tecnológica:**
   a) Descripción del Riesgo: La utilización de lenguajes de programación obsoletos puede llevar a la obsolescencia tecnológica de los sistemas de información.
   b) Impacto Potencial: La obsolescencia puede resultar en la incapacidad de aprovechar nuevas tecnologías, limitando la funcionalidad y eficiencia de los sistemas.
2) **Vulnerabilidades de Seguridad:**
   a) Descripción del Riesgo: La falta de actualizaciones y parches para sistemas obsoletos puede dejarlos expuestos a vulnerabilidades de seguridad.
   b) Impacto Potencial: La explotación de vulnerabilidades puede resultar en pérdida de datos, interrupciones del servicio y daño a la reputación.
3) **Limitaciones en la Integración:**
   a) Descripción del Riesgo: La falta de compatibilidad de lenguajes obsoletos puede dificultar la integración con sistemas más modernos.
   b) Impacto Potencial: Las limitaciones en la integración pueden afectar la interoperabilidad de los sistemas y la eficiencia de los procesos.

4) **Costos Elevados de Mantenimiento:**
   a) Descripción del Riesgo: El mantenimiento de sistemas obsoletos puede implicar costos elevados debido a la escasez de recursos y especialistas en lenguajes obsoletos.
   b) Impacto Potencial: Los costos elevados pueden afectar el presupuesto de la entidad y comprometer recursos destinados a otras iniciativas.
5) **Incapacidad para Cumplir con Requisitos Normativos:**
   a) Descripción del Riesgo: La obsolescencia puede dificultar el cumplimiento de requisitos normativos y estándares de seguridad.
   b) Impacto Potencial: El incumplimiento normativo puede resultar en sanciones legales, multas y pérdida de confianza por parte de las autoridades reguladoras.
6) **Percepción Negativa de los Ciudadanos:**
   a) Descripción del Riesgo: La incapacidad de ofrecer servicios eficientes y modernos puede generar una percepción negativa entre los ciudadanos.
   b) Impacto Potencial: La insatisfacción de los ciudadanos puede afectar la reputación y la relación con stakeholders.

R18. La posibilidad de pérdida económica y reputacional por equipos tecnológicos obsoletos o tecnología desactualizada, debido a que su vida útil ya se ha terminado, es un riesgo significativo que puede tener consecuencias importantes. A continuación, se detallan los aspectos clave relacionados con este riesgo:

1) **Obsolescencia Tecnológica:**
   a) Descripción del Riesgo: El uso de equipos tecnológicos con vida útil expirada puede resultar en la obsolescencia tecnológica.
   b) Impacto Potencial: La obsolescencia puede afectar la eficiencia operativa, la productividad y la capacidad de respuesta de la entidad a las demandas tecnológicas actuales.
2) **Vulnerabilidades de Seguridad:**
   a) Descripción del Riesgo: Los equipos obsoletos pueden ser más propensos a vulnerabilidades de seguridad al no recibir actualizaciones y parches de seguridad.
   b) Impacto Potencial: La explotación de vulnerabilidades puede resultar en pérdida de datos, interrupciones del servicio y daño a la reputación.
3) **Costos Elevados de Mantenimiento:**
   a) Descripción del Riesgo: El mantenimiento de equipos obsoletos puede implicar costos elevados debido a la dificultad para encontrar repuestos y personal capacitado.
   b) Impacto Potencial: Los costos elevados pueden afectar el presupuesto de la entidad y comprometer recursos destinados a otras iniciativas.

4) **Incapacidad para Cumplir con Requisitos Normativos:**
   a) Descripción del Riesgo: La presencia de tecnología desactualizada puede dificultar el cumplimiento de requisitos normativos y estándares de seguridad.
   b) Impacto Potencial: El incumplimiento normativo puede resultar en sanciones legales, multas y pérdida de confianza por parte de las autoridades reguladoras.
5) **Ineficiencias Operativas:**
   a) Descripción del Riesgo: La obsolescencia tecnológica puede generar ineficiencias en las operaciones, afectando la entrega de servicios y la satisfacción del usuario.
   b) Impacto Potencial: La baja eficiencia operativa puede tener repercusiones negativas en la percepción de la entidad por parte de usuarios y stakeholders.
6) **Percepción Negativa de la ciudadanía:**
   a) Descripción del Riesgo: La incapacidad para proporcionar servicios eficientes debido a equipos obsoletos puede generar una percepción negativa entre los usuarios.
   b) Impacto Potencial: La insatisfacción de los usuarios puede afectar la reputación y la relación con stakeholders.

La supervisión de los riesgos informáticos en la Alcaldía Mayor de Cartagena de Indias se realiza conforme a la 7a Dimensión del Modelo Integrado de Planeación y Gestión, de acuerdo con la actualización del Modelo Estándar de Control Interno (MECI). Esta supervisión implica la verificación de los controles diseñados y el seguimiento en la evaluación de la política de seguridad digital e información, todo ello bajo los lineamientos y la supervisión de la Alta Dirección. El objetivo es definir el tratamiento, manejo y seguimiento de los riesgos de seguridad digital que puedan afectar el logro de los objetivos institucionales del Distrito.

Para llevar a cabo esta tarea, la Alcaldía Mayor de Cartagena de Indias debe contar con mecanismos efectivos de evaluación de riesgos. Esto implica establecer el nivel de riesgo inherente y residual y diseñar actividades de control pertinentes en los procesos de gestión de la seguridad, así como en la adquisición, desarrollo y mantenimiento de tecnologías. El propósito final es contribuir a la mitigación de los Riesgos Informáticos, llevándolos a niveles aceptables que permitan alcanzar los objetivos institucionales. Este enfoque se alinea con las normativas y directrices establecidas por las ISSAI (Normas Internacionales de las Entidades Fiscalizadoras Superiores).

4.2 RESULTADOS EN RELACIÓN CON EL OBJETIVO ESPECÍFICO No. 1
Emitir concepto sobre la gestión fiscal, administrativa y contractual adelantada para la contratación y ejecución de los proyectos de tecnología del PETI, verificando la recepción de los bienes y servicios de conformidad con las especificaciones técnicas establecidas y la cobertura a la población beneficiaria.

Con el objeto de establecer los criterios técnicos necesarios relativos a la información objeto de análisis del universo de la contratación, se determinó una muestra estadística, que permitiera establecer a qué contratos dentro de los ejecutados para adelantar proyectos de Tecnologias de Informacion se le debia aplicar los procedimientos técnicos de control para fundamentar los resultados de la auditoria.

Con el fin de establecer los criterios técnicos necesarios relacionados con la información sujeta a análisis en el universo de contratación, se ha definido una muestra estadística. Esta selección tiene como objetivo determinar qué contratos, específicamente aquellos ejecutados para llevar a cabo proyectos de Tecnologías de la Información, deben ser sometidos a los procedimientos técnicos de control. La aplicación de estos procedimientos busca fundamentar de manera sólida los resultados obtenidos en la auditoría.

La utilización de una muestra estadística permite abordar de manera eficiente y representativa la diversidad de contratos en el ámbito de Tecnologías de la Información, asegurando que la auditoría se enfoque en aquellos contratos que tienen un impacto significativo en los proyectos y que son clave para la evaluación integral de la gestión contractual. Este enfoque metodológico contribuye a optimizar los recursos y a obtener resultados precisos y relevantes en el marco de la auditoría.

Para la vigencia auditada el total de la contratación asciende a cien (100) contratos por un valor de $2.603.967.107,90, la muestra seleccionada asciende a 39 contratos, equivalentes al 39% de los contratos suscritos y que en conjunto suman un valor de $1.718.567.108, equivalentes al 65,9% del monto total ejecutado durante la vigencia.

Se pudo establecer que el desempeño del sujeto de control en materia fiscal, administrativa y contractual, particularmente en lo concerniente a la contratación y ejecución de proyectos tecnológicos del PETI, está alineado con el objetivo específico establecido.

La evaluación abarcó una revisión detallada de los procesos vinculados a la gestión fiscal, administrativa y contractual, con énfasis en la adquisición y ejecución de proyectos tecnológicos. Además, se verificó minuciosamente la recepción de bienes y servicios, asegurando la estricta conformidad con las especificaciones técnicas predefinidas, así como la adecuada cobertura destinada a la población beneficiaria. Lo auditado demuestra el cumplimiento riguroso de la organización auditada con los parámetros establecidos para el logro eficiente de los objetivos del PETI.

4.3 RESULTADOS EN RELACIÓN CON EL OBJETIVO ESPECÍFICO No. 2
Evaluar el estado de implementación de la política de Gobierno Digital en el Distrito de Cartagena.

Gobierno Digital
Gobierno Digital, como política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, tiene como propósito fomentar el uso y aprovechamiento de las tecnologías de la información y las comunicaciones con el objetivo de consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, generando valor público en un entorno de confianza digital.

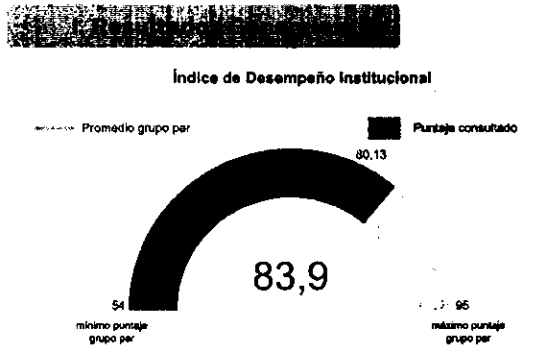
La implementación de la Política de Gobierno Digital implica que las entidades públicas deben seguir el Manual de Gobierno Digital, el cual establece los lineamientos, estándares y acciones que los sujetos obligados deben llevar a cabo. Este manual será elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones en colaboración con el Departamento Nacional de Planeación.

Con el propósito de guiar la implementación de la Política de Gobierno Digital, el Manual de Gobierno Digital ha delineado dos componentes fundamentales: TIC para el Estado y TIC para la Sociedad. Estos componentes son habilitados por tres elementos transversales clave: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales. Todos estos elementos se desarrollan mediante lineamientos y estándares que representan los requisitos mínimos que los sujetos obligados deben cumplir para lograr los objetivos establecidos por la política gubernamental.

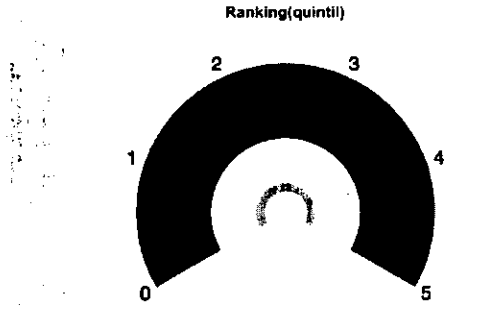
Índice de desempeño Institucional

El Índice de desempeño institucional constituye una métrica que evalúa el grado de implementación de los lineamientos establecidos en varias areas, incluida la Política de Gobierno Digital. Este índice posibilita al Ministerio de Tecnologías de la Información y las Comunicaciones realizar una evaluación que identifica tanto las buenas prácticas de implementación como las áreas susceptibles de mejora, proporcionando la base para estrategias focalizadas de acompañamiento.

Además, este índice otorga a las entidades públicas, a nivel nacional y territorial, la capacidad de tomar decisiones informadas y definir acciones específicas orientadas a mejorar su gestión y resultados en el ámbito de Gobierno Digital. En este sentido, se convierte en una herramienta clave para orientar la toma de decisiones y direccionar esfuerzos hacia la optimización de prácticas y resultados en concordancia con los principios de la Política de Gobierno Digital.
Para la vigencia 2022 el Índice de Desempeño Institucional para la Alcaldia Distrital de Cartagena de Indias obtuvo los siguientes resultados generales:



Nota 1 : El promedio del grupo par corresponde al promedio de puntajes de las entidades que hacen parte de dicho grupo. Este valor solo se visualiza cuando se filtra o consulta una sola entidad.



Nota 1: La información de este gráfico solo es válida cuando se filtra o consulta una sola entidad. No aplica para otros filtros.
Nota 2: Las entidades con puntajes más altos están ubicadas en el quintil 5; las entidades con menores puntajes están ubicadas en el quintil 1.

POLITICA	INDICE	PUNTAJE OBTENIDO	PROMEDIO GRUPO PAR
Gobierno digital	Arquitectura	75,4	69,9
	Cultura y apropiación	100,0	86,7
	Decisiones basadas en datos	46,7	62,0
	Estado abierto	90,7	92,4
	Gobernanza	83,3	72,8
	Innovacion pública Digital	80,6	70,3
	Proyectos de transformación Digital	77,8	87,1

	Seguridad y privacidad de la información	76,4	67,0
	Servicios y procesos inteligentes	64,7	37,3
Seguridad Digital	Asignación de recursos	50,0	60,9
	Despliegue de controles	95,0	80,9
	Implementacion de lineamientos de política	79,3	71,4
Transparencia, acceso a la información y lucha contra la corrupción	Indice de Transparencia y Acceso a la información pública	95,6	92,6

Considerando la información presentada y los resultados obtenidos en la vigencia inmediatamente anterior a la evaluada en esta ocasión, se destaca un avance bastante evidente por parte del la administracion distrital en un alto numero de indicadores, no osbtante se hace un llamado a definir acciones efectivas con el fin de completar las tareas pendientes en la implementación de procesos, trámites o servicios de la entidad que requieren interoperabilidad y que permitan aumentar el desempeño institucional en algunas metricas que aun muestran marcadores en miveles bajo o medio.

Luego de realizar el seguimiento y análisis de los resultados de desempeño institucional en el territorio para la vigencia 2022, los cuales están registrados en la página web del DAFP, se evidenció que la Alcaldía Mayor de Cartagena de Indias logró un 83,9%, el cual representa un avance del 15,1% con respecto a los resultados en la medicion de la vigencia inmediatamente anterior.

Estos resultados proporcionan una visión general del desempeño de la Alcaldía Mayor de Cartagena de Indias en relación con la Política de Gobierno Digital, la Política de Seguridad Digital y la Política de Transparencia, Acceso a la informacion y lucha contra la corrupcion, destacando áreas de mejora y resaltando el rendimiento alcanzado en comparación con los valores de referencia y los resultados de la medicion obtenidos en la vigencia anterior.

En línea con la información presentada, se observa una tendencia general hacia la mejora en la implementación de estas políticas mencionadas anteriormente en la entidad. En este contexto, se alienta a continuar con las estrategias que se han

venido desarrollando, y a fortalecer aquellas áreas donde aún puedan existir aspectos débiles.

Este progreso positivo indica un compromiso y esfuerzo en la adopción de prácticas de Gobierno Digital, y se destaca como un paso significativo hacia el cumplimiento total de los lineamientos establecidos. La continuidad en el fortalecimiento de las áreas identificadas como oportunidades de mejora contribuirá a consolidar los avances y a garantizar la plena implementación de la Política de Gobierno Digital en la Alcaldía Mayor de Cartagena de Indias.

Durante la revisión integral de la organización, se verificó con detalle que el estado de implementación de la política de Gobierno Digital en el Distrito de Cartagena cumple con el objetivo específico establecido.

La auditoría abordó de manera exhaustiva los procesos involucrados en la aplicación de la política de Gobierno Digital, evaluando la efectividad de su implementación en el contexto del distrito. Se identificaron y analizaron los elementos clave, destacando el compromiso de la entidad auditada con la modernización y eficiencia en la prestación de servicios públicos mediante el uso de tecnologías digitales.

Este análisis integral respalda la conclusión de que la organización ha alcanzado un estado satisfactorio en la implementación de la política de Gobierno Digital en el Distrito de Cartagena.