CORANTIOQUIA - Subdirección Administrativa y Financiera Medellín
RESOLUCIÓN
CORPORACIÓN AUTÓNOMA REGIONAL DEL
Fecha: 27-dic-2024 10:16 AM Pág: 4
Anexos: 282 PÁGINAS
Archivar en:
Radicado por: Claudia María Gómez Londoño

040-RES2412-5920
Favor citar este número al responder

Por la cual se adopta el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC 2024-2027, el Plan de Seguridad y Privacidad de la Información 2024-2027 y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027 de la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA-

La directora general de la Corporación Autónoma Regional del Centro de Antioquia, en uso de sus facultades legales y estatutarias y en especial las que le confieren el artículo 29 de la Ley 99 de 1993 y el Decreto 1768 de 1994 y,

CONSIDERANDO

Que la Ley 1341 de 2009 estableció el marco general del sector de las Tecnologías de la Información y las Comunicaciones, incorporando principios, conceptos y competencias sobre su organización y desarrollo e igualmente señaló que las Tecnologías de la Información y las Comunicaciones deben servir al interés general y, por tanto, es deber del Estado promover su acceso eficiente y en igualdad de oportunidades a todos los habitantes del territorio nacional.

Que el Decreto 1083 de 2015, adicionado por el Decreto 415 de 2016, establece la definición de los lineamientos para el fortalecimiento institucional en materia de TICs, cuyo ámbito de aplicación, de acuerdo con el artículo 2.2.35.2., corresponde a las entidades del Estado de orden nacional y territorial, los organismos autónomos y de control.

Que el artículo 2.2.35.3. del Decreto 1083 de 2015, adicionado por el Decreto número 415 de 2016, establece como objetivos del fortalecimiento institucional:

> *"3. Desarrollar los lineamientos en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que habiliten la gestión de la entidad y/o sector en beneficio de la prestación efectiva de sus servicios y que a su vez faciliten la gobernabilidad y gestión de las Tecnologías de la Información y las Comunicaciones TIC. Así mismo, velar por el cumplimiento y actualización de las políticas y estándares en esta materia"*
>
> *...11. Desarrollar estrategias de gestión de información para garantizar la pertinencia, calidad, oportunidad, seguridad e*

Carrera 65 n.° 44A - 32. Tel: 604 493 88 88 - Ext. 1200
www.corantioquia.gov.co - Municipio: Medellín , Antioquia
Correo electrónico: administrativa@corantioquia.gov.co

Código Dependencia-

intercambio con el fin de lograr un flujo eficiente de información disponible para el uso en la gestión y la toma de decisiones en la entidad y/o sector".

Que la Ley 2294 de 2022, por el cual se expide el plan nacional de desarrollo 2022- 2026 "Colombia potencia mundial de la vida", en su artículo 143. TRANSFORMACIÓN DIGITAL COMO MOTOR DE OPORTUNIDADES E IGUALDAD, establece la importancia de "Promover la consolidación de una sociedad digital para que todos los ciudadanos tengan las herramientas necesarias para hacer del Internet y de las tecnologías digitales un instrumento de transformación social".

Que el Decreto 1499 de 2017 determina el cumplimiento institucional de las Políticas de Gobierno y Seguridad Digital en relación con el habilitador "Seguridad de la Información" conforme a la Resolución 500 de 2021 (MinTIC) y la Política de Seguridad Digital acorde con los lineamientos de los documentos CONPES 3701 de 2011 Lineamiento de Políticas de Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad Digital, CONPES 3975 de 2019 Política Nacional para la Transformación Digital e Inteligencia Digital, CONPES 3995 de 2020 Política Nacional de Confianza y Seguridad Digital.

Que el Decreto 1008 de 2018, 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. Dentro de la política se detalla el Habilitador de Arquitectura, el cual contiene todas las temáticas y productos que deberán desarrollar las entidades en el marco del fortalecimiento de las capacidades internas de gestión de las tecnologías, así mismo el Marco de Referencia de Arquitectura Empresarial V 3.0 es uno de los pilares de este habilitador.

Que así mismo, una de las metas que pretende alcanzar el Programa Visión Colombia 2019 impulsado por el Departamento Nacional de Planeación DNP, es el cumplimiento del objetivo "Un Estado al Servicio de los Ciudadanos", el desarrollo de la estrategia "Avanzar hacia una Sociedad Informada", la cual dispone que: "En 2019 la información deberá ser un derecho efectivo y un instrumento de difusión y apropiación del conocimiento, que promueva el desarrollo económico, la equidad social y la democracia. En ese contexto, Colombia deberá alcanzar estándares adecuados de generación de información confiable y oportuna, y de uso colectivo. El Estado promoverá su diseminación, aprovechando el uso de las tecnologías de la información y las comunicaciones", cumpliendo con los estándares de gobierno, con su nueva Política de Gobierno Digital, basada en los siguientes aspectos: TIC para lograr un Estado más eficiente, TIC para prestar mejores servicios y como herramienta para innovar en el Estado, y el nuevo enfoque hacia un Gobierno Digital.

Carrera 65 n.° **44**A - 32. Tel: 60**4** 493 88 88 - Ext. **1**200
www.corantioquia.gov.co - Municipio: Medellín , Antioquia
Correo electrónico: administrativa@corantioquia.gov.co

Código Dependencia-

Que el Plan de Gestión Ambiental Regional 2020 – 2031 "Un Plan Intergeneracional", contempla en su modelo de gestión y operación para la administración de los recursos naturales, la implementación de tecnologías que optimicen las capacidades técnicas y jurídicas de respuesta, la atención integral, la racionalización y atención oportuna de las etapas de evaluación, control y seguimiento de los trámites integrados.

Que el Plan de Acción Cuatrienal 2024-2027 «Conectados por la Vida», contempla la implementación de las Tecnologías de la Información y las Comunicaciones (TIC) y establece estrategias y acciones específicas para fortalecer las capacidades tecnológicas de la entidad y mejorar la eficiencia y efectividad en la gestión ambiental en su jurisdicción.

Que la Resolución 040-RES2010-5756, Por la cual se adopta la Política General de Tecnología, de Seguridad y Privacidad de la Información en la Corporación Autónoma Regional del Centro de Antioquia - Corantioquia, se constituyen en un instrumento de planificación que orientan la ruta de acción en materia de seguridad y privacidad de la Información corporativa.

Que el 23 de diciembre de 2024, se presentaron en el Comité Institucional de Gestión y Desempeño, el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC 2024-2027, el Plan de Seguridad y Privacidad de la Información 2024-2027 y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027.

Que, por las consideraciones antes expuestas, la directora general de la Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA- en mérito de lo expuesto,

RESUELVE

Artículo 1º. **Objeto**: Adoptar el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC 2024-2027, el Plan de Seguridad y Privacidad de la Información 2024-2027 y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027, los cuales se encuentran establecidos en los anexos que hacen parte integral del presente acto administrativo.

Artículo 2º. **Implementación**: La Corporación Autónoma Regional del Centro de Antioquia -CORANTIOQUIA- deberá implementar el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC 2024-2027, el Plan de Seguridad y Privacidad de la Información 2024-2027 y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027, adoptadas a través del presente acto administrativo, conforme a sus responsabilidades y competencias, para lo cual se dará a conocer a los servidores públicos, contratistas, usuarios, a través de comunicados, en los

Carrera 65 n.° **44**A - 32. Tel: 60**4** 493 88 88 - Ext. **1**200
www.corantioquia.gov.co - Municipio: Medellín , Antioquia
Correo electrónico: administrativa@corantioquia.gov.co

Código Dependencia-

procesos de inducción y reinducción y de las diferentes plataformas tecnológicas de comunicación.

Artículo 3º. **Seguimiento y Revisión**: La Subdirección Administrativa y Financiera, Grupo Interno de Trabajo Tecnologías de la Información y las Comunicaciones o la dependencia que sea delegada por la Dirección General para liderar los procesos tecnológicos de la Corporación, será responsable de hacer seguimiento anual o antes si existiesen modificaciones que así lo requieran, a la implementación del Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC 2024-2027, el Plan de Seguridad y Privacidad de la Información 2024-2027 y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027, con el propósito de que se mantengan actualizados, sean oportunos, suficientes y eficaces.

Artículo 4º. **Vigencia y derogatoria**: La presente Resolución rige a partir de la fecha de su expedición y deroga cualquier otra disposición que le sea contraria.

Artículo 5°. Publicación. La presente Resolución será publicada en el Boletín Oficial de la Corporación Autónoma Regional del Centro de Antioquia Corantioquia, página web www.corantioquia.gov.co.

Dado en el Distrito de Ciencia, Tecnología e Innovación de Medellín, el 26 de diciembre de 2024.

PUBLÍQUESE Y CUMPLASE

LILIANA MARIA TABORDA GONZALEZ

Directora General

Expediente N/A

Tiempo: 1 (hora)

Asignación: N/A

CORANTIOQUIA - Subdirección Administrativa y Financiera Medellín
RESOLUCIÓN
CORPORACIÓN AUTÓNOMA REGIONAL DEL
Fecha: 27-dic-2024 10:16 AM Pág: 4
Anexos: 282 PÁGINAS
Archivar en:
Radicado por: Claudia María Gómez Londoño

040-RES2412-5920
Favor citar este número al responder

Anexo: Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC 2024-2027 (160 páginas)
Plan de Seguridad y Privacidad de la Información 2024-2027 (35 páginas)
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027 (33 páginas)

Elaboró: Janeth Cristina Aguirre Montoya Ambrosio Caicedo Celis

Revisó: Edgar Alexander Osorio Londoño

Bertha Janeth Osorio Giraldo

Fecha de elaboración: 2024-12-23

Carrera 65 n.° **44**A - 32. Tel: 60**4** 493 88 88 - Ext. **1**200
www.corantioquia.gov.co - Municipio: Medellín , Antioquia
Correo electrónico: administrativa@corantioquia.gov.co

Liliana María Taborda González
Directora general
Corporación Autónoma Regional del Centro de Antioquia

2024-12-26

Aprobado y adoptado mediante Resolución n.° xxx

Tabla de contenido

CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

Presentación

El Plan Nacional de Desarrollo 2022 – 2026: Colombia, potencia mundial de la vida, en su artículo 143. Transformación digital como motor de oportunidades e igualdad, establece la importancia de "Promover la consolidación de una sociedad digital para que todos los ciudadanos tengan las herramientas necesarias para hacer del Internet y de las tecnologías digitales un instrumento de transformación social".

El Decreto 1008 de 2018, 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.

El Grupo Interno de Trabajo TIC que lidera los procesos tecnológicos de la Corporación, a través de la definición de su Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) 2024 - 2027, tendrá la oportunidad de transformar digitalmente los servicios que brinda a sus grupos de interés, adoptar los lineamientos de la Gestión de TI del Estado Colombiano, desarrollar su rol estratégico al interior de la Entidad, apoyar las áreas misionales mientras se piensa en tecnología, liderar las iniciativas de TI que deriven en soluciones reales y tener la capacidad de transformar su gestión, como parte de los beneficios que un Plan Estratégico de TIC debe producir una vez se inicie su ejecución.

El PETIC 2024-2027 está alineado con la estrategia Nacional, Territorial e Institucional, y contempla el análisis de la situación actual, la arquitectura actual de gestión y gobierno de TI, la arquitectura destino de gestión y gobierno de TI, y Marco Normativo. Por último, se establecen las iniciativas estratégicas de TI, el portafolio de proyectos y su hoja de ruta a corto, mediano y largo plazo.

La estructuración y la puesta en ejecución del PETIC 2024-2027 cuenta con importantes beneficios estratégicos y tácticos para la Entidad:

- Coadyuvar con el cumplimiento de los retos y metas establecidas en los planes estratégicos y de gestión de la Entidad.
- Fortalecer las capacidades de la dependencia que lidera los procesos tecnológicos de la Corporación, para apoyar la estrategia y modelo operativo de la Entidad.
- Identificar herramientas que ayuden a contar con información oportuna para la toma de decisiones y permitan el desarrollo y mejoramiento de la Entidad.
- Adquirir e implementar buenas prácticas de gestión de TI.
- Adoptar tecnologías disruptivas para apoyar la gestión institucional.
- Mejorar la seguridad de la información corporativa.

El PETIC 2024-2027 busca entonces recopilar el sentir de la entidad, Identificar las necesidades y oportunidades en todas las dependencias de la Corporación, que puedan ser solucionadas y aprovechadas por medio de la implementación tecnológica, para

proponer un camino de crecimiento alineado con el cumplimiento de los objetivos estratégicos de la Entidad.

Es así como el PETIC 2024-2027 se encuentra alineado con lo definido en el Modelo de Gestión y Gobierno de TI – MGGTI del Marco de Referencia de Arquitectura Empresarial del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y funge como uno de los instrumentos o productos definidos para generar las capacidades institucionales de TI que se requieren para mejorar la prestación de los servicios de TI a los usuarios internos y externos mediante el uso adecuado de las tecnologías de la información y las comunicaciones en la *Corporación Autónoma Regional del Centro de Antioquia - CORANTIOQUIA,* en el marco del cumplimiento de la Política de Gobierno Digital.

Este instrumento de planificación tecnológico está alineado al Plan de Acción Cuatrienal 2024-2027 “Conectados por la Vida”. De igual forma, de ser necesario anualmente y durante su vigencia se actualizará su estructura programática.

1 Elementos estratégicos corporativos

1.1 Misión

Contribuir al logro del desarrollo sostenible, mediante el conocimiento y mejoramiento de la oferta ambiental y la administración del uso de los recursos para responder a su demanda, a través de la construcción de una cultura ambiental del territorio (Consejo Directivo, 2016)

1.2 Visión ambiental para el desarrollo regional

En 2031 los 80 municipios del centro de Antioquia forman un territorio sostenible en el que se protege el patrimonio ambiental biodiverso, se desarrollan actividades económicas en armonía con la madre tierra y sus actores regionales son corresponsables en la conservación de la diversidad biológica, étnica y cultural, y el respeto a la dignidad humana, para el buen vivir de las generaciones presentes y futuras. (Acuerdo Consejo Directivo 575, 2019)

1.3 Política de administración del riesgo

La Corporación Autónoma Regional del Centro de Antioquia - Corantioquia, es una organización de alto desempeño en la administración de los recursos naturales renovables, que tiene como misión contribuir al logro del desarrollo sostenible, comprometida con la satisfacción de las necesidades de la comunidad; asimismo, buscará la eficacia de las acciones formuladas a través del cumplimiento de los requisitos legales, los sistemas de gestión corporativos, transparencia en el acceso de los servicios, manejo adecuado de la información y el fortalecimiento de la cultura organizacional, mediante las relaciones establecidas entre las partes interesadas, con el fin de monitorear y controlar los posibles riesgos (Registro F-PPO-20 Mapa Riesgos y Oportunidades).

1.4 Código de integridad

Mediante Resolución (Resolución n.° 040-RES2112-9588, 2021) se adoptó el Código de Integridad Corporativo como guía, sello e ideal de cómo deben ser y obrar los servidores públicos y todos aquellos colaboradores de la administración que prestan sus servicios en la corporación, con el fin de cumplir con la misión, la visión y los objetivos institucionales dentro del marco de integridad y legalidad.

El Código de Integridad Corporativo reúne los valores de honestidad, respeto, compromiso, diligencia, justicia, servicio y resultados.

a) **Honestidad.** Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia, rectitud y siempre favoreciendo el interés general. (Función Pública, 2019)

b) **Respeto.** Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición. (Función Pública, 2019)
c) **Compromiso.** Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar. (Función Pública, 2019)
d) **Diligencia.** Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos del Estado. (Función Pública, 2019)
e) **Justicia.** Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación. (Función Pública, 2019)
f) **Servicio.** Sirvo y atiendo las necesidades de los ciudadanos, poniendo a disposición mis capacidades y anteponiendo los máximos fines del Estado a cualquier propósito o interés particular.
g) **Resultados.** Tengo claridad frente al rol que desempeño, el empoderamiento individual respecto a los objetivos y la generación de resultados.

El Código de Integridad proporciona el marco ético y de valores que guía la implementación del PETIC 2024 – 2027.

La relación entre el Código de Integridad y el PETIC 2024 – 2027 es fundamental para asegurar que las acciones y decisiones tecnológicas de la Corporación se alineen con principios éticos, de transparencia y de manera responsable.

1.5 Política del SGI

Corantioquia es una entidad pública, encargada de administrar el patrimonio ambiental de los 80 municipios de su jurisdicción, enfocada al cumplimiento de los requisitos legales y reglamentarios; la generación de valor público y la satisfacción de los actores del territorio; el mejoramiento continuo del SGI y sus procesos; a la participación de los actores del territorio; el fortalecimiento de la cultura organizacional y ambiental; la prevención de la contaminación y la protección del ambiente; la gestión de los riesgos y oportunidades organizacionales y el bienestar de los servidores públicos, contratistas, subcontratistas, visitantes, participantes en eventos corporativos y actores viales; contribuyendo así al desarrollo sostenible. (Resolución 040-RES2408-3589).

2 Articulación con instrumentos de planificación

2.1 Articulación con el PGAR 2020-2031

El PETIC está alineado al Plan de Gestión Ambiental Regional 2020-2031 a través del Capítulo 5 “Línea estratégicas del PGAR“, Línea 4 “Fortalecimiento de la cultura ambiental y de las capacidades de los actores para la gestión conjunta y el logro de los resultados”, Objetivo 4 “Generar la gobernanza que permita consolidar el escenario de sostenibilidad ambiental de la jurisdicción” , Componente 13 “Institucionalidad fortalecida para una gestión ambiental corresponsable , Componente 15 “ la gestión de la información y el conocimiento investigación + Desarrollo + Innovación” , Componente 18 ”Incidencia institucional para una eficiente coordinación y cooperación con las autoridades étnicas en materia de gestión ambiental” , Retos : 30, 35, 36, 37 y 49.

Figura 1 Articulación del PETIC con los retos y Componentes 13, 15 y 18 del PGAR 2020 – 2031

Fuente Elaboración Propia

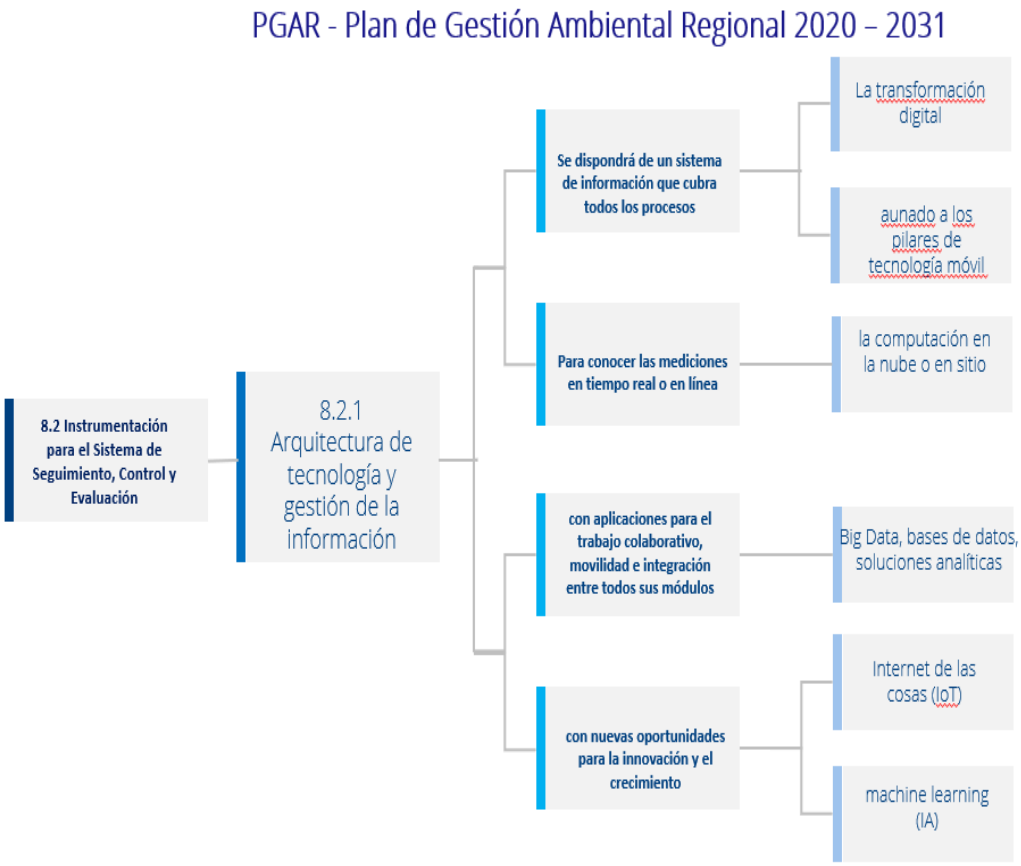


Figura 2 Articulación del PETIC con las tecnologías relacionadas en el instrumento de Planificación PGAR 2020 – 2031.

Fuente Elaboración Propia a Partir del PGAR 2020 – 2031

2.2 Articulación con el Plan de Acción 2024-2027

El PETIC está alineado al Plan de acción 2024-2027 a través del programa 5 “Conexión Institucional “dentro el cual se encuentra el proyecto 5.3 denominado “Gestión de la Información para la toma de decisiones en la gestión ambiental”, dentro de los cuales se encuentra 3 actividades que son:

- **Actividad 5.3.1**. Diseño del Centro de Monitoreo para la administración integral del territorio con énfasis en el recurso agua. (*Indicador: Centro de monitoreo diseñado*).

- **Actividad 5.3.2.** Implementación del Centro de Monitoreo para la administración integral del territorio con énfasis en el recurso agua.

*(**Indicador:** Porcentaje de Avance en el levantamiento de los requerimientos, diagnóstico e implementación integral de las plataformas institucionales.*
***Indicador:** Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027.*
***Indicador:** Porcentaje de avance de la formulación e implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información*
***Indicador:** Porcentaje de avance de la formulación e implementación del Plan de Seguridad y Privacidad de la Información.*
***Indicador:** Porcentaje de avance en el diagnóstico integral e implementación de soluciones a las necesidades interoperabilidad*
***Indicador:** Porcentaje de avance de las actividades priorizadas anualmente para la implementación del Centro de Monitoreo).*

- **Actividad 5.3.3.** Articulación del centro de monitoreo con otras entidades del Sistema Nacional Ambiental – SINA En el marco de Sistema de información para Colombia – SIAC. (*Indicador: % de avance de las actividades priorizadas anualmente para la interoperabilidad del Centro de Monitoreo)*.

2.3 Articulación con otros instrumentos de planificación

La Corporación dispone de diferentes Instrumentos de Planificación (Estratégica, Temática o Misional, Institucional o de Gestión y Desempeño), los cuales incorporan diferentes estrategias para el logro de su propósito articuladas con asuntos de las TIC, que requieren en primer lugar ser identificadas y en segundo lugar articuladas con el PETIC:

1. **Planes Temáticos o Misionales:** Corresponden a los planes que se desarrollan en el marco de la sostenibilidad del territorio de la Jurisdicción, los cuales disponen de normativa específica para su formulación, seguimiento y actualización:

    - + Aire Puro.
    - Plan de Ordenación Forestal.
    - Plan Regional de Cambio Climático.
    - Plan de Manejo de Acuíferos.
    - Plan de Manejo de Áreas Protegidas.
    - Planes de Manejo de Microcuencas.
    - Planes de Ordenación y Manejo de Cuencas Hidrográficas.
    - Planes de Ordenamiento del Recurso Hídrico.
    - Plan de Negocio Asociativo en Turismo de Naturaleza.
    - Plan de Conservación y Manejo de Especies Priorizadas de Flora.
    - Plan de Conservación y Manejo de Especies Priorizadas de Fauna.

La articulación entre los planes misionales, los Planes de Gestión y Desempeño y el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) es esencial para asegurar que las iniciativas transformación digital y modernización tecnológica apoyen directamente los objetivos fundamentales de la Corporación que impactarán la gestión corporativa.

2. **Planes de Gestión y Desempeño:** Corresponden a los Planes Institucionales y Estratégicos que establece el Decreto 612 de 2018, los cuales se deben actualizar anualmente a más tardar el 31 de enero de cada vigencia e integrar al Plan de Acción de la Corporación, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión (MIPG):

    - Plan Institucional de Archivos de la Entidad -PINAR.
    - Plan Anual de Adquisiciones.
    - Plan Anual de Vacantes.
    - Plan de Previsión de Recursos Humanos.
    - Plan Estratégico de Talento Humano.
    - Plan Institucional de Capacitación.
    - Plan de Incentivos Institucionales.
    - Plan de Trabajo Anual en Seguridad y Salud en el Trabajo.
    - El Programa de Transparencia y Ética Pública.
    - Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI.
    - Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
    - Plan de Seguridad y Privacidad de la Información.

3 Objetivos

3.1 Objetivo general

Trazar la ruta de transformación digital de la Corporación Autónoma Regional de Centro de Antioquia durante el periodo 2024 – 2027, con el uso de tecnologías, a fin de contribuir al cumplimiento de los objetivos estratégicos de la entidad y generar valor. Incluye la visión, los principios, los indicadores, el mapa de ruta, el plan de comunicación, el plan de proyectos y la descripción de todos los demás aspectos (financieros, operativos, de manejo de riesgos) necesarios para la puesta en marcha y gestión del plan estratégico a través de las iniciativas y proyectos de tecnología e información, basados en el Marco de Referencia de Arquitectura Empresarial del Estado Colombiano MRAE v3.0

3.2 Objetivos específicos

La materialización del Objetivo general del PETIC se desarrolla a través del cumplimiento de los siguientes objetivos específicos:

1. Apoyar la transformación digital de la Corporación mediante la definición y ejecución de iniciativas y proyectos de tecnología e información, alineados con los objetivos y metas de los instrumentos de planificación corporativos, entre estos, el Plan de Acción 2024-2027, que en el Programa 5. Conexión Institucional, se encuentra el Proyecto 5.3. Gestión de la Información para la toma de decisiones en la gestión ambiental, donde se incluye el diseño e implementación del Centro de Monitoreo para la administración integral del territorio con énfasis en el recurso agua, de tal manera que apalanquen y ayuden a la entidad a alcanzar las metas de su estrategia en el corto, mediano y largo Plazo.
2. Definir un plan de implementación consistente, realizable y medible en tiempo, recursos y presupuesto, donde se definió para cada iniciativa indicadores de cumplimiento y periodos de medición que permitan alcanzar las metas trazadas.
3. Fortalecer las capacidades de la dependencia que lidera los procesos tecnológicos de la Corporación estableciendo un modelo de gestión estructurado.

4 Glosario

4.1 Siglas

ODS. Objetivos de Desarrollo Sostenible.

PGAR. Plan de Gestión Ambiental Regional.

SGI. Sistema de gestión integral.

4.2 Definiciones

Actividades. Son el conjunto de procesos bajo el control del responsable de la intervención pública, que transforma insumos en productos. (DNP, 2014)

Efectividad. Es el grado en el que los resultados deseados se alcanzan a través de los productos». (DNP, 2014)

Eficacia. Es el grado de cumplimiento de las metas y objetivos a nivel de productos y resultados. (DNP, 2014)

Eficiencia. Hace referencia al uso óptimo de recursos en una actividad productiva. Es la máxima cantidad de un producto específico que un nivel dado de costo en insumos puede generar, o alternativamente, es el mínimo costo en insumos que se requiere para generar una cantidad dada de un producto específico. Es decir, la eficiencia compara la productividad observada con una productividad esperada. (DNP, 2014)

Estrategias. Conjunto de directrices coordinadas que ayudan a elegir las acciones adecuadas para alcanzar los objetivos de la planeación estratégica (PGAR y Plan de Acción), orientados a la consecución de resultados. Permiten la definición de condiciones de interés, planes de acción, mecanismos de coordinación, responsables, metas, etc. y orientan el proceso de priorización en la asignación de recursos. (DNP, 2014)

Evaluación. Es la apreciación, lo más sistemática y objetiva posible, de un proyecto, programa o política en curso o concluido, de su diseño, su puesta en práctica y sus resultados. El objetivo es determinar la pertinencia y el logro de los objetivos, así como la eficiencia, la eficacia, el impacto y la sostenibilidad para el desarrollo. (SINA, 2018)

Impacto. Son los efectos exclusivamente atribuibles a la intervención pública. La evaluación del impacto trata de identificar todos estos efectos y centrarse en la determinación de los efectos netos atribuibles a la intervención». (DNP, 2014)

Indicador de producto. Mide los bienes y servicios provistos por la corporación que se obtienen de la transformación de los insumos a través de las actividades». Adaptado del (DNP, 2014)

I**ndicador de resultado.** Mide los efectos derivados de la intervención pública, una vez se han consumido los bienes y servicios proveídos por ésta. (DNP, 2014)

Indicador. Variable o factor cuantitativo o cualitativo que proporciona un medio sencillo y fiable para medir logros, reflejar los cambios vinculados con una intervención o ayudar a evaluar los resultados de un organismo de desarrollo. (DNP, 2014)

Modelo causal. Establecimiento de las relaciones entre los productos estratégicos que se deben entregar y los resultados estratégicos que se esperan alcanzar. (DNP, 2014)

Productos. Son los bienes y servicios generados por la intervención pública, que se obtienen mediante los procesos de transformación de los insumos. (DNP, 2014)

Programas. Intervención pública que materializa los objetivos planteados en la planeación a través de la entrega coordinada de productos y la generación de resultados estratégicos a escala territorial con la participación de diferentes actores. Cuenta con una estructura de seguimiento basada en la disposición y el uso de información de desempeño para retroalimentar las decisiones y orientar las decisiones gerenciales. Adaptado de (DNP, 2014)

Proyecto de inversión. Proceso único, temporal y no divisible que, a través de una tecnología específica, y utilizando como insumos factores productivos, bienes o servicios, genera productos que buscan dar solución a una problemática particular enmarcada en los lineamientos de los programas establecidos. De (Arregocés, Jola, & Velásquez, 2011ª, referenciado en (DNP, 2014).

Resultados. «son los efectos intencionales o no de la intervención pública, una vez se han consumido los productos. (DNP, 2014)

Seguimiento. Es el proceso continuo que debe llevarse a cabo con una periodicidad regular, y que debe centrarse en la evaluación del cumplimiento de los diversos aspectos de la ejecución como por ejemplo la evaluación de los indicadores. Al tratarse de un proceso sistemático y periódico, permite que se recopile y se analice información con el objeto de comparar los avances logrados en función de los planes formulados. Ayuda además a identificar tendencias y patrones, a adaptar las estrategias y a fundamentar las decisiones relativas a la gestión del proyecto o programa. Un seguimiento continuo garantiza que cualquier irregularidad se detecte y corrija a tiempo. Para que resulte verdaderamente eficaz, debe realizarse de forma abierta con una amplia participación de los interesados. (SINA, 2018)

Seguimiento del desempeño (Performance monitoring). Proceso continuo de recolección y análisis de datos para comparar en qué medida se está ejecutando un proyecto, programa o política en función de los resultados previstos. (DNP, 2014)

Seguimiento-monitoreo. Función continua que utiliza una recopilación sistemática de datos sobre indicadores especificados para proporcionar a los administradores, y a las principales partes interesadas de una intervención para el desarrollo, indicaciones sobre el avance y logro de los objetivos, así como de la utilización de los fondos asignados. (DNP, 2014)

5 Roles y responsabilidades

Frente al PETIC se tienen identificados los siguientes roles y responsabilidades que permitan su implementación:

Tabla 1 Roles y Responsabilidades

PROCESO	ROLES Y/O RESPONSABILIDADES			
	Grupo Interno de Trabajo	**Profesional Especializado**	**Profesional Universitario**	**Técnico Operativo**
Gestión administrativa, de alineamiento, organización & planeación de ti	TIC	X		
Gestión ciclo de vida de los sistemas de información	GIC TIC		X	X
Gestión de la infraestructura de ti	TIC	X	X	X
Administrar los datos	TIC	X	X	
Gestión de licenciamientos y suscripciones	TIC		X	X
Gestión operativa de los servicios de ti	TIC	X	X	X
Administración de la seguridad y privacidad de la información	TIC	X	X	X

.

6 Contexto del plan

6.1 Diagnóstico

6.1.1 Servicios de TI

A continuación, se describen los Servicios de TI con los que actualmente cuenta la Corporación para la prestación de sus servicios internos y externos.

Tabla 2 Servicio de Acceso a Internet por Wifi

ID	001
Nombre	Acceso a internet por WIFI
Descripción	Acceso a la red de CORAN (Servicios Internos), CORANFREE (Visitantes) y COLABORADORES (Contratistas) de la Entidad de manera inalámbrica a través de dispositivos móviles y computadores portátiles. La velocidad de bajada se encuentra abierta para ser utilizada por toda la red de la Corporación, para un total del canal de navegación de 100 MB dedicado.
Categoría	Conectividad
Usuario objetivo	Servidores Públicos, Contratistas y Visitantes
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 96% (Contrato Datacenter)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1

Tabla 3 Servicio de Acceso a la Intranet

ID	002
Nombre	Acceso a la intranet
Descripción	Acceso a la red protegida de la Entidad CORANET para el acceso a la información de interés Corporativa.
Categoría	Conectividad
Usuario objetivo	Servidores Públicos y Contratistas
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	No se cuenta
Hallazgos u oportunidades de mejora	Definir ANS

Tabla 4 Servicio de Acceso a la Red Interna por VPN

ID	003
Nombre	Acceso a la red interna por VPN
Descripción	Acceso a la red interna Corporativa desde el exterior de la Entidad.
Categoría	Conectividad
Usuario objetivo	Servidores Públicos y Contratistas
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico

ID	003
	• Verbal
Acuerdo de nivel de servicio	No se cuenta
Hallazgos u oportunidades de mejora	Definir ANS

Tabla 5 Servicio de Correo Electrónico y Herramientas Colaborativas

ID	004
Nombre	Correo electrónico junto con las herramientas colaborativas
Descripción	Basado en Microsoft MS365 E3 con un buzón de almacenamiento de 100 GB y un espacio de almacenamiento en la nube a través de OneDrive de 2 TB y acceso desde el cliente Microsoft Outlook o a través del navegador web (OWA).
Categoría	Comunicación
Usuario objetivo	Servidores Públicos y Contratistas
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 99% (Contrato Microsoft)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1
Nro. del Contrato actual	190-OC2402-124782

Tabla 6 Servicio de Entrenamiento y Capacitación

ID	005
Nombre	Servicio de entrenamiento y capacitación uso de las soluciones de TI
Descripción	Servicio que suministra capacitación y entrenamiento sobre las funciones de los sistemas de información que maneja la Entidad a través de los Proveedores de Servicios, del Plan Institucional de Capacitación y de la Estrategia del Miércoles del Conocimiento.
Categoría	Uso y Apropiación de TI
Usuario objetivo	Servidores Públicos y Contratistas
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	No se cuenta
Hallazgos u oportunidades de mejora	Definir ANS y articulación con el Plan Institucional de Capacitación

Tabla 7 Servicio de Telefonía IP

ID	006
Nombre	Telefonía IP
Descripción	Servicio de comunicaciones telefónicas entre usuarios internos y externos de la institución.
Categoría	Comunicación
Usuario objetivo	Servidores Públicos y Contratistas

Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter), ANS Nivel 3: 5*8 (Fabricante)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1
Nro. del Contrato actual	190-CNT2312-183

Tabla 8 Servicio de Plataforma Mesa de Servicio

ID	**007**
Nombre	Plataforma de mesa de servicio
Descripción	Plataforma para registro, consulta y respuesta de requerimientos e incidentes tecnológicos.
Categoría	Sistemas de Información
Usuario objetivo	Servidores Públicos, Contratistas y Usuarios
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	Actualmente la Entidad no cuenta con Mesa de Servicio
Hallazgos u oportunidades de mejora	Lograr contar con una Mesa de Servicio de Soporte Nivel 1

Tabla 9 Servicio Gestión de Red Interna Colaboradores

ID	008
Nombre	Gestión de red interna
Descripción	Gestión de la administración y configuración centralizada de la seguridad de la red institucional (internet e intranet).
Categoría	Comunicación
Usuario objetivo	Entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1

Tabla 10 Servicio Gestión de Red de Infraestructura Tecnológica

ID	009
Nombre	Gestión de red de infraestructura tecnológica
Descripción	Gestión de la administración y configuración centralizada de la seguridad de la red que usan los Sistemas de Información.
Categoría	Comunicación
Usuario objetivo	Entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio

ID	009
	• Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1
Nro. del Contrato actual	040-COV2406-8

Tabla 11 Servicio de Antivirus

ID	010
Nombre	Antimalware
Descripción	Software que detecta y elimina malware y otras amenazas informáticas en la red, sistemas de información, PC, dispositivos móviles y demás.
Categoría	Seguridad
Usuario objetivo	Entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter), ANS Nivel 3: 7*24 (Fabricante)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1
Nro. del Contrato actual	190-CNT2111-152

Tabla 12 Servicio Gestión Equipos de Cómputo

ID	011
Nombre	Gestión de equipos de cómputo
Descripción	Adquisición, instalación, configuración y mantenimientos preventivos y correctivos de hardware y software de los equipos asignados a los Servidores Públicos y Contratitas de la Entidad.
Categoría	Gestión de Infraestructura de TI
Usuario objetivo	Servidores Públicos y Contratistas
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	No se cuenta
Hallazgos u oportunidades de mejora	Definir ANS
Nro. del Contrato actual	190-CNT2210-145

Tabla 13 Servicio Instalación de Software en Equipos de Cómputo

ID	012
Nombre	Instalación de software en equipos de cómputo
Descripción	Instalación de software por demanda en los equipos de cómputo de los Servidores Públicos o Contratitas.
Categoría	Servicios Tecnológicos
Usuario objetivo	Servidores Públicos y Contratistas

ID	012
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	No se cuenta
Hallazgos u oportunidades de mejora	Definir ANS
Nro. del Contrato actual	190-CNT2210-145

Tabla 14 Servicio de Videoconferencias

ID	013
Nombre	Videoconferencias
Descripción	Acceso de servicio de video llamada a través de herramienta Teams.
Categoría	Servicios Tecnológicos
Usuario objetivo	Servidores Públicos y Contratistas
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 99% (Contrato Microsoft)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1

Tabla 15 Servicio Página Web Institucional

ID	014
Nombre	Página web institucional
Descripción	Sitio web institucional disponible a los ciudadanos que integra información sobre servicios institucionales, trámites, noticias, eventos de interés, políticas y normatividad.
Categoría	Comunicación
Usuario objetivo	Ciudadanos
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1

Tabla 16 Servicio Soporte de Aplicaciones

ID	016
Nombre	Soporte aplicaciones
Descripción	Gestión de requerimientos e incidentes y/o problemas presentados en las aplicaciones.
Categoría	Sistemas de Información
Usuario objetivo	Servidores Públicos y Contratistas
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico

ID	016
	• Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter), ANS Nivel 3: 5*8 (Proveedor de la Solución)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1
Nro. del Contrato actual	190-CNT2402-18 – Soporte Sistema Financiero SAFIX 190-CNT2407-135 - Soporte Sirena / e-Sirena

Tabla 17 Servicio Configuración de Ambientes de Desarrollo, Pruebas, Capacitación, Preproducción

ID	017
Nombre	Configuración de ambientes de desarrollo, pruebas, capacitación y preproducción
Descripción	Preparación y configuración de ambientes para desarrollos, procesos de aseguramiento de calidad y capacitaciones en los diferentes sistemas de información
Categoría	Sistemas de Información
Usuario objetivo	Servidores Públicos y Contratistas
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter), ANS Nivel 3: 5*8 (Proveedor de la Solución)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1

ID	017
Nro. del Contrato actual	040-COV2406-8

Tabla 18 Servicio Despliegue de Software en Producción

ID	018
Nombre	Despliegue de software en producción
Descripción	Preparación, configuración y despliegue de las soluciones generadas por el área de TI.
Categoría	Sistemas de Información
Usuario objetivo	Usuarios de los sistemas de información
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter), ANS Nivel 3: 5*8 (Proveedor de la Solución)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1
Nro. del Contrato actual	040-COV2406-8

Tabla 19 Servicio Gestión de Infraestructura de TI

ID	019
Nombre	Gestión de infraestructura de TI
Descripción	Administración y monitoreo de servidores, servidores de aplicaciones, servidores web, sistemas de información, herramientas de software, soluciones en la nube y demás elementos de infraestructura de TI.
Categoría	Gestión de Infraestructura de TI
Usuario objetivo	Área de TI
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter), ANS Nivel 3: 5*8 (Fabricante)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1
Nro. del Contrato actual	040-COV2406-8

Tabla 20 Servicio Adquisición de Licencias de Software

ID	020
Nombre	Adquisición de licencias de software
Descripción	Servicio de adquisición de licencias de software requeridas para usar en los diferentes procesos de la organización.
Categoría	Servicios Tecnológicos
Usuario objetivo	Área de TI
Horario de prestación del servicio	8 horas, 5 días a la semana

ID	020
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	3 meses antes a la adquisición o vencimiento
Hallazgos u oportunidades de mejora	No aplica
Nro. del Contrato actual	190-OC2402-124782 – Licenciamiento Microsoft 190-AO2402-1 - Certificado SSL (Secure Socket Layer) 090-OC2402-124287 - Licenciamiento ArcGIS 190-OC2311-119289 - Licenciamiento Oracle 190-AO2404-3 - Licenciamiento Veeam.

Tabla 21 Servicio Mantenimiento de Aplicaciones

ID	021
Nombre	Mantenimiento de aplicaciones
Descripción	Servicio que se encarga de realizar cambios en los sistemas de información para: • Corregir errores recurrentes • Actualizar software base • Aumentar la capacidad funcional de la aplicación
Categoría	Sistemas de Información
Usuario objetivo	Usuarios de los sistemas de información
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal

ID	021
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter), ANS Nivel 3: 5*8 (Proveedor de la Solución)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1
Nro. del Contrato actual	190-CNT2402-18 – Soporte Sistema Financiero SAFIX 190-CNT2407-135 - Soporte Sirena / e-Sirena

Tabla 19 Servicio Administración de Bases de Datos

ID	022
Nombre	Administración de bases de datos
Descripción	Servicio que se encarga de la administración de las bases de datos que maneja la entidad.
Categoría	Sistemas de Información
Usuario objetivo	Área de TI
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter), ANS Nivel 3: 5*8 (Proveedor de la Solución)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1
Nro. del Contrato actual	040-COV2406-8

Tabla 20 Servicio Gestión de Backup

ID	023
Nombre	Gestión de backup
Descripción	Servicio que se encarga de generar respaldo de datos de los sistemas de información
Categoría	Gestión de Infraestructura de TI
Usuario objetivo	Área de TI
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	ANS Nivel 1: No se cuenta, ANS Nivel 2: 98% (Contrato Datacenter), ANS Nivel 3: 5*8 (Proveedor de la Solución)
Hallazgos u oportunidades de mejora	Definir ANS Nivel 1
Nro. del Contrato actual	040-COV2406-8

Tabla 21 Servicio Pruebas de Vulnerabilidad

ID	024
Nombre	Pruebas de vulnerabilidades
Descripción	Servicio que se encarga de realizar pruebas de vulnerabilidades a la arquitectura de TI.
Categoría	Seguridad
Usuario objetivo	Área de TI
Horario de prestación del servicio	No aplica

ID	024
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	No se realizan pruebas de vulnerabilidades
Hallazgos u oportunidades de mejora	Realizar de pruebas de vulnerabilidades

Tabla 22 Servicio Versionamiento de Fuentes de Desarrollo

ID	025
Nombre	Versionamiento de fuentes de desarrollo a nivel interno
Descripción	Servicio que se encarga de generar versionamiento del código de software generado en las distintas actividades de desarrollo de software.
Categoría	Sistemas de Información
Usuario objetivo	Área de TI
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	Por definir
Hallazgos u oportunidades de mejora	No se cuenta con área de desarrollo

Tabla 23 Servicio Gestión Proyectos de TI

ID	026
Nombre	Gestión de proyectos de TI
Descripción	Servicio que permite planear, ejecutar y realizar seguimiento a proyectos que afectan los procesos o elementos de la arquitectura de TI.
Categoría	Estrategia de TI
Usuario objetivo	Todas las áreas de la entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	En la gestión de cada proyecto se definen los ANS a aplicar
Hallazgos u oportunidades de mejora	

Tabla 24 Servicio Gestión de Identidades

ID	027
Nombre	Gestión de identidades
Descripción	Permite asignar permisos a los servicios tecnológicos y aplicaciones a los Servidores Públicos y Contratistas de la Entidad, así mismo, provee los mecanismos de autenticación y autorización para el acceso a estos recursos.
Categoría	Seguridad
Usuario objetivo	Todas las áreas de la entidad

ID	027
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	No se cuenta
Hallazgos u oportunidades de mejora	Definir ANS

Tabla 25 Servicio DNS

ID	028
Nombre	DNS
Descripción	Servicio que permite asignar nombre de dominio a los diferentes elementos que hacen parte de la red.
Categoría	Infraestructura de TI
Usuario objetivo	Todas las áreas de la entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	8 horas hábiles
Hallazgos u oportunidades de mejora	98%

Tabla 26 Servicio Virtualización de Servidores

ID	029
Nombre	Servicio de Virtualización de servidores
Descripción	Servicio que permite virtualizar servidores físicos en varias máquinas virtuales, las cuales pueden proveer a su vez servicios de hosting a las diferentes soluciones de software.
Categoría	Infraestructura de TI
Usuario objetivo	Todas las áreas de la entidad
Horario de prestación del servicio	24 horas, 7 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	98%
Hallazgos u oportunidades de mejora	
Nro. del Contrato actual	040-COV2406-8

Tabla 27 Servicio Aseguramiento de la Calidad del Software

ID	030
Nombre	Aseguramiento de la calidad del software
Descripción	Servicio que permite asegurar la calidad de las soluciones de software.
Categoría	Sistemas de Información

ID	030
Usuario objetivo	Área de TI
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	De acuerdo con estimación
Hallazgos u oportunidades de mejora	

Tabla 28 Servicio de Supervisión de Proveedores de TI

ID	031
Nombre	Servicio de supervisión de proveedores de TI
Descripción	Servicio que permite asegurar que los proveedores cumplan con las obligaciones contractuales.
Categoría	Infraestructura de TI
Usuario objetivo	Área de TI
Horario de prestación del servicio	8 horas, 5 días a la semana
Canal de soporte	• Correo electrónico • Software de mesa de servicio • Canal telefónico • Verbal
Acuerdo de nivel de servicio	En la gestión de cada contrato se definen los ANS a aplicar

ID	031
Hallazgos u oportunidades de mejora	

6.1.2 *Capacidades de TI*

A continuación, se relacionan las Capacidades de TI que hacen parte de la gestión de las Tecnologías de la Información de la Entidad.

Tabla 29 Capacidades de TI

Categoría	Capacidad	Cuenta con la Capacidad en la Entidad
Estrategia	Gestionar arquitectura empresarial	NO
	Gestionar Proyectos de TI	SÍ
	Definir políticas de TI	SÍ
Gobierno	Gestionar Procesos de TI	NO
Información	Administrar modelos de datos	NO
	Gestionar flujos de información	NO
Sistemas de Información	Definir arquitectura de Sistemas de Información	NO
	Administrar Sistemas de Información	SÍ
	Interoperar	NO
Infraestructura	Gestionar disponibilidad	SÍ
	Realizar soporte a usuarios	SÍ
	Gestionar cambios	NO
	Administrar infraestructura tecnológica	SÍ
Uso y apropiación	Apropiar TI	SÍ
Seguridad	Gestionar seguridad de la información	NO

6.1.3 Gobierno de TI

Las Tecnologías de la Información y las Comunicaciones en la Entidad requieren disponer de un modelo administrativo de Gobierno y Gestión de las TIC que dé el direccionamiento y supervisión ejecutiva y además garantice el alineamiento, la planeación, organización, entrega de servicios de TI de manera oportuna, continua y segura

6.1.4 Modelo de Gobierno de TI

La Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA, mediante Acuerdo del Consejo Directivo número 180-ACU2209-642 del 29 septiembre de 2022 modificó su estructura administrativa y se definieron las funciones de cada dependencia, quedando de la siguiente manera:

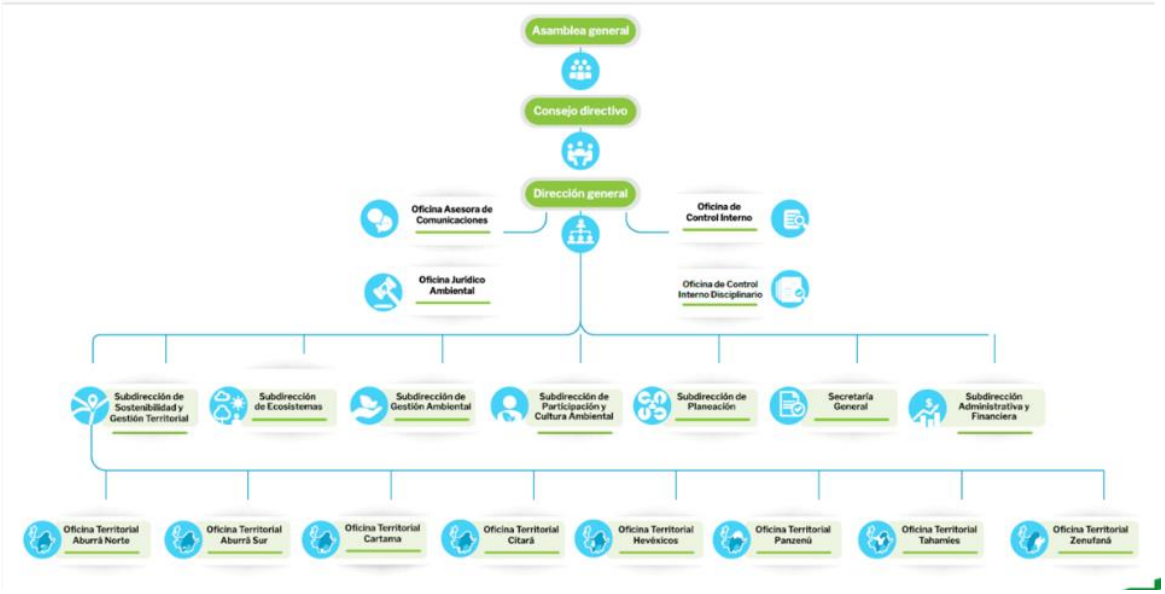


Figura 3 Organigrama Institucional

Fuente Elaboración Propia

6.1.4.1 Mapa Procesos Corporativo

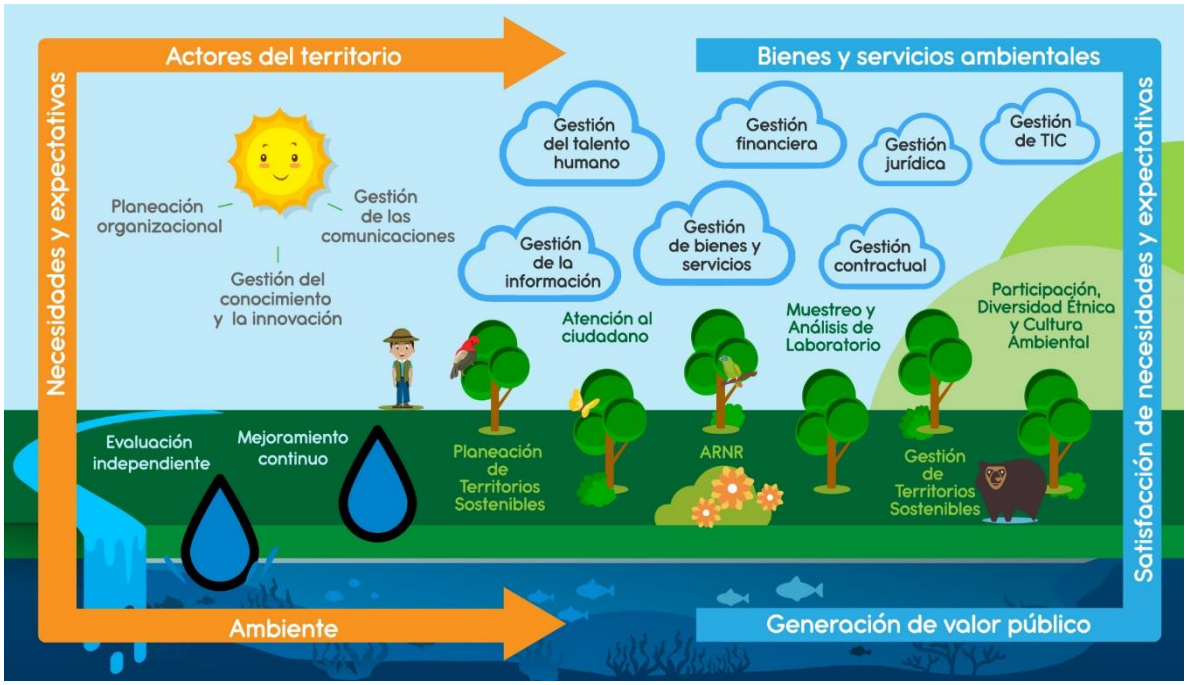


Figura 4 Mapa de Procesos Corporativo

Fuente: Elaboración Propia

Cada uno de estos procesos dispone de su respectiva caracterización (objetivo, alcance, responsable, entradas, salidas, actividades, partes interesadas, indicadores, riesgos, aspectos e impactos ambientales, riesgos y peligros en SST). En este mapa, se identifica el Proceso de Gestión de TIC, el cual se encarga de gestionar los servicios de TIC para garantizar la confiabilidad, integridad y disponibilidad de la información y contribuir a la continuidad de los procesos corporativos.

El Gobierno de TI en la Corporación, está conformado por el Grupo Interno de Trabajo Tecnologías de la Información y las Comunicaciones adscrito a la Subdirección Administrativa y Financiera y el Grupo Interno de Trabajo Gestión de la Información y el Conocimiento adscrito a la Subdirección de Planeación.

Grupo Interno de Trabajo Tecnologías de la Información y las Comunicaciones (GIT TIC): Mediante la Resolución 040-RES1708-4392 del 22 de agosto de 2017 se creó el Grupo Interno de Trabajo Tecnologías de la Información y las Comunicaciones adscrito a la Subdirección Administrativa de la Corporación, el cual está conformado por los siguientes empleos: Un (1) Profesional Especializado, Código 2028, Grado 19; Dos (2) Profesionales Universitarios, Código 2044, Grado 9; y Tres (3) Técnicos Operativos, Código 3132, Grado 16.

Grupo Interno de Trabajo Gestión de la Información y el Conocimiento (GIT GIC): Mediante la Resolución 040-RES1803-1083 del 07 de marzo de 2018 se creó el Grupo Interno de Trabajo Gestión de la Información y el Conocimiento adscrito a la Subdirección de Planeación de la Corporación, el cual está conformado por los siguientes empleos: Un (1) Profesional Especializado, Código 2028, Grado 17; Dos (2) Profesionales Especializados, Código 2028, Grado 15; Dos (2) Profesionales Universitarios, Código 2044, Grado 11; Tres (3) Profesionales Universitarios, Código 2044, Grado 09; Un (1) Técnico Administrativo, Código 3124, Grado 18, y Un (1) Técnico Operativos, Código 3132, Grado 16.

Los principios para consolidar la función de TI según las buenas prácticas internacionales se muestran en el siguiente diagrama y toma como referencia las buenas prácticas de ITIL, COBIT y COSO.

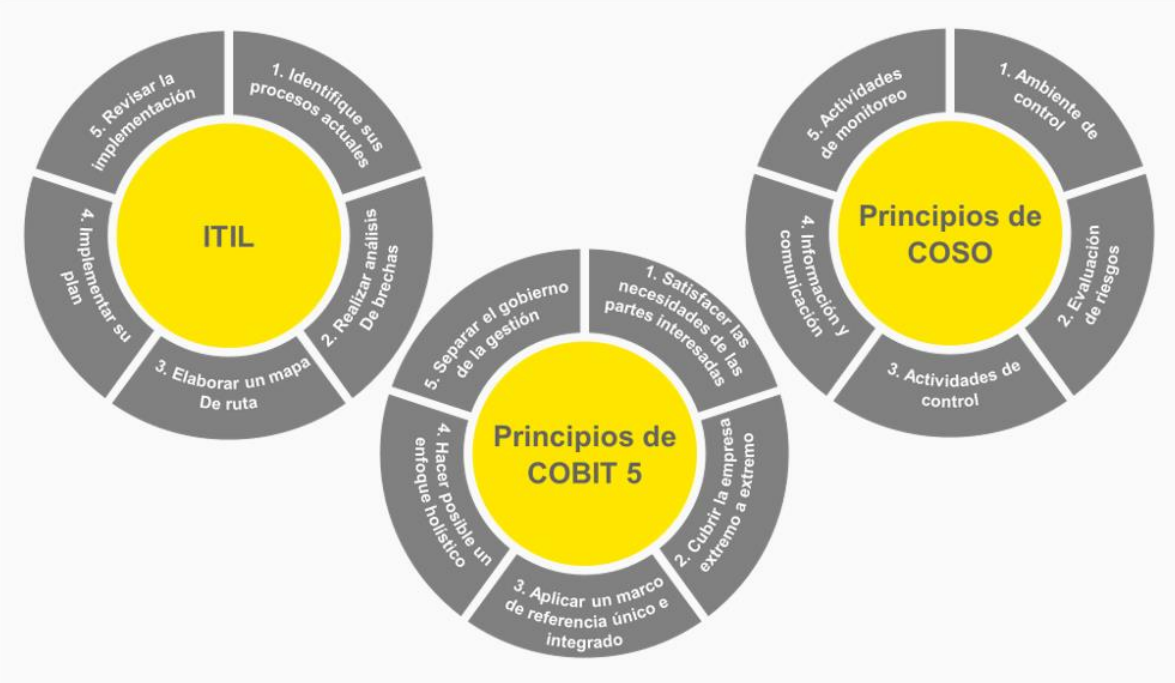


Figura 5 Metodologías Ágiles

Fuente: Documentación Contrato 190-CNT1909-110

En el análisis realizado, se contrastó la Estructura Organizacional que soporta las funciones de TI en la Corporación, dando como resultado lo que se muestra en la Figura 7 Análisis Gobierno de TI.

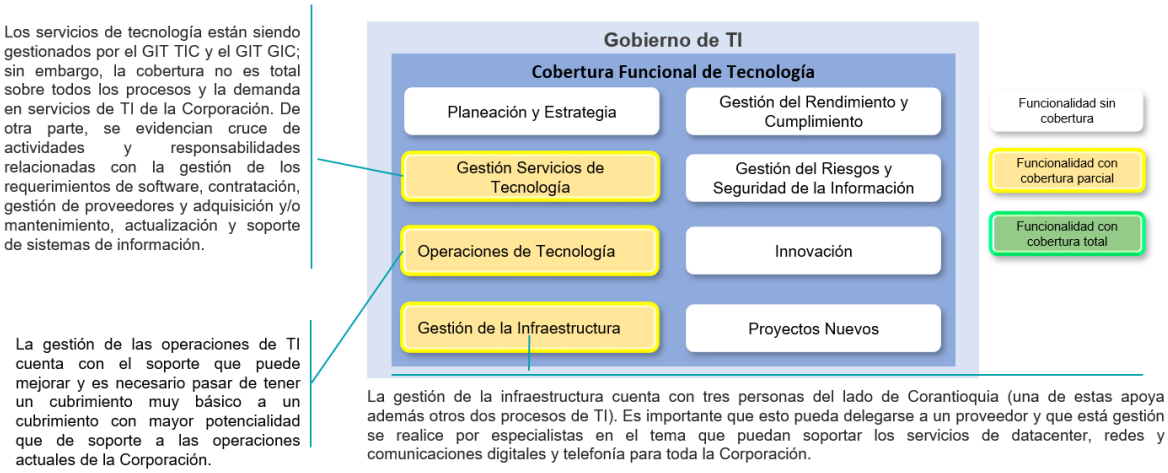


Figura 6 Análisis Gobierno de TI

Fuente: Documentación Contrato 190-CNT1909-110

6.1.5 Modelo de Gestión de TI

A continuación, se relacionan las actividades del Modelo de Gestión de TI.

Gestión administrativa, de alineamiento, organización & planeación de ti

- Planeación estratégica de TI.
- Gestión presupuestal de TI.
- Gestión relacionamiento con actores clave de la Entidad.
- Estructuración de proyectos y contrataciones:
    - Gestión contractual recursos y servicios de TI.
    - Supervisión de contratos de TI.
- Administración personal de TIC (Servidores Públicos).
- Gestión de uso y apropiación de la tecnología.
- Administración instalaciones físicas personal TI.

Gestión ciclo de vida de los sistemas de información

- Ingeniería de requerimientos de soluciones.
- Desarrollar y mantener arquitectura de soluciones de TI.
- Diseño detallado de soluciones (software).
- Administrar integraciones, interfaces, Apis y esquemas de interoperabilidad.

- Desarrollo de software.
- Pruebas de aceptación.
- Gestión de defectos.
- Entrenamiento de partes interesadas.
- Administración de la configuración.
- Administración de ambientes (desarrollo, producción).

Gestión de la infraestructura de TI

- Desarrollar y mantener arquitectura de infraestructura.
- Instalar y configurar equipos de la infraestructura.
- Mantener actualizados componentes de software servidores.
- Monitorear el desempeño de la infraestructura.
- Administrar incidentes en equipos de la infraestructura.
- Administración de la infraestructura tecnológica de TI.

Administrar los datos

- Administración de las bases de datos.
- Administrar bodegas y lagos de datos.
- Administrar repositorios de contenido (Plataforma Moodle y Sharepoint).
- Administrar publicaciones de contenido en portales.
- Administrar los respaldos (backups).

Gestión de licenciamientos y suscripciones

- Administrar licenciamientos de productos y usuarios.
- Gestión de novedades de licenciamiento y suscripción.
- Contratación en la adquisición y renovación de los servicios de licenciamiento.

Gestión operativa de los servicios de TI

- Gestión de acuerdos de niveles de servicio.
- Administrar configuración herramienta de mesa de servicios.
- Gestión de incidentes.
- Gestión de solución de problemas (causa raíz).
- Gestión de cambios a componentes del servicio.
- Gestión de versiones y administración configuración.
- Gestión de la capacidad y el desempeño de los servicios.
- Gestión de almacenamiento y respaldo de información.

Administración de la seguridad y privacidad de la información

- Gestión de políticas de seguridad de la información.
- Gestión y desarrollo de la cultura de seguridad de la información.
- Gestión de cuentas usuarios, permisos, perfiles.
- Gestión de incidentes de seguridad.

- Administrar configuración equipos de seguridad informática (UTM y Antimalware).

6.1.6 *Estructura y Organización Humana de TI*

A continuación, se describe la estructura organizacional de TI de la Entidad, la cual está alineada con los procesos, procedimientos y actividades que soportan la Gestión de las Tecnologías de la Entidad, según la Resolución 040-RES1708-4392 del 22 de agosto de 2017.

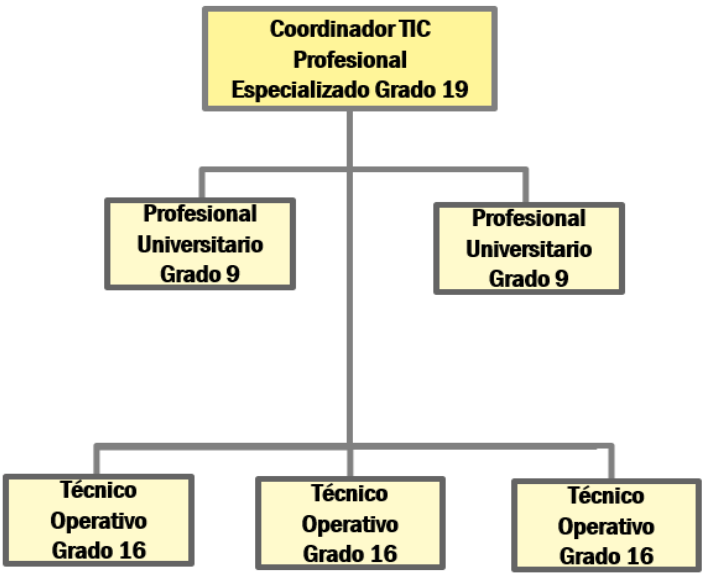


Figura 7 Estructura y Organización Humana de TI

6.1.7 *Gestión de Proyectos*

El Modelo de Gestión de Proyectos, guía la planificación, ejecución, monitoreo y cierre de proyectos de tecnología de la información. Este modelo se enfoca en asegurar que los proyectos de TI se gestionen de manera eficiente, cumpliendo con los objetivos estratégicos de la organización y optimizando el uso de recursos. No solo se enfoca en la entrega de proyectos dentro del tiempo y presupuesto, sino también en la alineación con los objetivos estratégicos de la Corporación, la gestión de la calidad y la satisfacción de los interesados.

6.1.8 *Gestión de Información*

La Gestión de Información de TI incluye la supervisión y administración de los sistemas de información y sistemas informáticos de la Corporación, incluyendo hardware, software y redes. Su objetivo principal es asegurar que estos sistemas funcionen de manera eficiente y segura, apoyando las operaciones y objetivos estratégicos de la entidad.

6.1.9 *Arquitectura de Información*

La Arquitectura de Información de TI es fundamental para asegurar que los sistemas de información de la Corporación estén bien estructurados, sean eficientes y puedan adaptarse a las necesidades cambiantes de la entidad.

Tabla 30 Matriz de Entidades vs Componentes de TI

	Sirena y e-Sirena	Safix	Pgar	Facturación y Cartera	Laboratorio	SGI - Megateso	Base de Datos TUA y TR	Base de Datos Fauna y Flora	Bases de Datos Ambientales (Piragua, Sembratón)	Tableros de Control	Portal Web	Visor Geográfico
Usuario	X							X	X		X	X
Comunidad	X										X	X
Servidores Públicos y Contratistas	X	X	X	X	X	X	X	X	X	X	X	X
Entes de Control	X	X	X	X	X	X	X	X	X	X	X	X
Entes Territoriales	X								X		X	X
Entidades del Estado											X	X
Proveedores de Servicios	X							X	X		X	X

	Sirena y e-Sirena	Safix	Pgar	Facturación y Cartera	Laboratorio	SGI - Megateso	Base de Datos TUA y TR	Base de Datos Fauna y Flora	Bases de Datos Ambientales (Piragua, Sembratón)	Tableros de Control	Portal Web	Visor Geográfico
Agencias de Cooperación	X								X		X	X
Asamblea Corporativa	X								X		X	X
Consejo Directivo	X								X		X	X
Despachos Judiciales	X										X	X
Empresas de Servicios Públicos Domiciliarios	X										X	X
Bomberos											X	X
Centros de Mantenimiento Vehicular									X			
Ente Acreditador											X	X
Ente Certificador											X	X
Gestores de Residuos Peligrosos	X										X	
Medios de Comunicación											X	
Organizaciones Socioambientales e											X	X

	Sirena y e-Sirena	Safix	Pgar	Facturación y Cartera	Laboratorio	SGI - Megateso	Base de Datos TUA y TR	Base de Datos Fauna y Flora	Bases de Datos Ambientales (Piragua, Sembratón)	Tableros de Control	Portal Web	Visor Geográfico
Instancias de Gestión Ambiental												
Sectores Económicos[1]	X										X	X
Vecinos y Empresas Colindantes											X	
Veedurías Ciudadanas	X										X	X

6.1.10 Catálogo de los Sistemas de Información

El catálogo de Sistemas de Información Corresponde al inventario de los sistemas relacionando por cada uno un conjunto de datos funcionales, técnicos y de gestión. Esto permite la identificación rápida de aspectos claves de los Sistemas conllevando a tomar decisiones ágiles sobre la arquitectura de sistemas de información.

La Arquitectura de Información de TI es fundamental para asegurar que los sistemas de información de la Corporación estén bien estructurados, sean eficientes y puedan adaptarse a las necesidades cambiantes de la entidad.

Tabla 31 Sistema SECOP II

Nombre aplicación	**SECOP II**
Descripción Funcional	Plataforma transaccional para gestionar en línea todos los Procesos de Contratación, con cuentas para entidades y proveedores; y vista pública para cualquier tercero interesado en hacer seguimiento a la contratación pública.

[1] Sector Industrial, Comercial, Agrícola, entre otros.

Nombre aplicación	SECOP II
Información que gestiona	Contratos Documentos de soporte Procesos pre-contractuales Proponentes Oferentes Licitaciones Subastas
Tipo de software	Software como servicio
Estado	Productivo
Esquema de licenciamiento	Libre para entidades públicas
Fabricante	Agencia Nacional de Contratación Pública – Colombia Compa Eficiente
Integraciones con otros sistemas	No aplica
Debilidades o hallazgos estructurales	Ninguna

Tabla 32 Sistema SIGEP

Nombre aplicación	SIGEP II
Descripción Funcional	El SIGEP es un Sistema de Información y Gestión del Empleo Público al servicio de la administración pública y de los ciudadanos. Contiene información de carácter institucional tanto nacional como territorial, relacionada con: tipo de entidad, sector al que pertenece, conformación, planta de personal, empleos que posee, manual de funciones, salarios, prestaciones, etc.; información con la cual se identifican las instituciones del Estado Colombiano.
Información que gestiona	Información de funcionarios Manual de funciones Entidades del Estado Hojas de vida

Nombre aplicación	**SIGEP II**
	Declaración de bienes y rentas Plan institucional de capacitación Evaluación de desempeño
Tipo de software	Software como Servicio
Estado	Productivo
Esquema de licenciamiento	Software libre para entidades públicas
Integraciones con otros sistemas	Ninguna
Debilidades o hallazgos estructurales	

Tabla 33 M365 E3

Nombre aplicación	**M365 E3**
Descripción Funcional	M365 E3 es una plataforma de productividad, comunicación y colaboración, alojada en la nube, que agrupa las herramientas como: Correo Electrónico, Word, Excel, PowerPoint, entre otras más. Además, es una solución que ofrece a los usuarios la capacidad de trabajar en cualquier momento y desde cualquier lugar, comunicarse por videoconferencia con cualquier persona, compartir su trabajo en tiempo real y con total seguridad, utilizar el correo electrónico, el calendario y la información de los contactos desde prácticamente todo tipo de dispositivos, disponer de una red de colaboración manejando niveles de seguridad y privacidad.
Información que gestiona	Correo electrónico Documentos Herramientas colaborativas
Tipo de software	Software como servicio
Estado	Productivo
Esquema de licenciamiento	Microsoft – Enterprise Agreement

Nombre aplicación	**M365 E3**
Integraciones con otros sistemas	- Megateso.
Debilidades o hallazgos estructurales	Migrar a la versión de M365 con el fin contar con los módulos de seguridad avanzada y buenas prácticas para el producto.

Tabla 34 Página Web

Nombre aplicación	**Portal Web CORANTIOQUIA**
Descripción Funcional	Sitio web institucional disponible a los ciudadanos que integra información sobre servicios institucionales, trámites, noticias, eventos de interés, políticas y normatividad.
Información que gestiona	Licencias ambientales Normatividad Noticias Servicios institucionales Trámites Información organizacional Información de transparencia y acceso a la información pública
Tipo de software	Software como servicio
Estado	Productivo
Esquema de licenciamiento	Microsoft – Enterprise Agreement
Integraciones con otros sistemas	- e-Sirena. - Pagos en línea. - SUIT. - Redes sociales. - Correo electrónico. - Megateso. - Coranet. - Entidades del Orden Nacional.

Debilidades o hallazgos estructurales	Indicar las debilidades y hallazgos estructurales - Actualmente se está realizando análisis de requerimientos para mejorar el diseño y fortalecer el portal web institucional.

Tabla 35 Sistema Administrativo y Financiero

Nombre aplicación	**Sistema Administrativo y Financiero SAFIX**
Descripción Funcional	Sistema administrativo y financiero que permite realizar el seguimiento a las diversas áreas de la compañía como presupuesto, tesorería, contabilidad, almacén, talento humano, nómina, entre otros.
Información que gestiona	Presupuesto Contabilidad Tesorería Almacén Nómina Viáticos
Tipo de software	Comercial
Estado	Productivo
Esquema de licenciamiento	Suscripción anual de licenciamiento
Integraciones con otros sistemas	- Sirena y e-Sirena - Facturación y Cartera - Pgar
Debilidades o hallazgos estructurales	Migrar la aplicación a su versión web.

Tabla 36 Sistema Misional Sirena - e-Sirena

Nombre aplicación	**Sirena – e-Sirena**
Descripción Funcional	Sistema misional que permite administrar la información jurídica y técnica relacionada con el trámite realizado a un Permiso, Concesión o Licencia Ambiental con facilidad de acceso y manipulación a la misma en cuanto a consultas, búsquedas o reportes que se requieran.

Nombre aplicación	Sirena – e-Sirena
Información que gestiona	Trámites ambientales Expedientes ambientales TUA y TR Pagos en línea
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	La aplicación es propiedad de la Corporación
Integraciones con otros sistemas	- Facturación y Cartera - Pgar - Safix - Portal web (Página web institucional)
Debilidades o hallazgos estructurales	Migrar la aplicación a su versión web y mejorar la experiencia de usuario (generación de reportes, tableros de control) y la interoperabilidad con otros sistemas de información del Orden Nacional.

Tabla 37 Sistema PGAR

Nombre aplicación	PGAR
Descripción Funcional	Sistema de apoyo a la gestión que permite hacer seguimiento a la Contratación y Plan de Adquisiciones.
Información que gestiona	Contratación Seguimiento a proyectos
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	Suscripción anual de licenciamiento
Integraciones con otros sistemas	- Sirena y e-Sirena. - Facturación y Cartera - Safix

Nombre aplicación	PGAR
Debilidades o hallazgos estructurales	Migrar la aplicación a su versión web y mejorar la experiencia de usuario (generación de reportes, tableros de control), la interoperabilidad con otros sistemas de información del Orden Nacional y la gestión actual de proyectos.

Tabla 38 Sistema Facturación y Cartera

Nombre aplicación	Facturación y Cartera
Descripción Funcional	Sistema de apoyo para el control de la facturación y cartera, cobros coactivos y convenios de pago.
Información que gestiona	Facturación física y electrónica Cobro coactivo Acuerdos de pago
Tipo de software	Comercial
Estado	Productivo
Esquema de licenciamiento	Suscripción anual de licenciamiento
Integraciones con otros sistemas	- Sirena y e-Sirena - Safix - Aplicación para Facturación Electrónica
Debilidades o hallazgos estructurales	Migrar la aplicación a su versión web y mejorar la experiencia de usuario (generación de reportes, tableros de control), la interoperabilidad con otros sistemas de información del Orden Nacional, la gestión actual de facturación y cartera permitiendo su automatización.

Tabla 39 Sistema de Laboratorio Ambiental

Nombre aplicación	Laboratorio Ambiental
Descripción Funcional	Sistema de apoyo que permite administrar la información de los servicios prestados por el Laboratorio Ambiental de la Corporación.
Información que gestiona	Cotizaciones Facturación de servicios Recepción de muestras Entrega de resultados

Nombre aplicación	Laboratorio Ambiental
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	Desarrollo a la medida
Integraciones con otros sistemas	- Facturación y Cartera
Debilidades o hallazgos estructurales	Migrar la aplicación a su versión web y mejorar la experiencia de usuario (generación de reportes, tableros de control) y la interoperabilidad con otros sistemas de información del Orden Nacional.

Tabla 40 Sistema de Información Geográfica

Nombre aplicación	Sistema de Información Geográfica (SIG)
Descripción Funcional	Visor cartográfico en línea que contiene funcionalidades básicas de navegación y consulta sobre los mapas, así como funciones avanzadas de superposición de capas, edición, consulta de direcciones, entre otros.
Información que gestiona	Documentación cartográfica.
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	Desarrollo a la medida
Integraciones con otros sistemas	- Visor Geográfico. - Sirena.
Debilidades o hallazgos estructurales	Migrar la aplicación a su versión web y mejorar la experiencia de usuario (generación de reportes, tableros de control) y la interoperabilidad con otros sistemas de información del Orden Nacional.

Tabla 41 Visor Geográfico

Nombre aplicación	Visor Geográfico
Descripción Funcional	Visor cartográfico en línea que contiene funcionalidades básicas de navegación y consulta sobre los mapas, así como

	funciones avanzadas de superposición de capas, edición, consulta de direcciones, entre otros.
Información que gestiona	Visor geográfico de la cartografía temática de la Corporación
Tipo de software	Comercial
Estado	Productivo
Esquema de licenciamiento	Suscripción anual de licenciamiento
Integraciones con otros sistemas	- Sirena y e-Sirena - Base de Datos Espacial GISCA
Debilidades o hallazgos estructurales	Dependencia absoluta con el Proveedor para el soporte, mantenimiento y actualización.

Tabla 42 Sistema de Gestión Documental

Nombre aplicación	**Sistema de Gestión Documental (Sirena, e-Sirena)**
Descripción Funcional	Sistema donde se alojan la documentación en general (interna y externa), trámites y licencias ambientales, gestión contractual, así como los expedientes y documentos relacionados con los procesos de la Entidad.
Información que gestiona	Expedientes Todos los documentos en formato digital
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	La aplicación es propiedad de la Corporación
Integraciones con otros sistemas	- Facturación y Cartera - Safix - Pgar - Portal web (Página web institucional)
Debilidades o hallazgos estructurales	Contar con un Sistema de Gestión Documental que maneje las tablas de retención, flujos de documentos, entre otros.

Tabla 43 Sistema PQRS

Nombre aplicación	**Sistema de Gestión de PQRSDIF (Sirena, e-Sirena)**
Descripción Funcional	Sistema que se encarga de la gestión de las peticiones, quejas y reclamos que los ciudadanos u otras organizaciones realizan a la Entidad.
Información que gestiona	Petición Queja Reclamo Sugerencia Denuncia Información Felicitación
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	La aplicación es propiedad de la Corporación
Integraciones con otros sistemas	- Facturación y Cartera - Safix - Pgar - Portal web (Página web institucional)
Debilidades o hallazgos estructurales	Contar con un Sistema de Gestión Documental que integre la gestión de las PQRSDIF.

Tabla 44 Sistema KOHA

Nombre aplicación	**KOHA**
Descripción Funcional	Sistema de apoyo que permite la búsqueda online de material de la memoria institucional y material bibliográfico de la Corporación.
Información que gestiona	Información ambiental producida por la Corporación Material bibliográfico Estudios, investigaciones, entre otros
Tipo de software	Open Source
Estado	Productivo

Nombre aplicación	KOHA
Esquema de licenciamiento	Suscripción anual de licenciamiento
Integraciones con otros sistemas	No aplica
Debilidades o hallazgos estructurales	Actualizar aplicación y componentes a su última versión.

Tabla 45 Plataforma (MEGATESO)

Nombre aplicación	(Metas Estratégicas de Gestión Ambiental para Territorios Sostenibles - MEGATESO)
Descripción Funcional	Es una plataforma que fomenta el trabajo colaborativo, a través de varios componentes de software basadas en Microsoft 365, que permiten la gestión de los procesos, generando, obteniendo y fortaleciendo el conocimiento en factores como la seguridad, disponibilidad, accesibilidad e integralidad de la información.
Información que gestiona	Con Megateso se pretende dar cobertura a todas dependencias de la Entidad teniendo en cuenta los distintos grupos internos de trabajo, por ello, la estructura se hace extensiva, lo que permite brindar una herramienta que unifica la gestión. Cada una de las dependencias, subdirecciones, Oficinas, el Sistema de Gestión integral (SGI), así como las distintas mesas en la Corporación (instrumentos económicos, Calidad del Aire, Consulta previa, entre otras), dispondrán de un espacio que les permitirá disfrutar de todas las ventajas de Megateso. Adicionalmente en MEGATESO se incluyen: Tableros de Control Sistema de Gestión Integral Accesos a aplicativos corporativos Pruebas de escritorio de indicadores
Tipo de software	Software como servicio

Nombre aplicación	**(Metas Estratégicas de Gestión Ambiental para Territorios Sostenibles - MEGATESO)**
Estado	Productivo
Esquema de licenciamiento	Microsoft – Enterprise Agreement
Integraciones con otros sistemas	Comercial
Debilidades o hallazgos estructurales	Aplicación utilizada recientemente, por tal motivo, no se han identificado oportunidades de mejora.

Tabla 46 Aplicación Sembratón

Nombre aplicación	**Sembratón**
Descripción Funcional	Sistema de apoyo a la gestión que permite registrar la información de reforestación en la Jurisdicción de la Corporación, así mismo, el registro y seguimiento a la Estrategia BIO+.
Información que gestiona	Registro de la reforestación arbórea en la Jurisdicción
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	La aplicación es propiedad de la Corporación
Integraciones con otros sistemas	No aplica
Debilidades o hallazgos estructurales	Integración con otras aplicaciones de la Corporación.

Tabla 47 Plataforma VITAL

Nombre aplicación	**VITAL**
Descripción Funcional	La plataforma VITAL (Ventanilla Integral de Trámites Ambientales en Línea) que administra el Ministerio de Ambiente y Desarrollo Sostenible (MADS) es un sistema

Nombre aplicación	VITAL
	centralizado que permite gestionar trámites ambientales en línea.
Información que gestiona	Esta herramienta facilita a los ciudadanos y empresas la solicitud y seguimiento de permisos, licencias y otros trámites ambientales, promoviendo la eficiencia, transparencia y eficacia en la gestión pública.
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	La plataforma la administra el Ministerio de Ambiente y Desarrollo Sostenible (MADS).
Integraciones con otros sistemas	Plataforma con interoperabilidad con los sistemas de información misionales de cada autoridad ambiental o entidad del sector ambiente.
Debilidades o hallazgos estructurales	No aplica.

Tabla 48 Plataforma RESPEL

Nombre aplicación	RESPEL
Descripción Funcional	La plataforma RESPEL (Registro de Generadores de Residuos o Desechos Peligrosos) es una herramienta gestionada por el Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM).
Información que gestiona	Esta plataforma captura información normalizada y sistemática sobre la generación y manejo de residuos peligrosos en el país.
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	La plataforma la administra el Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM).
Integraciones con otros sistemas	No aplica.

Nombre aplicación	RESPEL
Debilidades o hallazgos estructurales	No aplica.

Tabla 49 Plataforma SISAIRE

Nombre aplicación	SISAIRE
Descripción Funcional	La plataforma SISAIRE (Subsistema de Información sobre Calidad del Aire) es una herramienta gestionada por el Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM) de Colombia.
Información que gestiona	Su principal objetivo es recolectar, analizar y difundir información sobre la calidad del aire en el país. Esta plataforma es fundamental para la gestión ambiental en Colombia, ayudando a monitorear y mejorar la calidad del aire, lo cual es crucial para la salud pública y el medio ambiente.
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	La plataforma la administra el Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM).
Integraciones con otros sistemas	No aplica.
Debilidades o hallazgos estructurales	No aplica.

Tabla 50 Plataforma SIRH

Nombre aplicación	SIRH
Descripción Funcional	La plataforma SIRH (Sistema de Información del Recurso Hídrico) en Colombia es una herramienta gestionada por el Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM).

Nombre aplicación	SIRH
Información que gestiona	Su objetivo principal es integrar y estandarizar la recolección, registro, manejo y consulta de datos relacionados con el recurso hídrico.
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	La plataforma la administra el Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM).
Integraciones con otros sistemas	No aplica.
Debilidades o hallazgos estructurales	No aplica.

Tabla 51 Plataforma SIPGACAR-CARDINAL

Nombre aplicación	SIPGACAR-CARDINAL
Descripción Funcional	La plataforma SIPGACAR-CARDINAL (Sistema de Información sobre Planeación y Gestión de las CAR) es una herramienta desarrollada para mejorar la planificación y gestión ambiental de las Corporaciones Autónomas Regionales (CAR) y de Desarrollo Sostenible.
Información que gestiona	SIPGACAR es un sistema en línea que facilita el reporte de los Planes de Acción Institucional de las CAR.
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	La plataforma la administra el Ministerio de Ambiente y Desarrollo Sostenible (MADS).
Integraciones con otros sistemas	No aplica.
Debilidades o hallazgos estructurales	No aplica.

Tabla 52 Plataforma SNIF

Nombre aplicación	SNIF
Descripción Funcional	La plataforma SNIF (Sistema Nacional de Información Forestal) es una herramienta gestionada por el Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM).
Información que gestiona	Su objetivo principal es integrar y estandarizar la captura, almacenamiento, análisis, procesamiento, difusión, manejo, verificación y consulta de datos relacionados con los recursos forestales.
Tipo de software	Desarrollo a la medida
Estado	Productivo
Esquema de licenciamiento	La plataforma la administra el Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM).
Integraciones con otros sistemas	No aplica.
Debilidades o hallazgos estructurales	No aplica.

6.1.11 Capacidades Funcionales de los Sistemas de Información

A continuación, se presenta la matriz que relaciona las capacidades funcionales de cada una de las aplicaciones ayudando a identificar las aplicaciones que apoyan su gestión.

Tabla 53 Capacidades Funcionales de los SI

Función	Sirena y e-Sirena	Safix	Pgar	Facturación y Cartera	Laboratorio	SGI - Megateso	Piragua Y Sembratón	Portal Web	Visor Geográfico	Koha
Administrar información jurídica y técnica	X									
Administrar información administrativa y financiera		X								
Realizar seguimiento a la Contratación y Plan de Adquisiciones			X							
Controlar la facturación y cartera, cobro coactivo y convenios de pago				X						
Administrar información de servicios de laboratorio					X					

Función	Sirena y e-Sirena	Safix	Pgar	Facturación y Cartera	Laboratorio	SGI - Megateso	Piragua Y Sembratón	Portal Web	Visor Geográfico	Koha
Administrar la información de seguimiento a las metas y estrategias Corporativas del SGI						X				
Pagos electrónicos (PSE)	X									
Facturación TUA y TR				X						
PQRSDIF	X									
Consulta de Trámites Ambientales en Línea	X									
Colillas de pago	X									
Monitoreo de Recursos Naturales (Agua y Aire) de la Jurisdicción							X			

Función	Sirena y e-Sirena	Safix	Pgar	Facturación y Cartera	Laboratorio	SGI - Megateso	Piragua Y Sembratón	Portal Web	Visor Geográfico	Koha
Transparencia y Acceso a la Información Pública								X		X
Visor Cartográfico de la Jurisdicción									X	

6.1.12 Ciclo de Vida de los Sistemas de Información

A partir del año 2020 la Corporación emprendió proyectos de desarrollo de soluciones tecnológicas y de aplicaciones Web con personal vinculado y con profesionales de apoyo a la gestión corporativa (Contratistas). En este sentido, la Corporación se encuentra en una etapa inicial para sus proyectos de desarrollo, diseñando los procedimientos y formatos para su posterior inclusión en el Sistema de Gestión Integral de la Corporación.

Tabla 54 Situación Actual del Ciclo de Vida de los SI

Actividad	Grado de Madurez	Descripción Hallazgo u Oportunidad de Mejora
Levantamiento de necesidades de Sistemas de Información	Informal	Se cuenta con un formato en el cual se realiza el levantamiento de requerimientos, a través de la metodología de entrevistas, análisis y recolección de información.
Análisis de requisitos funcionales y no funcionales	Informal	A partir de las necesidades manifiestas en el levantamiento de requerimientos, se realiza la formulación de los requisitos funcionales y no funcionales del sistema de

Actividad	Grado de Madurez	Descripción Hallazgo u Oportunidad de Mejora
		información para su posterior revisión y aprobación por parte del solicitante.
Diseño de la solución	Informal	De acuerdo con los requerimientos funcionales, se realiza la estructuración de la base de datos y el diseño o interfaz de la aplicación para su revisión y aprobación por parte del solicitante. Se utiliza la metodología SCRUM para estos procesos.
Codificación del software	Informal	Con la aprobación del diseño de la solución se inicia el desarrollo de la aplicación utilizando control de versionamiento. Como oportunidad de mejora se debe definir el estándar de codificación de los desarrollos.
Aseguramiento de la calidad (pruebas)	Informal	Actualmente se realizan pruebas manuales de calidad, como oportunidad de mejora se deben definir y diseñar las pruebas automatizadas.
Despliegue en Producción	Informal	Al verificar el funcionamiento de la aplicación se procede a realizar toda la preparación para su despliegue en los servidores de la Corporación.

Como oportunidad de mejora general se deben implementar políticas, procedimientos y formatos para los ciclos de vida de los Sistemas de Información.

6.1.13 Mantenimiento de los Sistemas de Información

En esta sección se describen los diferentes tipos de mantenimientos de software que se realizan en la Entidad, así mismo, se identifican hallazgos u oportunidades de mejora que puedan tener cada uno de los procedimientos de mantenimiento.

Tabla 55 Matriz de Mantenimientos de SI

Actividad	Grado de Madurez	Descripción Hallazgo u Oportunidad de Mejora
Mantenimientos correctivos	Informal	Los procesos de contratación cuyo objeto son soporte y mantenimiento de las aplicaciones, incluyen la realización de mantenimientos correctivos a cada una, sin embargo, no se cuenta con un procedimiento formal que establezca periodicidad y tipo de mantenimiento a llevar a cabo. La identificación de causas, requerimientos e incidentes se realiza diariamente con los usuarios.
Mantenimientos preventivos	Informal	Los procesos de contratación cuyo objeto son soporte y mantenimiento de las aplicaciones, incluyen la realización de mantenimientos preventivos a cada una, sin embargo, no se cuenta con un procedimiento formal que establezca periodicidad y tipo de mantenimiento a llevar a cabo. La identificación de causas, requerimientos e incidentes se realiza diariamente con los usuarios.
Mantenimientos adaptativos	No tiene	No se cuenta con un plan de rollback en caso de que la actualización impacte negativamente el comportamiento del sistema.
Mantenimientos evolutivos	No tiene	Tiempos de respuesta muy altos en la evolución de los sistemas. No se cuenta con un plan de mantenimiento evolutivo que permita mejorar el performance de las aplicaciones.

6.1.14 Soporte de los Sistemas de Información

En esta sección se describen los diferentes tipos de soporte de aplicaciones que se realizan en la Entidad, así mismo, se identifican hallazgos u oportunidades de mejora que puedan tener cada uno de los procedimientos de soporte.

Tabla 56 Matriz de Soportes de SI

Actividad	Grado de Madurez	Descripción Hallazgo u Oportunidad de Mejora
Soporte de aplicaciones nivel 1	Informal	No hay suficientes Servidores Públicos en el GIT TIC para atender el volumen de requerimientos e incidentes reportados de las aplicaciones. Se cuenta con una aplicación Open Source llamada HelpDesk para recibir los requerimientos de los usuarios, sin embargo, no se tienen definidos ANS que permitan hacer gestión y seguimiento a las solicitudes.
Soporte de aplicaciones nivel 2	Informal	No hay suficientes Servidores Públicos en el GIT TIC para atender el volumen de requerimientos e incidentes reportados de las aplicaciones. Con el contrato de Datacenter se cuenta con el Soporte Nivel 2, y el Contratista cuenta con una aplicación para recibir los requerimientos e incidentes reportados por el GIT TIC. Se cuentan con ANS definidos para atender, gestionar y resolver las solicitudes.
Soporte de aplicaciones nivel 3	Informal	Se cuenta con soporte y ANS definidos por parte del Fabricante.

6.1.15 Infraestructura de TI

A continuación, se muestra el diagrama de la Infraestructura Tecnológica Actual de la Corporación, donde se visualizan los equipos activos de red, infraestructura de servidores y sistema de almacenamiento centralizado (SAN), con conexión a la red pública Internet.

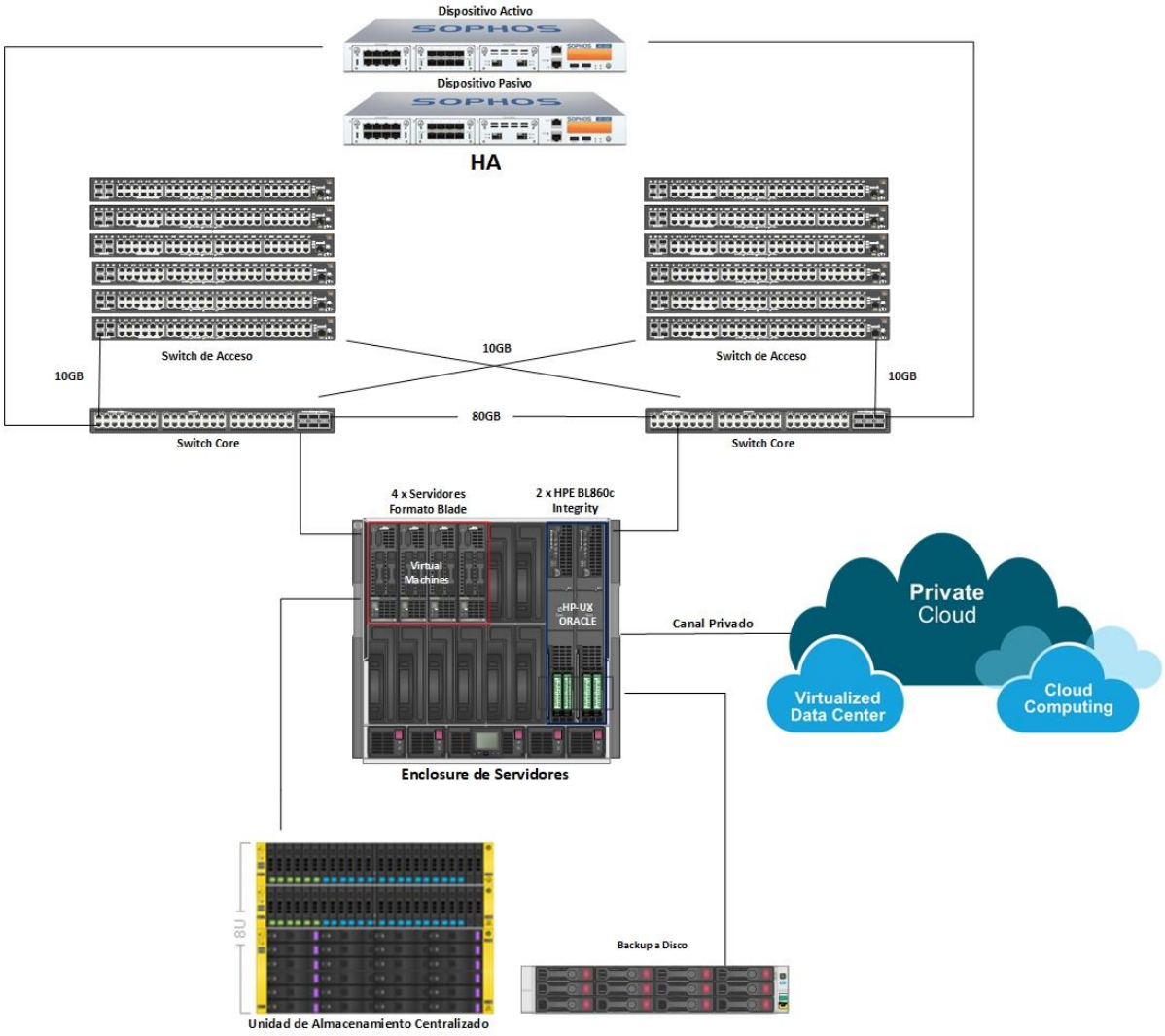


Figura 8 Infraestructura de TI CORANTIOQUIA

Fuente: Elaboración Propia

6.1.16 *Catálogo de Servicios de Infraestructura de TI.*

A continuación, se relacionan los servicios de infraestructura de la Corporación.

Tabla 57 Servicios de Infraestructura de TI

Servicio de Infraestructura	Descripción
Nube	Servicio de nube pública donde se alojan las aplicaciones colaborativas como Outlook, Teams, Sharepoint, OneDrive, Forms, Stream, entre otras.
Redes	Servicio SDWAN que permite la conectividad a internet, a los servicios LAN que le permite a los usuarios de la Entidad acceder a los sistemas de información y la comunicación con las Oficinas Territoriales.
Seguridad	Servicio de seguridad perimetral que permite controlar el tráfico de red desde y hacia Internet y aporta protección contra ataques externos, además, se cuenta con una protección endpoint, es decir, el antimalware.
Servidores	Servicio de infraestructura de hardware para el alojamiento de aplicaciones.
Almacenamiento	Servicio de infraestructura de hardware para el almacenamiento de información y copias de respaldo.
Telefonía	Servicio donde se centraliza y gestiona todas las consultas y peticiones relacionadas con la telefonía IP y móvil.
Facilities	Servicios asociados el centro de cómputo para garantizar la disponibilidad de los servicios alojados.
Periféricos	Servicios asociados a los equipos asignados a los usuarios finales como son impresoras, escáner, plotter y datamax.

6.1.17 *Catálogo de Elementos de Infraestructura.*

Puedes hacer uso del producto tipo de Catálogo de Elementos de Infraestructura para identificar los elementos de esta, su tipo y el servicio de infraestructura involucrado.

Tabla 58 Elementos de Infraestructura de TI

Elemento de infraestructura	Tipo	Servicio de Infraestructura involucrado
8 servidores físicos	Instalado en sitio	Servicio on premise
77 servidores virtuales	Instalado en sitio	Servicio on premise
Red de almacenamiento SAN	Instalado en sitio	Servicio de almacenamiento
Balanceador de carga	Instalado en sitio	Servicio de disponibilidad
14 servidores web	Instalado en sitio	Servicio on premise
4 servidores de aplicaciones	Instalado en sitio	Servicio on premise
Software virtualizador	Instalado en sitio	Servicio on premise
Motor base de datos	Instalado en sitio	Servicio on premise Servicio de aplicación Servicio de almacenamiento
Antimalware	Instalado en sitio	Servicio de seguridad
Firewall	Instalado en sitio	Servicio on premise Servicio de acceso red interna Servicio de VPN Servicio WAN
Web Application Firewall	Instalado en sitio	Servicio de seguridad Servicio de acceso red interna

Elemento de infraestructura	Tipo	Servicio de Infraestructura involucrado
Servidor DNS	Instalado en sitio	Servicio de enrutamiento
Servidor VPN	Instalado en sitio	Servicio de conexión remota
Servicio NTP Web	Software como servicio	Servicio de sincronización de reloj
Sistema de archivos	Instalado en sitio	Servicio de almacenamiento
Repositorio de certificados de seguridad	Instalado en sitio	Servicio de seguridad
Software de monitoreo de servidores	Instalado en sitio	Servicio de continuidad del negocio
Software de monitoreo de red	Instalado en sitio	Servicio de continuidad del negocio
Motor ETL	Instalado en sitio	Servicio de bases de datos Servicio de instalación de software
Framework de programación	Instalado en sitio	Servicio de instalación de software
Software de ofimática	Instalado en sitio Software como servicio	Servicio de instalación de software
Servidor correo electrónico	Software como servicio	Servicio de correo electrónico
Router	Instalado en sitio	Servicio de red LAN Servicio de red SDWAN

Elemento de infraestructura	Tipo	Servicio de Infraestructura involucrado
		Servicio de WIFI
Switch	Instalado en sitio	Servicio de red LAN Servicio de red SDWAN
Software de enmascaramiento de datos	Instalado en sitio	Servicio de seguridad-protección de datos
Software de cifrado de datos	Instalado en sitio	Servicio de seguridad-protección de datos
Software de diseño de planos	Instalado en sitio	Servicio de instalación de software
Software de georreferenciación	Instalado en sitio Software como servicio	Servicio de instalación de software
Ubicación física de Datacenter	Instalado en sitio	Servicio on premise
Computador personal	Instalado en sitio	Servicio on premise

6.1.18 Administración de la Capacidad de la Infraestructura Tecnológica

Define cuáles son los mecanismos y estrategias relacionadas a la administración de la capacidad de servicios claves de la infraestructura tecnológica.

A continuación, se definen elementos claves a gestionar.

- Infraestructura (Centro de Computo – Nube).
- Hardware y Software de Oficina.
- Conectividad.
- Red Local e Inalámbrica.
- Red WAN.
- Continuidad y Disponibilidad.
- Gestión de ANS.
- Seguridad.

6.1.19 Administración de la Operación

La operación de servicios tecnológicos de la Corporación busca garantizar la disponibilidad y continuidad de los servicios tecnológicos por medio de procesos, procedimientos, actividades y herramientas.

Tabla 59 Operación de los Servicios Tecnológicos

Identificador	Descripción	Sí	No
Monitoreo de la infraestructura de TI	Herramientas, actividades o procedimiento de monitoreo para identificar, monitorear y controlar el nivel de consumo de la infraestructura de TI.	X	
Capacidad de la infraestructura tecnológica	Se realizan planes de capacidades que permiten proyectar las capacidades de la infraestructura a partir de la identificación de las capacidades actuales.		X
Disposición de residuos tecnológicos	Se cuenta con procesos y procedimientos para una correcta disposición final de los residuos tecnológicos.	X	

La Corporación implementa los procesos de soporte y mantenimiento preventivo y correctivo de los servicios tecnológicos, de acuerdo con las necesidades de su operación.

Tabla 60 Matriz de Mantenimientos

Identificador	Descripción	Sí	No
Acuerdos de Nivel de Servicios	Se han establecido Acuerdos de Nivel de Servicios y se vela por el cumplimiento.	X	
Mesa de Servicio	Se tienen herramientas, procedimientos y actividades para atender requerimientos e incidentes de infraestructura tecnológica.		X
Planes de mantenimiento	Se generan y ejecutan planes de mantenimiento preventivo y correctivo sobre toda la infraestructura de TI.	X	

La implementación del protocolo IPv6 ya se ejecutó en la Corporación, de conformidad con los lineamientos de la Resolución del MinTIC 01126 de 2021.

Tabla 61 Fases de Implementación IPV6

Identificador	Descripción	Sí	No
Fase de Diagnóstico	Se han desarrollados actividades de diagnóstico de la infraestructura tecnológica para determinar el grado de alistamiento de la Entidad.	X	
Fase de Implementación	Se han desarrollado actividades de implementación del protocolo IPv6.	X	
Fase de Pruebas	Se han desarrollado pruebas de funcionalidad del protocolo IPv6 para garantizar la operación de los servicios tecnológicos.	X	

6.1.20 Uso y Apropiación

Los grupos de interés que se relacionan en la Caracterización del Proceso de Gestión de TIC requieren transferencia de conocimiento y capacitación permanente en el uso y apropiación de tecnologías de la información y las comunicaciones.

Necesidades y	Público objetivo	3. Cadena de valor público (Entradas - Actividades - Salidas) ➔ Resultados o efectos - Impactos	Bienes y	Público objetivo
3.1 Parte Interesada Interna (Grupo de valor)	**3.1 Entradas (satisfacen una necesidad o expectativa del proceso)**	**3.2. Actividades**	**3.3. Salidas (satisfacen una necesidad o expectativa de la parte interesada)**	**3.3 Parte Interesada Interna (Grupo de valor)**
Procesos organizacionales	• Requerimientos de soporte. • Solicitudes para el desarrollo de productos de software • Solicitudes de equipos, software y licencias. • Datos para custodia.	Coordinar formulación del Petic Coordinar formulación del plan de seguridad y privacidad de la información Coordinar formulación del plan de tratamiento de riesgos de seguridad y privacidad de la información Definir lineamientos y políticas Administrar riesgos y oportunidades, riesgos y peligros en SST y aspectos e impactos ambientales Coordinar la ejecución de los instrumentos de planificación del proceso Administrar arquitectura de TIC Administrar la plataforma tecnológica Desarrollar y administrar los aplicativos Gestionar mesa de servicios Implementar políticas y controles de seguridad y privacidad de la información Realizar seguimiento, medición, análisis y evaluación Formular e implementar planes de mejoramiento	• Plataforma tecnológica (hardware, software, almacenamiento de información en oinfa, disco y en la nube, red de voz y datos) disponible para el uso • Soporte en TIC (mesa de servicios) • Desarrollo y administración de productos de software • Lineamientos y políticas de TIC • Petic • Plan de seguridad y privacidad de la información • Plan de tratamiento de riesgos de seguridad y privacidad de la información	Procesos organizacionales
Planeación organizacional	**General:** • Direccionamiento estratégico • Instrumentos de planificación estratégica (PGAR y Plan de Acción) • PAAC • Instrumentos de planificación del SGI (planes de trabajo, de objetivos, del cambio, mapa de riesgos y oportunidades) • Arquitectura corporativa y mapa de procesos • Informes de gestión • Rendición de cuentas del SGI **Particular:** • Plan de cierre de brechas de MIPG (Gobierno digital y Seguridad digital)		• Necesidades y expectativas. • Información para la formulación de los instrumentos de planificación estratégica (PGAR y Plan de Acción) y del SGI • Seguimiento a metas en instrumentos de planificación estratégica (PGAR y Plan de Acción) y del SGI • Designación del enlace del SGI	Planeación organizacional
Gestión del conocimiento y la innovación	• Plan de gestión del conocimiento corporativo • Información ambiental y corporativa (cartográfica, documentos técnicos, entre otros). • Herramientas para compartir el conocimiento y la innovación. • Soluciones tecnológicas en el campo ambiental y corporativo.		**General:** • Requerimientos de información ambiental y corporativa. • Lecciones aprendidas. • Propuestas de innovación corporativa y territorial. • Resultados de la ejecución de proyectos, contratos y convenios corporativos que incorporan la gestión del conocimiento y la innovación. • Solicitudes de generación de soluciones tecnológicas. **Particular:** • Plataforma del portal geográfico disponible para el uso	Gestión del conocimiento y la innovación
Gestión de las comunicaciones	**General:** • Plan estratégico de comunicaciones • Manuales para la gestión de las comunicaciones • Información en medios • Productos comunicacionales • Eventos corporativos • Gestión de canales de comunicación institucionales • Gestión de relaciones públicas **Particular:** • Requerimientos de soporte respecto a la página web y la intranet		**General:** • Necesidades y solicitudes de comunicación interna y externa • Información (documentos, fotografías, cifras, testimonios, entre otros) **Particular:** • Plataforma de página web y de intranet disponible para el uso	Gestión de las comunicaciones
Planeación de territorios sostenibles	• Planes temáticos o misionales • Informes de ejecución de planes temáticos o misionales • Determinantes ambientales		Necesidades y expectativas.	Planeación de territorios sostenibles
Atención al ciudadano	• Orientaciones para la atención al ciudadano • Solicitud de información para dar respuesta a PQRSDIF • Informes de satisfacción		Información para dar respuesta a PQRSDIF	Atención al ciudadano
Administración de los recursos naturales renovables	• Trámites y OPA publicados en SUIT • Registro de datos de operación de los trámites y OPA realizados • Modelo de Administración de los Recursos Naturales, con enfoque diferencial		Necesidades y expectativas respecto al Modelo de Administración de los Recursos Naturales, con enfoque diferencial.	Administración de los recursos naturales renovables
Muestreo y análisis de laboratorio	**Particular:** Requerimientos de soporte respecto al sistema de información Laboratorio		**Particular:** Sistema de información Laboratorio	Muestreo y análisis de laboratorio
Participación, diversidad étnica y cultura ambiental	Modelo de participación		Necesidades y expectativas respecto al Modelo de Participación	Participación, diversidad étnica y cultura ambiental
Gestión de territorios sostenibles	• Modelo de Administración de Áreas Protegidas • Modelo de operación para consolidar los viveros y el CAV		Necesidades y expectativas respecto al: Modelo de Administración de Áreas Protegidas y al Modelo de operación para consolidar los viveros y el CAV	Gestión de territorios sostenibles

Necesidades y / Público objetivo	3. Cadena de valor público (Entradas - Actividades - Salidas) → Resultados o efectos - Impactos			Bienes y / Público objetivo
3.1 Parte interesada interna (Grupo de valor)	**3.1 Entradas (satisfacen una necesidad o expectativa del proceso)**	**3.2. Actividades**	**3.3. Salidas (satisfacen una necesidad o expectativa de la parte interesada)**	**3.3 Parte interesada interna (Grupo de valor)**
Gestión del talento humano	• Personal y practicantes (cantidad y competencia) • Plan estratégico de talento humano • Código de integridad • Lineamientos o políticas • Actividades de bienestar, de formación y capacitación • Incentivos • Constancias • Elementos de protección personal • Intervención de peligros y riesgos laborales • Acciones de prevención de accidentes e incidentes de trabajo y enfermedades laborales • Orientaciones y acompañamiento en la EDL • Servidores públicos preparados para el retiro del servicio público • Requerimientos de información	Coordinar formulación del PETIC Coordinar formulación del plan de seguridad y privacidad de la información Coordinar formulación del plan de tratamiento de riesgos de seguridad y privacidad de la información Definir lineamientos y políticas Administrar riesgos y oportunidades, riesgos y peligros en SST y aspectos e impactos ambientales Coordinar la ejecución de los instrumentos de planificación del proceso Administrar arquitectura de TIC Administrar la plataforma tecnológica Desarrollar y administrar los aplicativos Gestionar mesa de servicios Implementar políticas y controles de seguridad y privacidad de la información Realizar seguimiento, medición, análisis y evaluación Formular e implementar planes de mejoramiento	• Requerimientos de personal. • Requerimiento de fortalecimiento de competencias. • Retroalimentación.	Gestión del talento humano
Gestión de bienes y servicios	• Bienes muebles e inmuebles corporativos en adecuadas condiciones de uso y disfrute • Servicios de apoyo (aseo, vigilancia, aseguramiento, mantenimiento, transporte, suministros, control, custodia y administración) • Plan maestro de infraestructura física • Plan de movilidad empresarial sostenible • Manual de bienes muebles		**General:** • Solicitudes de compra y mantenimiento bienes muebles e inmuebles • Requerimientos de servicios de apoyo (aseo, vigilancia, aseguramiento, mantenimiento, transporte, suministros, control, custodia y administración) **Particular:** Residuos tecnológicos para su disposición	Gestión de bienes y servicios
Gestión de la información	• Instrumentos archivísticos (PINAR, TRD, PGD, SIC, registros de activos de información, esquema de publicación, índice de información clasificada y reservada) • Información interna y externa radicada • Información de transparencia de acceso público (página web) • Política de protección de datos personales • Información documentada incorporada en el SGI (Megateso). • Capacitaciones y socialización en gestión de la información		• Información para radicación y envío al destinatario. • Información requerida para dar cumplimiento a Ley de transparencia y acceso a la información pública. • Información documentada aprobada para controlar en el SGI. • Archivos para transferencia documental. • Solicitud de descriptores • Solicitud de capacitaciones y socialización	Gestión de la información
Gestión financiera	• Recursos financieros • Asesoría financiera en contratos y convenios • Información financiera		Necesidades de recursos financieros	Gestión financiera
Gestión contractual	**General:** • Plan anual de adquisiciones (PAA) • Asesoría y acompañamiento en la gestión contractual • Capacitaciones • Directrices y conceptos • Minutas de contratación • Actas de aprobación de garantía única • Bienes, servicios y obras **Particular:** • Solicitudes de asesoría en la incorporación de las TIC en los contratos y convenios		**General:** • Solicitud de contratación de bienes y servicios (Estudios previos) • Solicitud de elaboración de contratación en el aplicativo PGAR • Pólizas para aprobación • Necesidades de capacitación y asesoría • Información y documentación soporte para contratos y convenios. **Particular:** Recomendaciones a nivel de las TIC a considerar en los contratos y convenios.	Gestión contractual
Gestión jurídica	• Política de prevención del daño antijurídico • Emisión de actos administrativos y directrices • Sentencias		• Consultas de conceptos jurídicos • Solitudes de análisis de posible presentación de demandas • Información en relación con las consultas y demandas	Gestión jurídica
Evaluación independiente	• Informes de auditoría de control interno y de entes de control • Informes de ley e informes de seguimiento (Sistema de control interno y Ley de transparencia) **Nota:** los informes se referencian en el documento FT-MAS-07 Seguimiento informes legales del proceso		• Información requerida para ejercer los roles de control interno. • Acciones para el plan de mejoramiento de control interno y entes de control. • Respuesta a requerimientos.	Evaluación independiente
Mejoramiento continuo	• Informes de auditoría del SGI (interna y externa) • Informes de seguimiento (planes de mejoramiento del SGI y revisión por la dirección) • Informe del IEDI		• Designación de un servidor público para formarse y participar como auditor interno del SGI • Participación en auditorías internas. • Evaluación del equipo auditor. • Información para la revisión por la dirección. • Plan de mejoramiento del SGI (Oficina de Control Interno). • Plan de mejoramiento institucional.	Mejoramiento continuo

Necesidades y / Público objetivo	3. Cadena de valor público (Entradas - Actividades - Salidas) ➔ Resultados o efectos - Impactos			Bienes y / Público objetivo
3.1 Parte interesada interna (Grupo de valor)	3.1 Entradas (satisfacen una necesidad o expectativa del proceso)	3.2. Actividades	3.3. Salidas (satisfacen una necesidad o expectativa de la parte interesada)	3.3 Parte interesada interna (Grupo de valor)
3.4 Parte interesada externa	3.4 Entradas o expectativa del proceso	Coordinar formulación del Petic	3.5 Salidas o expectativas de la parte interesada	3.5 Parte interesada Externa
Usuarios de los servicios	Solicitudes de soporte	Coordinar formulación del plan de seguridad y privacidad de la información	Soporte en TIC (mesa de ayuda)	Usuarios de los servicios
MinTIC	• Lineamientos en relación a las TIC • Requerimientos de información	Coordinar formulación del plan de tratamiento de riesgos de seguridad y privacidad de la información	Respuesta a requerimientos	MinTIC
Entidades públicas del orden nacional	Acceso a aplicaciones para su interoperabilidad	Definir lineamientos y políticas	Requerimientos de interoperabilidad	Entidades públicas del orden nacional
Entes de control	• Requerimientos de información • Requerimientos de interoperabilidad	Administrar riesgos y oportunidades, riesgos y peligros en SST y aspectos e impactos ambientales	• Respuesta a requerimientos • Acceso a aplicaciones para su interoperabilidad	Entes de control
Servidores públicos de la corporación	Requerimientos de credenciales para acceso y uso de aplicativos y sistemas de información corporativos	Coordinar la ejecución de los instrumentos de planificación del proceso	Credenciales para acceso y uso de aplicativos y sistemas de información corporativos	Servidores públicos de la corporación
Contratistas y proveedores	• Licencias de software • Requerimientos de credenciales para acceso y uso de aplicativos y sistemas de información corporativos	Administrar arquitectura de TIC	Credenciales para acceso y uso de aplicativos y sistemas de información corporativos	Contratistas y proveedores
Veedurías ciudadanas	• Requerimientos de información y de control social	Administrar la plataforma tecnológica	• Respuesta a requerimientos de información y de control social • Espacios y canales de participación	Veedurías ciudadanas
		Desarrollar y administrar los aplicativos		
		Gestionar mesa de servicios		
		Implementar políticas y controles de seguridad y privacidad de la información		
		Realizar seguimiento, medición, análisis y evaluación		
		Formular e implementar planes de mejoramiento		

Figura 9 Matriz de Partes Interesadas Proceso Gestión TIC

Fuente: Elaboración Propia

6.1.20.1 Formación y capacitación

La Corporación a través del Plan Institucional de Capacitación (PIC) adoptado en el Plan Estratégico de Talento Humano, contempla formación y capacitación a los Servidores Públicos en el uso y apropiación de las TIC, además, a través de los Proveedores de Servicios Tecnológicos, se logra capacitación adicional en temas de ofimática, correo electrónico, y uso y apropiación de M365 E3.

6.1.21 Seguridad

Mediante el **Acuerdo del Consejo Directivo número 180-ACU2209-642 del 29 de septiembre de 2022,** se determinó la estructura organizacional de la Corporación.

El Gobierno de TI en Corantioquia está conformado por el Grupo Interno de Trabajo Tecnologías de la Información y las Comunicaciones y el Grupo Interno de Trabajo Gestión de la Información y el Conocimiento.

EY apoyó a CORANTIOQUIA en la **Formulación del Programa de Seguridad de la Información**. En el proyecto se identificaron múltiples vulnerabilidades y se planteó unas acciones requeridas por parte de la Corporación para cerrar las brechas de seguridad de la información.

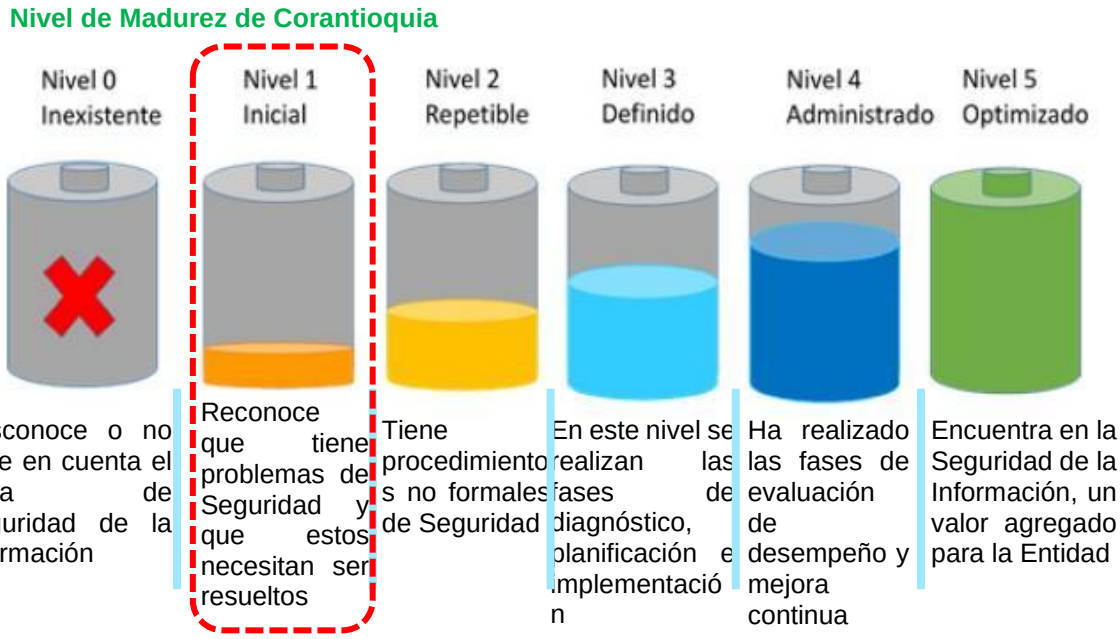


Figura 10 Situación Actual Seguridad CORANTIOQUIA

Fuente: Documentación Contrato 190-CNT1909-110

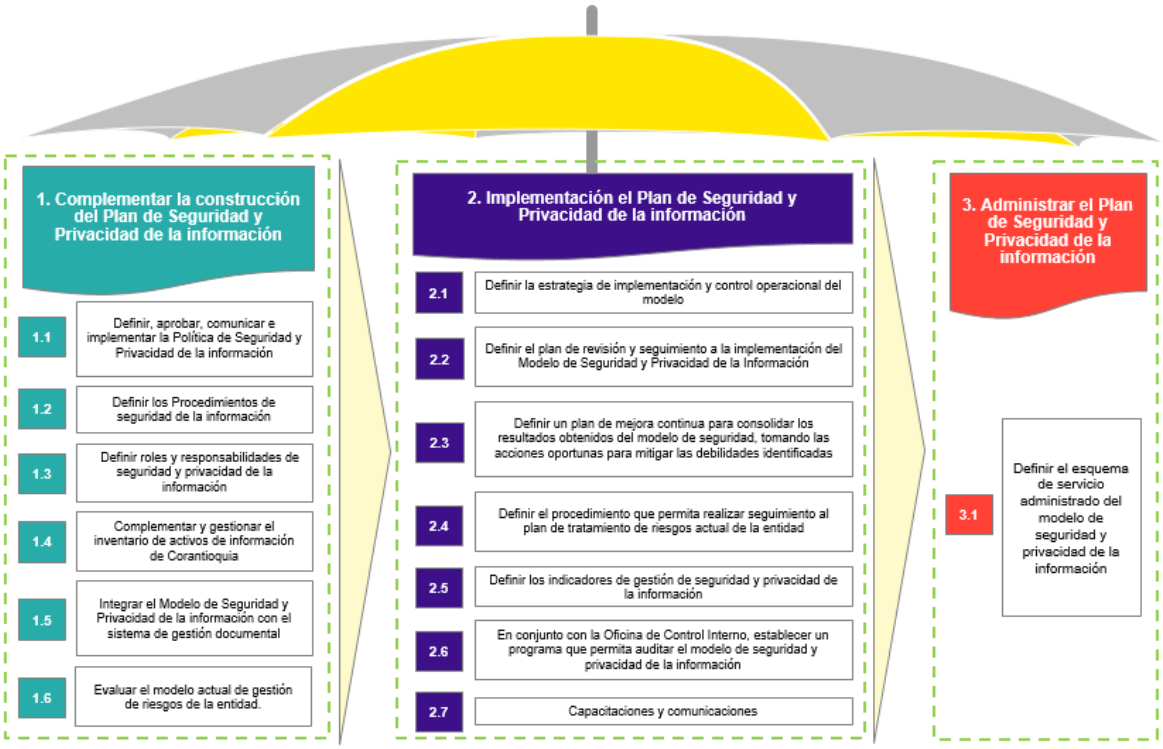


Figura 11 Estructuración Plan de Seguridad y Privacidad de la Información en CORANTIOQUIA

Fuente: Documentación Contrato 190-CNT1909-110

Por otro lado, previo a las actividades por ejecutar del Plan de Seguridad y Privacidad de la Información, se aplicará la herramienta establecida por el Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) "Instrumento Evaluación del Modelo de Seguridad y Privacidad de la información - MSPI" para autodiagnosticar el nivel de madurez de la entidad en seguridad y privacidad de la información, esto con el propósito de tener un enfoque estructurado y eficiente para cerrar los puntos claves o vulnerables identificados.

Adicionalmente contamos con la Política General de Tecnología de Seguridad y Privacidad de la Información que se requiere actualizar, y el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad, estos dos últimos se están formulando para el periodo 2024-2027.

6.2 Marco normativo

A continuación, se relaciona la normativa clave para la estructuración del Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC).

Tabla 62 Marco Normativo

Marco Normativo	Descripción
Decreto 2150 de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública.
Conpes 3292 de 2004	Proyecto de racionalización y automatización de trámites.
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. De los atentados informáticos y otras infracciones.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Norma Técnica Colombiana NTC 5854 de 2012	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.

Marco Normativo	Descripción
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Protección de Datos Personales.
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
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 2433 de 2015	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de
Conpes 3854 de 2016	Política Nacional de Seguridad Digital. El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el

Marco Normativo	Descripción
	ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
Resolución 2405 de 2016	Por la cual se adopta el modelo del Sello de Excelencia Gobierno en Línea y se conforma su Comité.
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1413 de 2017	Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.

Marco Normativo	Descripción
Conpes 3920 de 2018	Política Nacional de Explotación de Datos (Big Data). La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
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.
Ley 1978 de 2019	Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
Conpes 3975 de 2019	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
Decreto 2106 del 2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública. Cap. II Transformación Digital Para Una Gestión Publica Efectiva.

Marco Normativo	Descripción
Directiva 02 de 2019	Simplificación de la interacción digitalmente los ciudadanos y el estado. Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones. Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
Ley 2052 de 2020	Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y/ 0 administrativas en relación con la racionalización de trámites y se dictan otras disposiciones.
Decreto 620 de 2020	Por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Ley 2080 de 2021	Por medio de la cual se reforma el código de procedimiento administrativo y de lo contencioso administrativo -ley 1437 de 2011- y se dictan otras disposiciones en materia de descongestión en los procesos que se tramitan ante la jurisdicción

Marco Normativo	Descripción
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Resolución 1126 de 2021	Por la cual se modifica la Resolución 2710 de 2017.
Directiva 03 de 2021	Lineamientos para el Uso de Servicios en la Nube, Inteligencia Artificial, Seguridad Digital y Gestión de Datos. Imparte directrices en relación con los lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
Decreto 767 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 1263 de 2022	Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública.
Ley 2294 de 2023	Por el cual se expide el Plan Nacional de Desarrollo 2022-2026. “Colombia potencia mundial de la vida”. Artículo 142. Conectividad Digital para Cambiar Vidas. Artículo 143. Transformación Digital como Motor de Oportunidades e Igualdad. Artículo 144. Fortalecimiento del Sector TIC.

6.3 Logros

Como logros del PETIC 2022-2023 se dio cumplimiento a los siguientes proyectos enmarcados en las iniciativas de transformación digital:

1. Se adquirió y se encuentra en proceso de implementación el nuevo Sistema de Información Administrativo, Financiero, Contable y Fiscal, Integrado, en servicios de Nube (SaaS) denominado ERP SICOF.
2. Se migró entre el 25% y el 35% de la información almacenada en los equipos servidores corporativos, a servicios de nube (OneDrive, SharePoint).
3. Se incrementarán los canales de Internet y canales de datos en al menos un 25% (Interconexión Sede Central con las Oficinas Territoriales)
4. Se renovó la Solución de Seguridad Informática (Firewall, Antivirus, Anti-spam), Licenciamiento de Microsoft M365 E3, Firma digital y electrónica, Implementación del factor de doble autenticación (MFA), Adopción e implementación del Protocolo IPv6.

Figura 12 Logros del PETIC 2022-2023 sobre cuatro (4) iniciativas claves

6.4 Retos

Además de la estructura programática propuesta para la implementación del PETIC 2024-2027, se identifican los siguientes retos orientados a cumplir con las metas asociadas a las siguientes iniciativas de transformación digital y modernización tecnológica:

1. Adquisición o actualización del sistema misional SIRENA
2. Migración entre un 35% y el 70% de la información almacenada en los equipos servidores corporativos, a servicios de nube (OneDrive, SharePoint).
3. Incremento de los canales de Internet y canales de datos en al menos un 50% (Interconexión Sede Central con las Oficinas Territoriales)

4. Renovación de la Solución de Seguridad Informática (Firewall, Antivirus, Anti-spam), Licenciamiento de Microsoft M365 E3, Firma digital y electrónica, Continuar con el uso del factor de doble autenticación (MFA).

6.5 Tendencias tecnológicas

A continuación, se describe el estado y proyección de las tendencias tecnológicas en la Corporación que servirán como base para la formulación de las iniciativas y estrategias, alineado a las necesidades y oportunidades que se plantearán en el PETIC.

Tabla 63 Tendencias Tecnológicas

Nombre	Estado y Proyección de Tendencias Tecnológicas en la Corporación
Aplicaciones móviles	Uso de aplicaciones móviles para la captura y registro de información durante la realización de visitas técnicas en el territorio.
Uso de nube- Software como servicio	Las aplicaciones misionales y de apoyo a la gestión de la Corporación en el mediano plazo deberán migrarse a servicios de nube.
Uso de nube- Plataforma como servicio	La Corporación en el largo plazo contemplará la contratación de servicios en la nube, bajo la modalidad de alquiler o tercerización de plataformas tecnológicas como servicio.
Uso de nube- Infraestructura como servicio	La Corporación en el largo plazo contemplará la contratación de servicios en la nube, bajo la modalidad de alquiler o tercerización de la infraestructura tecnológica como servicio.
Automatización de procesos con motor BPM (Business Process Manager) y motor RPA (Robotic Process Automation)	La Corporación a mediano plazo deberá iniciar la automatización de procesos empresariales requiriendo un enfoque estratégico y bien planificado, identificando y

Nombre	Estado y Proyección de Tendencias Tecnológicas en la Corporación
	documentando los procesos actuales que podrían beneficiarse de la automatización, priorizando aquellos que son repetitivos, consumen mucho tiempo y son propensos a errores humanos, evaluando la viabilidad técnica y económica de automatizar estos procesos.
Software para análisis de datos descriptivo	La Corporación actualmente viene implementando la contratación de licenciamiento de herramientas de software como Power BI para la implementación del diseño y construcción de reportes y tableros de control.
Software para análisis de datos predictivo	El Programa Piragua dispone de un Sistema de Información para la gestión de las Bases de Datos y contenido de las herramientas Web: Geoportal, Sitio web y Aplicativo móvil con análisis de datos que incluye la generación de alertas tempranas.
Software de inteligencia artificial	La Corporación ha venido explorando con otras Entidades Públicas la aplicación de sistemas expertos en tiempo real para la identificación en áreas de la jurisdicción de prácticas de minería ilegal, entre otros aspectos que permitan ejercer la autoridad ambiental. Además, se realizarán las gestiones necesarias con el fin de brindar capacitación a los funcionarios en estos temas.

Nombre	Estado y Proyección de Tendencias Tecnológicas en la Corporación
Blockchain	La Corporación con la implementación soluciones tecnológicas de Bussiness Intelligent, realizará estudios de mercado que le permitan definir las mejores prácticas en sistemas distribuidos para identificar la veracidad y autenticidad de los datos e información que produce para sus usuarios internos y externos. Además, se realizarán las gestiones necesarias con el fin de brindar capacitación a los funcionarios en estos temas.
Gestión y análisis de datos estructurados (Motores ETL-ELT, Bodegas de datos y datamarts) y no estructurados (documentos, audios, videos) con Big Data	La Corporación se encuentra en el proceso de identificación de proyectos e iniciativas de transformación digital con el fin de implementar soluciones tecnológicas de Bussiness Intelligent a partir de la minería de datos, bodegas de datos (data Waterhouse, data marts), procedimientos OLAP, Dashboards y los DSS (Sistemas de soporte a decisiones) para contribuir con el proceso de toma de decisiones mediante la creación de informes dinámicos, flexibles e interactivos.
Herramientas de gestión de calidad de datos	La Corporación implementará herramientas que permitan la gestión de la calidad de datos en sus procesos, sistemas de información misionales y de apoyo.
Plataforma colaborativa	La Corporación implementará sistemas de colaboración abierta y masiva con acercamiento y enfoque al ciudadano.
Bases de datos NoSQL (Not Only SQL)	La Corporación se encuentra en el ejercicio de identificar proyectos e iniciativas donde se pueda implementar base de datos NoSQL.

Nombre	Estado y Proyección de Tendencias Tecnológicas en la Corporación
Internet de las cosas (IOT)	La Corporación explorará nuevas tecnologías que le permitan a través de diferentes dispositivos el ejercicio de la autoridad ambiental con integración a IoT.
Arquitectura de sistemas orientada a servicios SOA **Arquitectura de sistemas orientada a Microservicios**	La Corporación actualmente cuenta con interfaces que le permiten conectar algunas de sus aplicaciones internas con otras aplicaciones (internas y externas) a través del uso e implementación de Web Services y API.
Máquinas virtuales (Virtualización de hardware) **Virtualización de servidores.**	La Corporación actualmente a través del contrato de Gestión de su Infraestructura Tecnológica ha venido virtualizando su granja de servidores con el fin de fortalecer los servicios que presta a los usuarios internos y externos, contando con sistemas de alta disponibilidad y redundancia. Se cuenta con servicio de escritorio remoto (RDS) que permite a los usuarios conectarse a los servicios corporativos desde cualquier lugar con conexión a internet.
Metodologías ágiles	La Corporación se encuentra en proceso de identificación de proyectos e iniciativas de modernización tecnológica para aplicar metodologías agiles para el desarrollo de software.
Plataforma de interoperabilidad X-ROAD	La Corporación implementó la tecnología de X-ROAD para el proceso de interoperabilidad con la plataforma VITAL que administra el Ministerio de Ambiente y Desarrollo Sostenible (MADS).

Nombre	Estado y Proyección de Tendencias Tecnológicas en la Corporación
Carpeta ciudadana	La Corporación viene explorando el uso de la carpeta ciudadana digital para la consulta de trámites y contenidos.
Plataforma de publicación de datos abiertos	La Corporación actualmente ha venido dando cumplimiento a la Resolución del MinTIC 1519 del 2020, en lo que se refiriere al Artículo 7. Condiciones mínimas de publicación de datos abiertos, se han aprobados por el MinTIC y publicados en el portal de Datos Abiertos www.datos.gov.co 27 conjuntos de datos de 67, conforme con las directrices referidas en el Anexo 4, numeral 4.2 Estándares de Publicación de Datos Abiertos, de la presente Resolución. Esto incluyó las etapas de identificación, definición de metadatos, consolidación, estructuración y priorización de los conjuntos de datos corporativos.
Arquitectura Empresarial con el marco TOGAF 9.2 **Gobierno y Gestión de TI con el marco COBIT 2019** **Gestión de servicios de TI con el marco ITIL v4** **Gestión de proyectos con PMI**	La Corporación realizará las gestiones necesarias con el fin de brindar capacitación a los funcionarios en estos temas, y derivado de ello, en un mediano plazo iniciar con la implementación y aplicación de estas metodologías en beneficio de la Entidad.

7 Metodología empleada para la formulación

Para este Plan Estratégico de Tecnologías de la Información y las Comunicaciones 2024-2027 se toma como base la formulación e implementación del PETIC 2022-2023, las encuestas realizadas a directivos y servidores públicos realizadas en el 2024, las sesiones de trabajo con funcionarios de la Subdirección de Planeación y la Política de Gobierno Digital, establecida por el Decreto 767 de 2022.

7.1 Encuesta a Directivos

De la encuesta realizada a los directivos se obtuvo la siguiente información:

NOTA: Se evidencia que el diligenciamiento de la encuesta dirigida a los directivos de la Corporación la realizaron: una asesora de la Dirección General, dos Jefes de Oficina de la Sede Central y 7 Jefes de las Oficinas Territoriales

1. Por favor indique las necesidades actuales que usted considera se requieren de Tecnologías de la Información y las Comunicaciones en la Corporación.

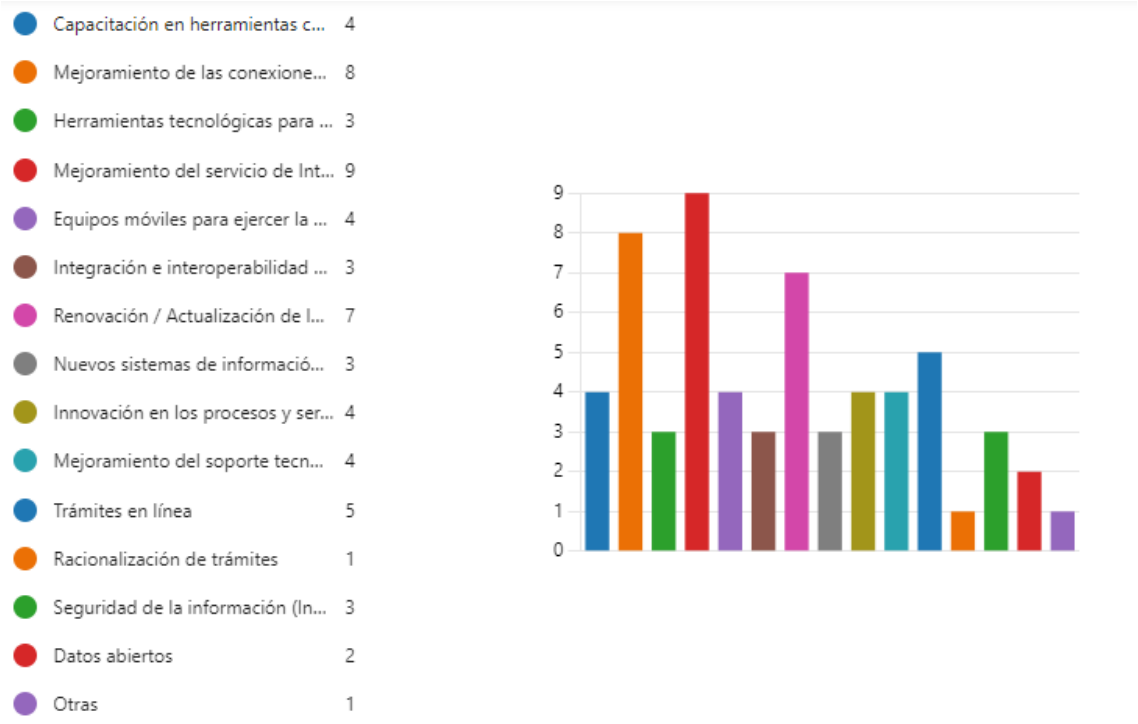


Figura 13 Respuesta N°1 a Directivos

Necesidad	Prioridad
Mejoramiento del servicio de Internet (mejorar velocidad y estabilidad).	9
Mejoramiento de las conexiones con los sistemas de información y aplicativos.	8
Renovación / Actualización de los sistemas de información actuales.	7
Trámites en línea.	5
Capacitación en herramientas colaborativas (Outlook, Sharepoint, Teams, OneDrive, Planner, Forms, Moodle, entre otras).	4
Equipos móviles para ejercer la autoridad ambiental (GPS, drones, entre otros).	4
Innovación en los procesos y servicios tecnológicos.	4
Mejoramiento del soporte tecnológico.	4
Herramientas tecnológicas para el Teletrabajo.	3
Integración e interoperabilidad entre aplicaciones y sistemas de información.	3
Seguridad de la información (Incluye la protección de datos personales).	3

Nuevos sistemas de información y aplicativos.	2
Datos abiertos.	2
Otros	1
Racionalización de trámites.	1

2. Por favor indique las expectativas para los próximos cuatro (4) años de Tecnologías de la Información y las Comunicaciones. (Que espera que el área de TI le proporcione a largo plazo, ejemplo, portafolio de proyectos, inversión, transformación digital, modernización tecnológica, entre otros).

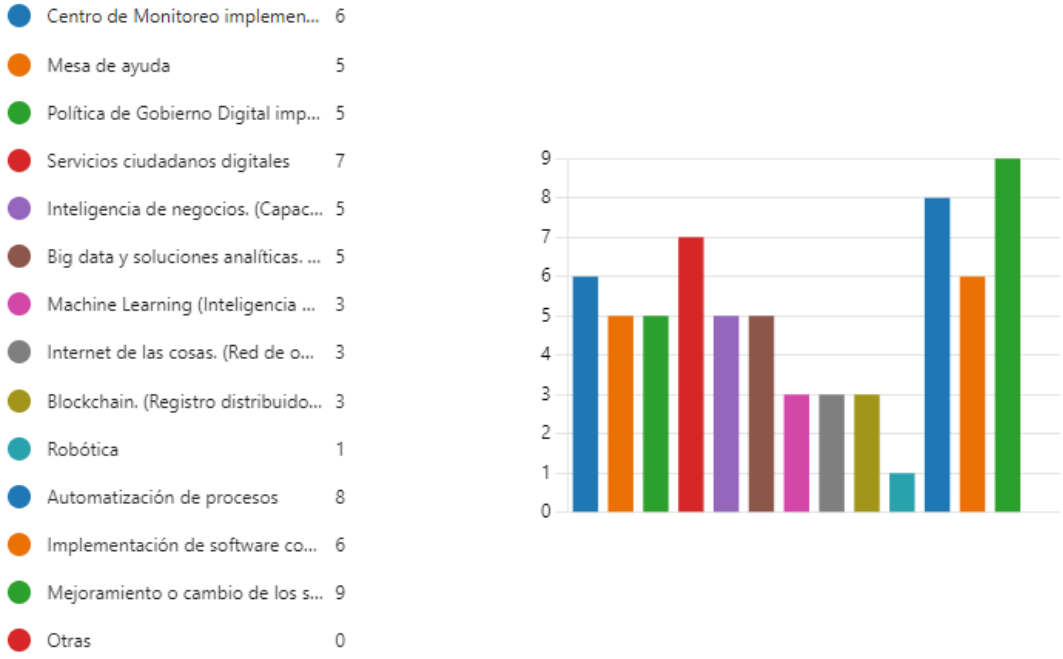


Figura 14 Respuesta N°2 a Directivos

Necesidad	Prioridad

Mejoramiento o cambio de los servicios tecnológicos (Equipos de cómputo, impresión, telefonía, audiovisuales, entre otros).	9
Automatización de procesos.	8
Servicios ciudadanos digitales.	7
Centro de Monitoreo implementado.	6
Implementación de software como servicio (Migración de las aplicaciones actuales a la nube).	6
Mesa de ayuda.	5
Política de Gobierno Digital implementada.	5
Inteligencia de negocios. (Capacidad para la toma de decisiones basada en la información actual).	5
Big data y soluciones analíticas. (Capacidad para la toma de decisiones basada en información predictiva, mirar hacia el futuro).	5
Machine Learning (Inteligencia artificial) (Aprendizaje automático de los sistemas).	3
Internet de las cosas. (Red de objetos físicos (vehículos, máquinas, electrodomésticos y más) que utiliza sensores para conectarse e intercambiar datos por internet).	3

Blockchain. (Registro distribuido que permite identificar la veracidad y autenticidad de un dato).	3
Robótica.	1
Otros	0

3. ¿Qué recomendaciones o sugerencias tiene para la Gestión de Tecnologías de la Información y las Comunicaciones en la Corporación? Ejemplo: Relacionar las actividades que no tienen apoyo de TIC.

Respuestas con mayor votación

“fortalecimiento en sistemas de información”

“Mejorar la disponibilidad del servicio de internet”

“Brindar capacitación permanente en sistemas de información internos”

Figura 15 Respuesta N°3 a Directivos

7.2 Encuesta a Servidores Públicos

De la encuesta realizada a los servidores públicos se obtuvo la siguiente información:

NOTA: Se evidencia que el diligenciamiento de la encuesta dirigida a los servidores públicos de la Corporación la realizaron 216 funcionarios de 461 funcionarios. (46.85%)

1. ¿Cuál es la percepción que tiene de las aplicaciones o herramientas tecnológicas de la corporación?

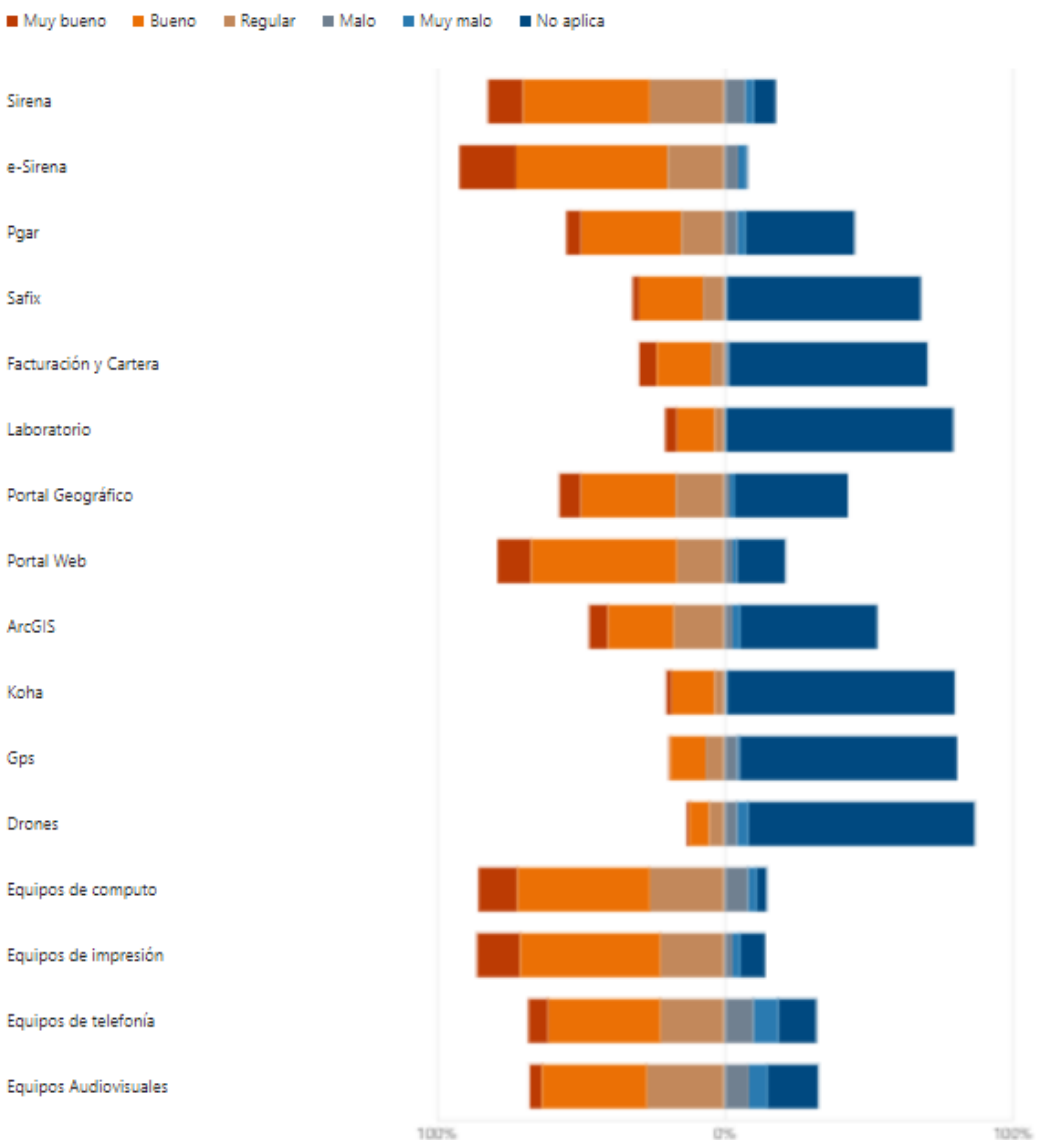


Figura 16 Respuesta N°1 SERVIDORES PÚBLICOS

2. Del siguiente listado, desde su percepción y situación actual, por favor indique cuales requieren de mejoras:

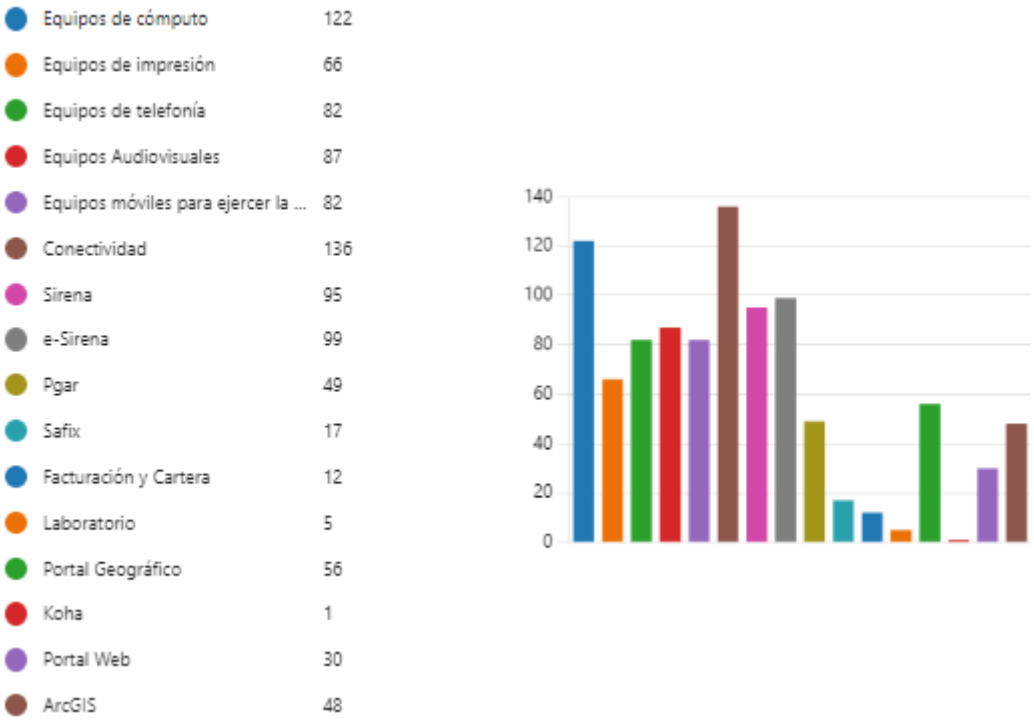


Figura 17 Respuesta N°2 SERVIDORES PÚBLICOS

3. De su respuesta anterior, ¿Qué mejoras requieren las opciones seleccionadas?

Respuestas con mayor votación

"actualización de algunos equipos de cómputo que ya están obsoletos, que los aplicativos Sirena y E sirena manejen los mismos módulos y permita una sincronización entre ambos, actualizar la interfaz de los aplicativos de manera que resulte más moderna y amena al usuario"

"actualización de la flota de drones"

"Se presenta mucha intermitencia con los aplicativos."

Figura 18 Respuesta N°3 SERVIDORES PÚBLICOS

4. Cuando usted tiene un problema con las aplicaciones, ¿Con quién se comunica para resolverlo?

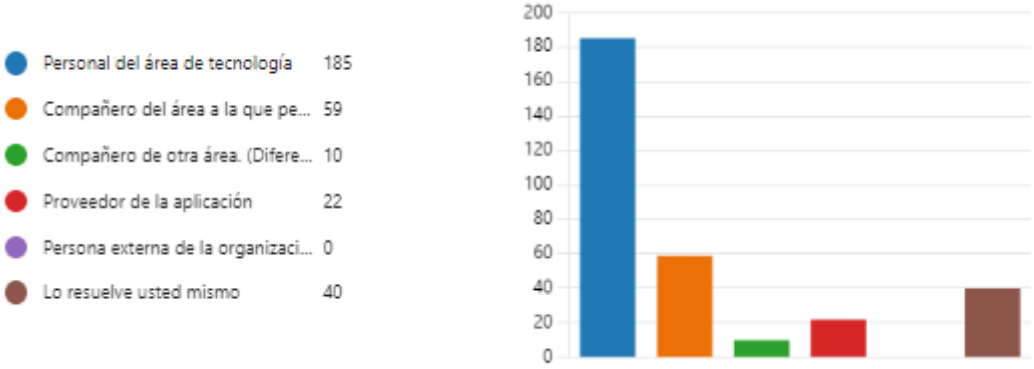


Figura 19 Respuesta N°4 SERVIDORES PÚBLICOS

Necesidad	Prioridad
Personal del área de tecnología.	185
Compañero del área a la que pertenece.	59
Lo resuelve usted mismo.	40
Proveedor de la aplicación.	22
Compañero de otra área. (Diferente a tecnología).	10
Persona externa de la organización	0

5. ¿Cómo califica usted el servicio de soporte tecnológico que presta la Corporación?

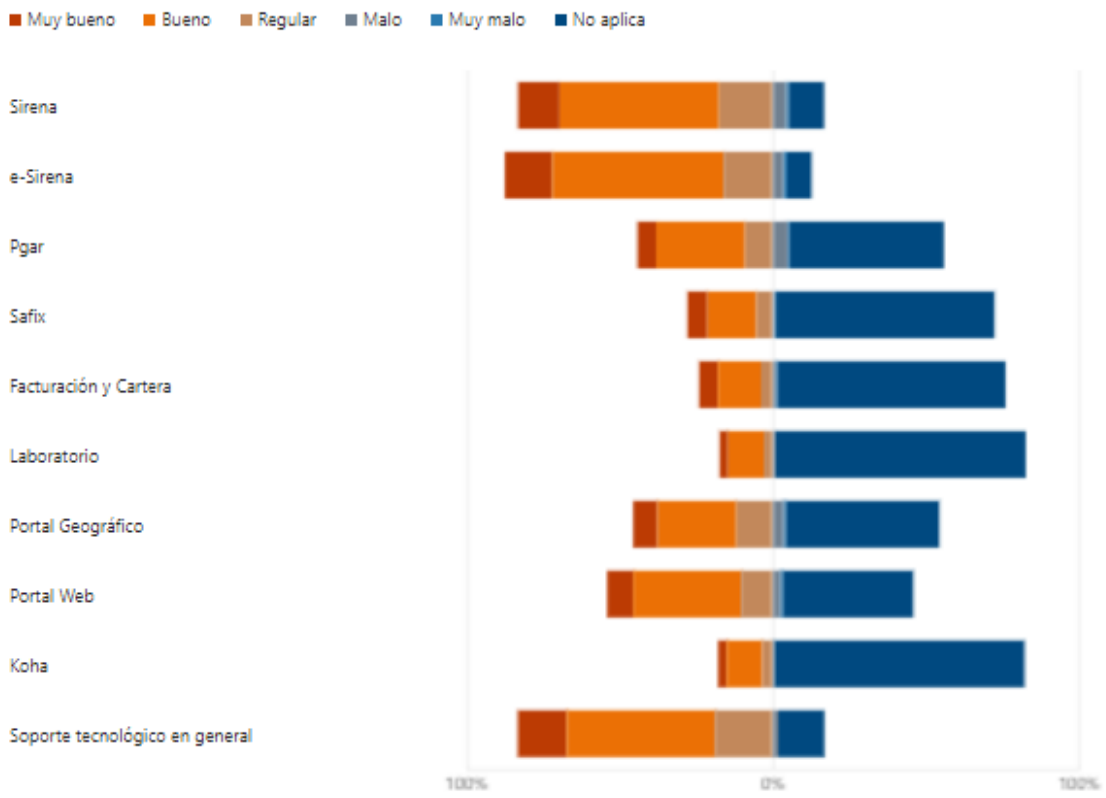


Figura 20 Respuesta N°5 SERVIDORES PÚBLICOS

6. De su respuesta anterior, por favor indique el motivo de su calificación, si su respuesta fue de “Regular” a “Muy Malo”; en caso contrario, seleccionar la opción “No aplica”:

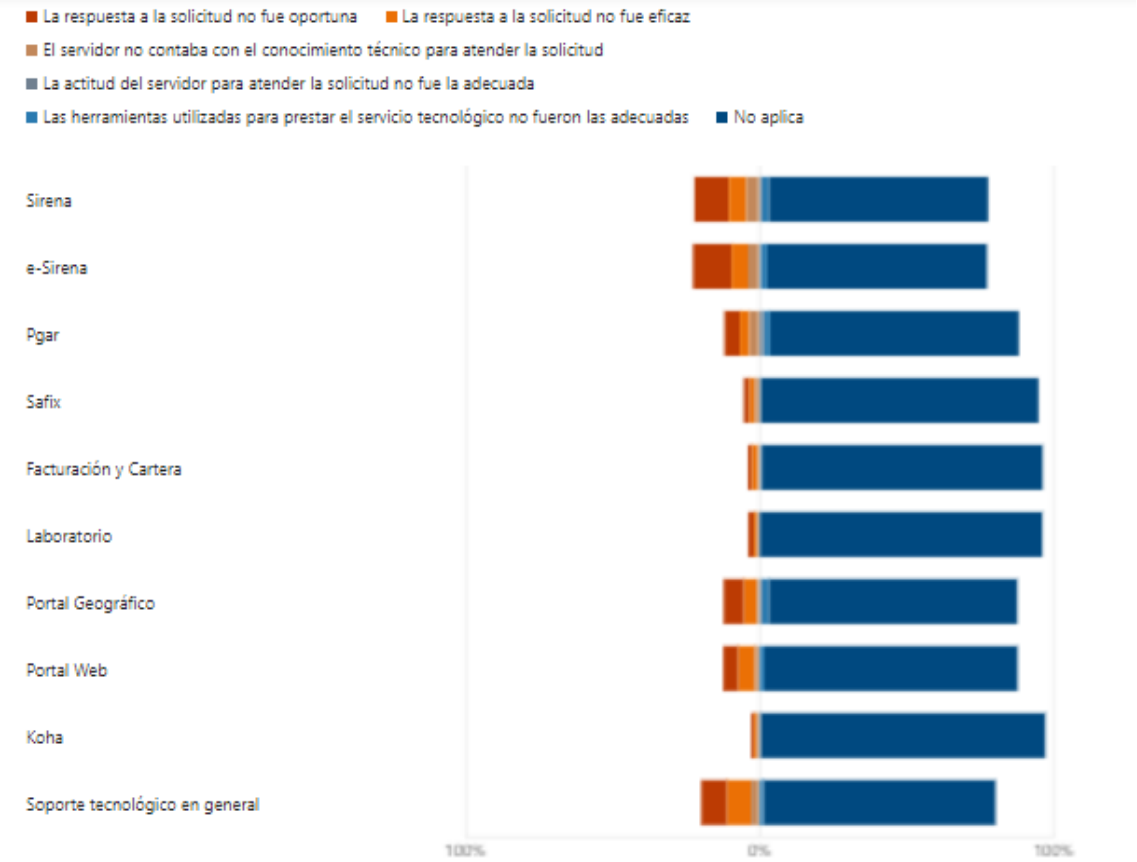


Figura 21 Respuesta N°6 SERVIDORES PÚBLICOS

7. Por favor indique las expectativas para los próximos cuatro (4) años en el área de Tecnologías de la Información y las Comunicaciones, en cuanto a los requerimientos en hardware (equipos), software (aplicaciones), desarrollos e implementaciones, usos y apropiación de las TIC para la mejora de las actividades del área o dependencia

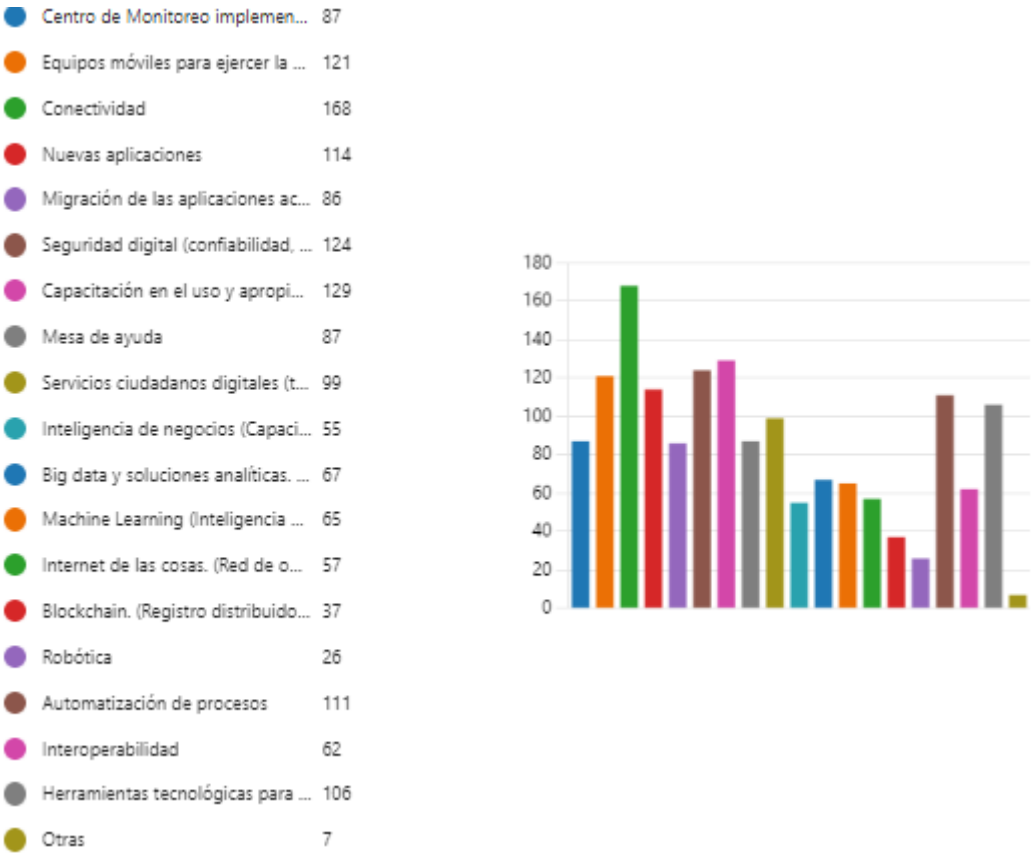


Figura 22 Respuesta N°7 SERVIDORES PÚBLICOS

Necesidad	Prioridad
Conectividad	170
Capacitación en el uso y apropiación de las TIC.	132
Seguridad digital (confiabilidad, integridad y disponibilidad de la información).	126
Equipos móviles para ejercer la autoridad ambiental (GPS, drones, entre otros).	124
Nuevas aplicaciones.	115
Automatización de procesos.	111
Herramientas tecnológicas para el Teletrabajo.	107
Servicios ciudadanos digitales (trámites en línea y racionalización de trámites).	101
Centro de Monitoreo implementado.	88
Migración de las aplicaciones actuales a la nube.	88
Mesa de ayuda.	88
Big data y soluciones analíticas. (Capacidad para la toma de	68

decisiones basada en información predictiva, mirar hacia el futuro).	
Machine Learning (Inteligencia artificial) (Aprendizaje automático de los sistemas).	66
Interoperabilidad.	63
Internet de las cosas. (Red de objetos físicos (vehículos, máquinas, electrodomésticos y más) que utiliza sensores para conectarse e intercambiar datos por internet).	57
Inteligencia de negocios (Capacidad para la toma de decisiones basada en la información oportuna, confiable, completa, pertinente y útil).	55
Blockchain. (Registro distribuido que permite identificar la veracidad y autenticidad de un dato).	37
Robótica.	26
Otras	7

8. De su respuesta anterior, ¿Qué esperaría se logre de las opciones seleccionadas?

Respuestas con mayor votación
"Mayor apropiación de las TICS para las labores diarias de autoridad ambiental en territorio, disponibilidad de los aplicativos e información documenta"
"actualización flota de drones"
"Mejorar no solo la capacidad operativa sino los tiempos de respuesta."

Figura 23 Respuesta N°8 SERVIDORES PÚBLICOS

8 Estructura programática

8.1 Iniciativas de Operación

Tabla 64 Iniciativa de Operación 01

FICHA DE PROYECTO			
Id del Proyecto	INI_OPE_01		
Nombre del Proyecto	Prestar servicios de intercomunicación de datos e internet para la Sede Central y Oficinas Territoriales.		
Objetivos del Proyecto	Mejorar la conectividad en los diferentes centros de trabajo (Sede Central, Oficinas Territoriales, Sedes locales, Viveros y CAV)		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$1.820.000.000

FICHA DE PROYECTO

Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		

Descripción/Alcance

Servicio de transmisión, recepción y administración de DATA WLAN, servicio de internet dedicado y suministro de direccionamiento IP público, en los siguientes Sedes:

Sede	Municipio	Tecnología Canal 1	Tecnología Canal 2
Central	Medellín	Multipunto MPLS	Internet dedicado por Fibra Óptica
Central	Medellín	Banda ancha por Fibra Óptica	N/A
Oficina Territorial Panzenú	Caucasia	Multipunto MPLS	Internet dedicado por Fibra Óptica
Oficina Territorial Tahamíes	Santa Rosa de osos	Multipunto MPLS	Internet dedicado por Fibra Óptica
Oficina Territorial Citará	Andes	Multipunto MPLS	Internet dedicado por Fibra Óptica
Oficina Territorial Hevéxicos	Santa fe de Antioquia	Multipunto MPLS	Internet dedicado por Fibra Óptica
Oficina Territorial Cartama	Jericó	Multipunto MPLS	Internet dedicado por Fibra Óptica
Oficina Territorial Zenufaná	Vegachí	Multipunto MPLS	Internet dedicado por Fibra Óptica

Sede	Municipio	Tecnología Canal 1	Tecnología Canal 2
Vivero	Santa Elena	Multipunto MPLS	Internet dedicado por Fibra Óptica
CAV	San Jerónimo	Pendiente Viabilidad Técnica	Pendiente Viabilidad Técnica
Vivero	Hispania	Pendiente Viabilidad Técnica	Pendiente Viabilidad Técnica

Tabla 65 Iniciativa de Operación 02

FICHA DE PROYECTO			
Id del Proyecto	INI_OPE_02		
Nombre del Proyecto	Uso y Apropiación de TIC.		
Objetivos del Proyecto	Capacitar al personal de la Corporación y al equipo TIC en el uso y apropiación de las TIC, sistemas de información, herramientas, licencias y Moodle.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	Asociado al Plan de Capacitación de la Corporación
Prioridad de la Implementación	**Alta** Media Baja		
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			
Generar y fortalecer en los grupos de interés, las competencias generales y específicas de TI, que permitan convertir la tecnología en habilitador de la estrategia de la institución.			

Tabla 66 Iniciativa de Operación 03

FICHA DE PROYECTO	
Id del Proyecto	INI_OPE_03
Nombre del Proyecto	Modelo de Atención al Ciudadano y Racionalización de Trámites.
Objetivos del Proyecto	Fortalecer el Modelo de Atención al Ciudadano a través de la implementación de asesores virtuales.

FICHA DE PROYECTO

Tiempo Aproximado de Ejecución	4 años		**Costo Aproximado de Implementación**	$30.000.000	
Prioridad de la Implementación	**Alta**	Media	Baja		
Responsables	Subdirección Administrativa y Financiera				

Descripción/Alcance

Dentro del componente del Plan de Transparencia y Ética Pública (PTEP) - Transparencia y Acceso a la Información Pública se busca contar con asesores virtuales, con quienes la población pueda tener comunicación directa para obtener respuestas inmediatas.

Se contemplan otras acciones que también buscan fortalecer el modelo de atención, entre las que se encuentran:

1. Contar con aplicaciones móviles, como estrategia para interactuar de manera virtual con los ciudadanos.

2. Contar con la consulta y radicación de peticiones, quejas, reclamos, solicitudes y denuncias (PQRSD) de la entidad, diseñada y habilitada para su uso en dispositivos móviles (ubicuidad o responsive).

3. Habilitar funcionalidades que permitan a los usuarios hacer seguimiento al estado de los trámites disponibles en línea o parcialmente en línea.

4. Promover el uso de las TIC facilitando el acceso de la ciudadanía a la información sobre trámites y a su ejecución por medios electrónicos (SUIT).

Tabla 67 Iniciativa de Operación 04

FICHA DE PROYECTO

Id del Proyecto	INI_OPE_04
Nombre del Proyecto	Portal Web Corporativo, Intranet y Datos Abiertos.

Objetivos del Proyecto	Actualizar la página web e intranet de la Corporación según la norma técnica NTC 5854 y lineamientos del MinTIC.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$100.000.000
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		

Descripción/Alcance

Optimización del sitio web e intranet de Corantioquia www.corantioquia.gov.co con la migración de plataforma, SEO, ciberseguridad y cumplimiento de normativa de Gobierno Digital, FURAG, ITA, NTC5854, MIPG y Resolución MinTIC 1519 de 2020 en sus anexos 1,2 y 3.

Adicionalmente, con base en el ejercicio de identificación de los conjuntos de datos corporativos que se determinaron mediante los talleres de Datos Abiertos realizados, y teniendo en consideración la obligatoriedad de las entidades públicas de “divulgar datos abiertos” según lo establecido en la Ley 1712 de 2014, artículo 11, literal k), se han realizado las siguientes actividades:

- Identificación de los conjuntos de datos corporativos.
- Priorización de los conjuntos de datos.
- Definición de metadatos.
- Consolidación y estructuración de los conjuntos de datos para publicarlos como Datos Abiertos.
- Cargue y publicación de los conjuntos de datos en la plataforma de Datos Abiertos https://www.datos.gov.co/.
- Fortalecimiento continuo de la estrategia.

Tabla 68 Iniciativa de Operación 05

FICHA DE PROYECTO				
Id del Proyecto	INI_OPE_05			
Nombre del Proyecto	Prestar el servicio de actualización, soporte y mantenimiento al Sistema Koha.			
Objetivos del Proyecto	Facilitar el acceso a la información de las bases de datos bibliográficas a los usuarios internos y externos.			
Tiempo aproximado de Ejecución	4 años	**Costo Aproximado de implementación**	$76.000.000	
Prioridad de la Implementación	**Alta**	Media	Baja	
Responsables	Subdirección Administrativa y Financiera y Planeación			
Descripción/Alcance				
Actualización del sistema a su última versión estable, garantizando el correcto funcionamiento de los módulos del sistema (Catalogación, Usuarios, Circulación y Préstamo, Publicaciones Periódicas, Adquisiciones, Autoridades, Catálogo en Línea, Reportes/Informes, Listas, Herramientas) y los módulos o desarrollos adicionales que tiene el sistema funcionando actualmente (código QR, Banner).				

Tabla 69 Iniciativa de Operación 06

FICHA DE PROYECTO	
Id del Proyecto	INI_OPE_06
Nombre del Proyecto	Servicio de soporte, mantenimiento, actualización y mejora del Visor Geográfico.

FICHA DE PROYECTO

Objetivos del Proyecto	Actualizar el Visor Geográfico de la Corporación, con su respectivo soporte y mantenimiento.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$347.000.000
Prioridad de la Implementación	**Alta** Media Baja		
Responsables	Subdirección Administrativa y Financiera y Planeación		

Descripción/Alcance

Contar con el servicio de:

- Licenciamiento y actualización del Visor Geográfico de Corantioquia a la última versión del visor geográfico MapGIS®.
- Soporte y mantenimiento del sistema.
- Transferencia de conocimiento.

Tabla 70 Iniciativa de Operación 07

FICHA DE PROYECTO

Id del Proyecto	INI_OPE_07		
Nombre del Proyecto	Soporte, mantenimiento y actualización de licencias ArcGIS.		
Objetivos del Proyecto	Actualizar licencias ArcGis, con su respectivo soporte y mantenimiento.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$765.000.000

FICHA DE PROYECTO

Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera y Planeación		

Descripción/Alcance

La Corporación cuenta con un Sistema de Información Geográfica (SIG) soportado a través del software licenciado ArcGIS de la casa Esri Colombia, a partir del cual se elabora, se revisa, se dispone y publica cartografía básica y temática para el uso interno y externo de la Corporación, así como para las Entidades del Sistema Nacional Ambiental (SINA) o aquellas que la requieran, con el fin de apoyar el desarrollo de Proyectos de Investigación, Planes de Ordenamiento Territorial y Planes de Desarrollo Municipal, entre otros, asegurando la transferencia y democratización de la información cartográfica, la cual contribuye a dinamizar el conocimiento de los usuarios que utilizan las herramientas geográficas a través de diferentes medios como la Web.

Tabla 71 Iniciativa de Operación 08

FICHA DE PROYECTO

Id del Proyecto	INI_OPE_08		
Nombre del Proyecto	Actualización, soporte y mantenimiento de los módulos del Sistema de Información Administrativo, Financiero, Contable y Fiscal.		
Objetivos del Proyecto	Actualización, soporte y mantenimiento de los módulos del Sistema de Información Administrativo, Financiero, Contable y Fiscal.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$ 1,693,202,880
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		

Descripción/Alcance
Actualización para nuevas versiones y cambios de Ley de los módulos del Sistema de Información Administrativo, Financiero, Contable y Fiscal: Inventario, Contabilidad, Nómina, Activos Fijos e Inmuebles, Presupuesto, Recursos Humanos, Tesorería, Contratos y Proyectos, con su respectivo servicio de soporte, mantenimiento y desarrollo de las aplicaciones, y transferir el conocimiento al personal corporativo que se designe según las necesidades de capacitación y refuerzo en los diferentes módulos y procesos.

Tabla 72 Iniciativa de Operación 09

FICHA DE PROYECTO			
Id del Proyecto	INI_OPE_09		
Nombre del Proyecto	Realizar el soporte y mantenimiento de las aplicaciones Sirena, Facturación y Cartera y Laboratorio.		
Objetivos del Proyecto	Realizar el soporte y mantenimiento de las aplicaciones Sirena, Facturación y Cartera y Laboratorio.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$1.500.000.000
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			
Actualización para nuevas versiones y cambios de Ley de la aplicación Sirena, e-Sirena, Laboratorio, con su respectivo servicio de soporte, mantenimiento, ajustes y nuevos desarrollos de los módulos que conforman las aplicaciones, y transferir el conocimiento al personal corporativo que se designe según las necesidades de capacitación y refuerzo en los diferentes módulos y procesos.			

Tabla 73 Iniciativa de Operación 10

FICHA DE PROYECTO			
Id del Proyecto	INI_OPE_10		
Nombre del Proyecto	Infraestructura Tecnológica.		
Objetivos del Proyecto	Prestar los servicios especializados que garanticen el buen funcionamiento de la Infraestructura Informática y de Telecomunicaciones de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA, que incluya el servicio de Mesa de Ayuda para mejorar la prestación de los servicios tecnológicos de la Corporación.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$2.756.000.000
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			
Realización de las operaciones técnicas necesarias para garantizar el correcto funcionamiento del centro de cómputo y los servicios informáticos y de telecomunicaciones de la Corporación Autónoma Regional del Centro de Antioquia, de conformidad con los Acuerdos de Nivel de Servicio (ANS), con un porcentaje de disponibilidad de la plataforma tecnológica de La Corporación, superior a 99,4%.			

Tabla 74 Iniciativa de Operación 11

FICHA DE PROYECTO	
Id del Proyecto	INI_OPE_11
Nombre del Proyecto	Mantenimiento de Equipos de Cómputo y Periféricos de la Entidad.

FICHA DE PROYECTO

Objetivos del Proyecto	Realizar el mantenimiento preventivo y correctivo a equipos de cómputo (todo en uno, portátiles y estaciones de trabajo), y tecnológicos y periféricos tales como, impresoras, plotter, escáneres, video proyectores, datamax, accesorios y/o equipos de telecomunicaciones de la Entidad.			
Tiempo Aproximado de Ejecución	4 años		**Costo Aproximado de Implementación**	$ 825,000,000
Prioridad de la Implementación	**Alta**	Media	Baja	
Responsables	Subdirección Administrativa y Financiera			

Descripción/Alcance

Realización de mantenimiento preventivo y correctivo, incluyendo elementos y partes nuevas a los equipos de cómputo y ofimáticos de la entidad que se encuentran ubicados en la Sede Central y en las Oficinas Territoriales de la Corporación, que incluye las siguientes actividades:

1: Realizar el mantenimiento preventivo a computadores portátiles y de escritorio, impresoras multifuncionales, impresoras de sticker, escáneres, videoproyectores y plotter; Incluyendo sus periféricos y accesorios básicos asociados a estos

2: Mantenimiento correctivo y provisión de las partes, repuestos y elementos nuevos y originales necesarios para la reparación y puesta en funcionamiento del plotter, escáneres, impresoras de stickers, videoproyectores, computadores portátiles y de escritorio defectuosos propiedad de la Corporación.

Tabla 75 Iniciativa de Operación 12

FICHA DE PROYECTO

Id del Proyecto	INI_OPE_12
Nombre del Proyecto	Licenciamiento de Productos de Software.

Objetivos del Proyecto	Contar con el licenciamiento necesario para el correcto funcionamiento del software Corporativo.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$7.096.000.000
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			
Contratar la suscripción de licencias de los productos M365 E3, Adobe, Oracle, Firewall, Avaya, HP. Este servicio deberá incorporar un esquema de uso y apropiación de las plataformas que permita a los usuarios de la Entidad hacer un uso eficiente de la totalidad de las herramientas incluidas en la suscripción.			

8.2 Iniciativas de Transformación Digital y Modernización Tecnológica

Tabla 76 Iniciativa de Transformación Digital y Modernización Tecnológica 01

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_01
Nombre del Proyecto	Modernización del Sistema de Información para la Administración de los Recursos Naturales para la Corporación Autónoma Regional del Centro de Antioquia - Corantioquia.
Objetivos del Proyecto	Modernizar el Sistema de Información en la Administración de los Recursos Naturales, para la Corporación Autónoma Regional del Centro de Antioquia - Corantioquia. Incluye Software como Servicio (SaaS)

FICHA DE PROYECTO

Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de implementación**	$ 1,600,000,000
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		

Descripción/Alcance

La plataforma tecnológica deberá cumplir como mínimo con las características funcionales, técnicas y tecnológicas, tanto en el diseño como en la versatilidad de sus aplicaciones, de acuerdo con los siguientes requerimientos:

- Hosting y/o alojamiento.
- Soporte técnico, mantenimiento y actualización de la solución.
- Especialistas por módulo.
- Transferencia de conocimiento.
- Documentación.

Tabla 77 Iniciativa de Transformación Digital y Modernización Tecnológica 02

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_02
Nombre del Proyecto	Renovación de la Infraestructura Tecnológica.
Objetivos del Proyecto	Migrar la Infraestructura Tecnológica de la Corporación a servicios de nube e híbrida (incluye migración de la infraestructura informática y de telecomunicaciones, sistemas de almacenamiento, sistemas de backups) según los lineamientos del MinTIC y la Directiva Presidencial 03 de 2021.

FICHA DE PROYECTO

Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$ 4,286,844,564
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			

Migración de la Infraestructura Tecnológica actual a la nube e híbrida, lo que permitirá centralizar toda la información de la Corporación en un espacio virtual que puede ser de forma pública o privada, es decir, puede permitir que sea consultada por muchos usuarios o bien decidir que solo tengan acceso un determinado número de usuarios; además, estas características hacen posible que los usuarios internos y externos puedan acceder a datos de interés desde cualquier lugar y reducir así los tradicionales procesos para compartir datos que solían gastar más tiempo.

Tabla 78 Iniciativa de Transformación Digital y Modernización Tecnológica 03

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_03		
Nombre del Proyecto	Renovación de Equipos Tecnológicos y Periféricos.		
Objetivos del Proyecto	Adquirir y renovar equipos tecnológicos de última generación de acuerdo con las necesidades de los procesos.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$1,600,000,000
Prioridad de la Implementación	Alta	**Media**	Baja

FICHA DE PROYECTO	
Responsables	Subdirección Administrativa y Financiera
Descripción/Alcance	
Adquisición de recursos tecnológicos, entre los cuales se encuentran: Equipos Servidores, almacenamiento, redes, equipos de escritorio, tabletas, portátiles, dispositivos electrónicos, periféricos, entre otros, para la prestación de los servicios que apoyan y soportan la operación, desarrollo y crecimiento de la Corporación.	

Tabla 79 Iniciativa de Transformación Digital y Modernización Tecnológica 04

FICHA DE PROYECTO			
Id del Proyecto	INI_TMOD_04		
Nombre del Proyecto	Nuevas Tecnologías para la Jurisdicción de la Corporación.		
Objetivos del Proyecto	Implementar tecnología de punta en el ejercicio de la autoridad ambiental y gestión de territorios sostenibles: equipos móviles (GPS, drones, entre otros) y aplicaciones.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$ 270,000,000
Prioridad de la Implementación	Alta	**Media**	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			
Implementación y operación de plataformas tecnológicas que permitan programar, gestionar, recolectar y almacenar la información de trabajo en campo que realiza la Entidad, en sus procesos misionales, tales como, Saneamiento, Guardabosques, Gestión del Riesgo, Negocios Verdes, con la posibilidad de incorporar de forma			

FICHA DE PROYECTO

dinámica nuevos formularios inteligentes para atender otros procesos de la Corporación.

Tabla 80 Iniciativa de Transformación Digital y Modernización Tecnológica 05

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_05		
Nombre del Proyecto	Planes Institucionales y Estratégicos de Tecnología alineados al PETIC.		
Objetivos del Proyecto	Actualizar el Modelo de Seguridad y Privacidad de la Información, alineado al Plan de Seguridad y Privacidad de la Información y al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$0 - Con recurso interno
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			

Formulación e implementación del Plan de Seguridad y Privacidad de la Información, Plan de Continuidad de TI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Comunicaciones de TI, alineados con la Política de Gobierno de Digital, Modelo de Seguridad y Privacidad de la Información y Modelo Operativo de TI del Ministerio de Tecnologías de la Información y las Comunicaciones.

Tabla 81 Iniciativa de Transformación Digital y Modernización Tecnológica 06

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_06		
Nombre del Proyecto	Gestión de Trámites Ambientales Integrados e Interoperables.		
Objetivos del Proyecto	Transformar la experiencia de los ciudadanos con los trámites y servicios por medios electrónicos, asegurando la promoción, la efectividad y la simplicidad (Interoperabilidad de las aplicaciones corporativas de carácter estratégica, misional y de apoyo con otras Entidades del Estado Nacionales y Territoriales), de conformidad con el nuevo el nuevo Modelo de Gestión y Operación de Administración de los Recursos Naturales Renovables, a través de la interoperabilidad con plataformas desarrolladas con nuevas tecnologías como por ejemplo la plataforma VITAL que administra el MADS y la implementación de la carpeta ciudadana digital, entre otras.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$300,000,000
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			

Para la integración e interoperabilidad con otras Entidades del Orden Nacional y Territorial, la Corporación dará cumplimiento a la normatividad del SINA, mejorará la eficiencia y eficacia en sus procesos, permitiendo la unificación de herramientas, la comunicación con otras Autoridades Ambientales y el cumplimiento de la estrategia de Gobierno Digital.

Tabla 82 Iniciativa de Transformación Digital y Modernización Tecnológica 07

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_07		
Nombre del Proyecto	Apoyo TIC al Teletrabajo.		
Objetivos del Proyecto	Implementar herramientas tecnológicas para el Teletrabajo.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$100,000,000
Prioridad de la Implementación	Alta Media **Baja**		
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			

Los Servidores Públicos de la Entidad reciben la posibilidad de trabajar en lugares distintos a su oficina (nuevas formas de trabajo) como una oportunidad para mejorar su calidad de vida y aumentar su rendimiento y productividad. Entre los beneficios específicos para ellos se encuentran:

- Ahorros en tiempos por desplazamientos entre hogar y oficina.
- Ahorros en dinero derivados de la disminución de desplazamientos, tangibles en la reducción de costos de combustible o pagos de transporte público.
- Reducción de la huella de carbono y el impacto ambiental producido por cada trabajador durante los desplazamientos y el consumo de energía en las oficinas.
- La utilización de tecnologías para facilitar la comunicación entre las partes sin necesidad de estar en un lugar físico determinado para cumplir sus funciones.
- Un modelo organizacional diferente al tradicional que replantea las formas de comunicación interna de la organización y en consecuencia genera nuevos mecanismos de control y seguimiento a las tareas.

Tabla 83 Iniciativa de Transformación Digital y Modernización Tecnológica 08

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_08			
Nombre del Proyecto	Tecnologías de las 4° Revolución Industrial.			
Objetivos del Proyecto	Implementar tecnologías de la IV y V Revolución Industrial (Sistemas de Inteligencia de Negocios, BigData, Analítica de Datos, Machine Learning, IoT, Robótica y Colaboración Abierta) que apoye la toma de decisiones y genere nuevo conocimiento en los procesos corporativos.			
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$400,000,000	
Prioridad de la Implementación	Alta	Media	**Baja**	
Responsables	Subdirección Administrativa y Financiera			

Descripción/Alcance

Implementación de soluciones que logren extraer información de distintos orígenes, detectando todos los documentos y procesos referentes a un tema de interés mediante la búsqueda inteligente de datos y el análisis de estos, sacando provecho de lo que ya se tiene (información interna) y poder correlacionar los diferentes tipos de datos para la toma de decisiones.

Implementación de Machine Learning o aprendizaje automático, es una forma de inteligencia artificial que le permite a un sistema aprender de los datos. La Corporación al recurrir al aprendizaje automático y a un modelo predictivo en sus planes y proyectos, logrará:

- Aumento en el volumen de datos e información útil para la toma de decisiones.
- Nuevos hábitos en la migración, transformación en integración de datos en proyectos analíticos.

Interconexión de dispositivos y objetos a través de una red (bien sea privada o Internet), dónde todos ellos podrían ser visibles e interaccionar, basados en las siguientes tendencias de tecnología:

FICHA DE PROYECTO

- Economías en la capacidad de cómputo.
- Avances en el análisis de datos.
- Computación en la nube.

Los procesos corporativos se deben automatizar y documentarse, con el fin de que el robot pueda ejecutar todas las acciones previstas, asegurando el cumplimiento de las reglas definidas y la disponibilidad de los datos existentes en un entorno digital.

Los proyectos colaborativos han logrado popularidad y abrir un espectro, donde se replantean los modelos internos de negocios y nuevas iniciativas abiertas y colaborativas. A partir de ahí se le permite a la comunidad aportar, así como también tienen la oportunidad de contribuir en las iniciativas de los demás. Consiste en una práctica que busca vincular a diferentes individuos o un grupo para trabajar por un interés común muchas veces relacionados a la innovación, resolución de problemas, eficiencia de procesos, generación de nuevas ideas; con frecuencia en un entorno online, contribuyendo con su conocimiento a nuevas ideas y soluciones, vínculos más fuertes con los consumidores, mejor posicionamiento, oportunidades de co-creación, optimización de tareas, reducción de costos, entre otros.

Tabla 84 Iniciativa de Transformación Digital y Modernización Tecnológica 09

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_09			
Nombre del Proyecto	Modelo Operativo de TI.			
Objetivos del Proyecto	Implementar el Modelo Operativo de Tecnologías de la Información y las Comunicaciones - Fortalecimiento de la capacidad operativa (Crear la Oficina de TIC).			
Tiempo Aproximado de Ejecución	4 años	**Costo de Implementación**	**$0**	
Prioridad de la Implementación	Alta	**Media**	Baja	

FICHA DE PROYECTO

Responsables	Subdirección Administrativa y Financiera

Descripción/Alcance

La Corporación debe realizar el entendimiento preciso, claro y documentado de la situación actual y objetivo de su modelo operativo que permita identificar los procesos, roles, actores y recursos que se habilitan en cada una de las capacidades institucionales.

Tabla 85 Iniciativa de Transformación Digital y Modernización Tecnológica 10

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_10		
Nombre del Proyecto	Sistema de Información con Enfoque Étnico y Participación Corporativa.		
Objetivos del Proyecto	Implementar sistemas de información y tecnologías enfocadas a las comunidades étnicas jurisdicción de la Corporación.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$500.000.000
Prioridad de la Implementación	**Alta** Media Baja		
Responsables	Subdirección Administrativa y Financiera		

Descripción/Alcance

Se cuenta con el levantamiento de requerimientos funcionales y no funcionales de la solución tecnológica, realizado conjuntamente con las comunidades y las dependencias participantes (Subdirecciones de Participación y Cultura Ambiental y de Planeación) y una primera versión del sistema étnico.

FICHA DE PROYECTO

El Sistema de Información Étnico servirá como apoyo a la toma de decisiones en asuntos relacionados a conflictos ambientales y socioambientales que permita generar reportes, informes y rutas de gestión en la jurisdicción de Corantioquia, al igual que posibilite una fuente de consulta en relación con mapas de actores, mapa de conflictos ambientales (mapa de calor), y caracterización de actores. Para el desarrollo de esta solución se determinará con la Dirección General y con las Subdirecciones de Participación y Cultura Ambiental y de Planeación el proceso de contratación más adecuado que permita su ejecución en el menor tiempo posible.

Tabla 86 Iniciativa de Transformación Digital y Modernización Tecnológica 11

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_11		
Nombre del Proyecto	Modernización Física del Data Center.		
Objetivos del Proyecto	Disponer de las apropiaciones presupuestales necesarias con el fin de modernizar el Data Center de la Corporación de conformidad con la norma ANSI/TIA 942, Telecommunications Infrastructure for Data Centers Standard, ANSI/BICSI 002-2014.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$580.000.000
Prioridad de la Implementación	Alta	**Media**	Baja
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			

Optimización del Centro de Datos (Datacenter) conforme a las normas ANSI/TIA 942, Telecommunications Infrastructure for Data Centers Standard, ANSI/BICSI 002-2014 y las siguientes características fundamentales:

- Nomenclatura estándar.

FICHA DE PROYECTO

- Funcionamiento a prueba de fallos.
- Aumento de la protección frente a agentes externos.
- Fiabilidad a largo plazo, mayores capacidades de expansión y escalabilidad.
- Porcentaje de disponibilidad de 99.671% conforme al Nivel de Fiabilidad TIER 1.

Tabla 87 Iniciativa de Transformación Digital y Modernización Tecnológica 12

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_12		
Nombre del Proyecto	Sistema de Información de Requerimientos e Incidentes.		
Objetivos del Proyecto	Realizar la adquisición, instalación, configuración, pruebas, puesta en funcionamiento y soporte de solución para la gestión de requerimientos e incidentes y gestión de inventarios tecnológicos.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$200.000.000
Prioridad de la Implementación	Alta	Media	**Baja**
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			
Sistema de información que permita el registro, control, gestión, solución, seguimiento y evaluación a las diferentes incidencias tecnológicas u otros proyectos, presentados o requeridos por los usuarios internos y externos, contando con diferentes canales de atención.			

Tabla 88 Iniciativa de Transformación Digital y Modernización Tecnológica 13

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_13		
Nombre del Proyecto	Actualización del licenciamiento y acuerdo de soporte de la solución de firewall de la Corporación.		
Objetivos del Proyecto	Realizar la adquisición de equipos y renovación del licenciamiento y acuerdo de soporte de la solución firewall de la Corporación por tres (3) años.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$ 1,470,000,000
Prioridad de la Implementación	**Alta** Media Baja		
Responsables	Subdirección Administrativa y Financiera		
Descripción/Alcance			
Suministro del licenciamiento que permita el uso y soporte de la solución firewall para la Corporación, incluyendo renovación y servicios profesionales con personal certificado por el fabricante para la adquisición de equipos, con el fin de garantizar la protección de la seguridad perimetral de la red de voz y datos corporativa y los servicios tecnológicos y usuarios en la navegación web, entre otros.			

Tabla 89 Iniciativa de Transformación Digital y Modernización Tecnológica 14

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_14
Nombre del Proyecto	Firma Electrónica y Digital.
Objetivos del Proyecto	Realizar la adquisición, instalación, configuración, pruebas, puesta en funcionamiento y soporte de una solución web para firma digital de documentos, con certificados de firma digital y sus respectivos tokens.

FICHA DE PROYECTO

Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$1.600.000.000
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		

Descripción/Alcance

Se cuente con estándares de seguridad robustos que permitan realizar el proceso de gestión documental de la Entidad y permitir a la Corporación estar a la vanguardia en últimas tecnologías aumentando la productividad y buen desempeño de sus Servidores Públicos, sus procesos misionales, planes, programas, proyectos metodologías y estrategias, contribuyendo a fortalecer y mejorar los servicios tecnológicos que presta la Corporación a los usuarios internos y externos.

Tabla 90 Iniciativa de Transformación Digital y Modernización Tecnológica 15

FICHA DE PROYECTO

Id del Proyecto	INI_TMOD_15		
Nombre del Proyecto	Adquisición e implementación de un software de gestión documental.		
Objetivos del Proyecto	Modernizar el manejo documental de la Corporación, mediante un sistema informático que contenga los componentes de un sistema de gestión documental.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$1.300.000.000
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección Administrativa y Financiera		

Descripción/Alcance
Aplicación informática de última generación, para Web y móvil que permita el manejo integral de la información y documentación de la entidad, desde su producción hasta su disposición integrando tecnologías de workflow, firmas digitales y protocolos de gestión documental como son: TRD, índices de expedientes (hojas de control), tiempos de retención, expedientes electrónicos, prestamos documentales entre otras.

Tabla 91 Iniciativa de Transformación Digital y Modernización Tecnológica 16

FICHA DE PROYECTO			
Id del Proyecto	INI_TMOD_16		
Nombre del Proyecto	Diseño e implementación del Centro de Monitoreo Ambiental.		
Objetivos del Proyecto	Acompañar la estructuración del diseño del Centro de Monitoreo Ambiental para la administración integral del territorio, en la jurisdicción de la Corporación Autónoma Regional del Centro de Antioquia.		
Tiempo Aproximado de Ejecución	4 años	**Costo Aproximado de Implementación**	$ Por definir
Prioridad de la Implementación	**Alta**	Media	Baja
Responsables	Subdirección de Planeación y Subdirección Administrativa y Financiera		

Descripción/Alcance
A través del Contrato 090-CNT2409-171 suscrito con la Corporación Interuniversitaria de Servicios (CIS) se está realizando el acompañamiento de la estructuración del diseño del Centro de Monitoreo Ambiental para la administración integral del territorio, en la jurisdicción de la Corporación Autónoma Regional del Centro de Antioquia. Este

contrato determinará el alcance, fases y costo de implementación del Centro de Monitoreo.

Los entregables del mencionado contrato son:

Alcance 1: Plan de Trabajo y cronogramas de actividades detallado, de acuerdo al objeto contractual.

Alcance 2: Levantamiento de requerimientos funcionales y no funcionales, los cuales deberán contener los puntos relacionados en el formato F-TIC -01 del SGI implementado en Corantioquia “Levantamiento de requerimientos de software”.

Alcance 3: Diagnóstico integral de acuerdo con el levantamiento de requerimientos, en el cual se deberán analizar cada uno de los elementos establecidos por la Corporación, y con estos, entregar las respectivas recomendaciones y conclusiones, incluyendo la entrega del Marco de Referencia de Arquitectura Empresarial alineado al diseño del centro de monitoreo.

Alcance 4: Elaboración del Diseño del Centro de Monitoreo.

Alcance 5: Formulación y estructuración del proyecto: diseño e implementación del Centro de Monitoreo en la Metodología General ajustada (MGA) del Departamento Nacional de Planeación de la República de Colombia.

9 Líneas de acción para la mitigación del riesgo

La ejecución del Plan está sujeta a riesgos y oportunidades del entorno las cuales se relacionan en la

Tabla 92 Gestión de riesgos para la ejecución del Plan.

DESCRIPCIÓN RIESGO	AMENAZA
Incumplimiento de las políticas de seguridad de la información por parte los funcionarios y colaboradores	Usuarios mal intencionados o por desconocimiento de la seguridad de la información ocasionan pérdida parcial o total de la información.

poniendo en riesgo la continuidad de las operaciones, servicios y/o sistemas de la Corporación	
Acceso no autorizado a sistemas y servicios, o abuso de privilegios de funcionarios o contratistas sobre los sistemas o servicios que están bajo su responsabilidad.	Acciones indebidas de los funcionarios o contratistas con privilegios de acceso (Usuarios mal intencionados o con desconocimiento de los procesos, procedimientos y/o políticas de la Entidad)
Ausencia de requisitos de seguridad de la información en los contratos suscritos con proveedores y contratistas.	Fuga de información Divulgación de procedimientos o información sensible o crítica Configuración por default de componentes tecnológicos

Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnológica.	Incendio, inundación, terremoto, polvo Funcionarios con acceso a Datacenter, inconformes y/o sin conocimientos en seguridad de la información Códigos maliciosos Proveedores tecnológicos Ciberdelincuentes Ataques terroristas Disturbios civiles Interrupción de los servicios de la entidad y página web Indisponibilidad de la plataforma tecnológica Indisponibilidad del fluido eléctrico continuo en el centro de datos y PCs Indisponibilidad de los equipos de protección contra incendios en caso de emergencia

Riesgos de navegación de usuarios, privilegios de descarga e instalación y uso de software en los sistemas operativos de los equipos de cómputo y servidores	Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generado por virus informáticos. Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso
Afectación de equipos informáticos (equipos de cómputo, servidores, equipos de comunicaciones, seguridad, dispositivos móviles) ocasionado por conexiones de dispositivos de medios extraíbles, ejecución de enlaces, o archivos adjuntos, etc.	Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generado por virus informáticos. Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso

Pérdida, alteración o sustracción de Información en medio magnético o físico, dada en custodia al proveedor de Backup's o los usuarios	Funcionarios/contratistas, Proveedores externos, Ciberataques, servicios de suministro, amenazas naturales
Pérdida de la información generada por las actividades propias de la gestión del proceso - Copias de respaldo / restauración	Afectación en la disponibilidad del respaldo de la información Insuficiencia de espacio o almacenamiento para el aseguramiento de la información Pérdida o corrupción de los datos Corrupción de las cintas en el momento de las copias y la restauración del Backups Inexistencia de Backup de la información misional y de gestión

Ataques informáticos internos/externos a la infraestructura tecnológica (páginas web, software misional, hardware, aplicaciones, equipos de comunicación, equipos de seguridad, red interna)	Indisponibilidad de los servicios y/o página web Administradores de tecnología sin conocimientos técnicos de seguridad de la información. Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la plataforma tecnológica Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso
Indisponibilidad del canal de comunicación (internet, intranet)	Falla en el suministro de energía Fallas en los servicios ofrecidos por el proveedor

Gestión y uso inadecuado de las contraseñas	Usuarios sin conocimiento de las políticas, manual y procedimientos de seguridad de la información
Acceso no autorizado a las redes de la entidad (interna y externa)	Red sin protección, sin las herramientas o equipos tecnológicos de comunicación que aseguren al usuarios su correcto funcionamiento Fuga de información debido al acceso de usuarios no autorizados a la infraestructura de red de la entidad. Indisponibilidad del servicio de la red inalámbrica debido a ataques de denegación de servicios (DoS). Suplantación de identidad para acceder a los aplicativos tecnológicos de la entidad que se encuentran disponibles a través de la red de datos. Funcionarios descontentos pueden hacer uso de usuarios y contraseñas de personal que ya no labora en la entidad para visualizar y/o sustraer información confidencial de la entidad.

Acceso no autorizado a información enviada mediante mensajería electrónica	Fuga y/o pérdida de información Divulgación no autorizada de información debido a acceso de terceros Secuestro de información generado por una aplicación ramsomware.
Interceptación de información en tránsito provocada por una pérdida de la confidencialidad	Usuarios mal intencionados, Atacantes, Códigos maliciosos
Alteración, suplantación, divulgación y/o uso mal intencionado de la información sensible para la Entidad.	Funcionarios y/o Contratistas inconformes Atacantes externos,
Incumplimiento de la legislación y procedimientos vigentes	Funcionarios con desconocimiento en temas de contratación de personal Cambios en las regulaciones y lineamientos del gobierno que puedan impactar las operaciones de la Corporación Insuficiente protección y privacidad de información personal

Pérdida de la confidencialidad, integridad y disponibilidad de la información cifrada	Robo o hurto de información catalogada como sensible por falta de implementación de herramientas que aseguren el transporte de la información por la red Acceso a información privada, reservada o sensible sin la debida autorización.
Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia	Funcionarios con roles de seguridad de la información sin conocimiento Interrupción completa en la continuidad del negocio (Daño en Data Center, Servicios Tecnológicos y pérdida de la Información) Los usuarios realizan trabajo en casa, manipulan información, acceden a los sistemas de información desde las conexiones establecidas en el hogar Practicas inapropiada que afecten la disponibilidad de la información y la plataforma tecnológica
Indisponibilidad de los recursos tecnológicos ocasionada por una inadecuada gestión a la capacidad (procesamiento, almacenamiento, memoria)	Ausencia de revisiones periódicas por parte de los administradores de los recursos de la infraestructura tecnológica

Perdida de confidencialidad, integridad de la información en la ejecución de proyectos relacionados con la adquisición de bienes o servicios por parte del GIT Apoyo informático	Filtración y manipulación de la información para beneficio de un tercero
Perdida de confidencialidad, integridad y disponibilidad durante el ciclo de desarrollo en los sistemas de información ya sean nuevos o existentes - Acceso no autorizado a los códigos fuente y ambientes de desarrollo	Proveedores de sistemas de información, funcionarios con roles de desarrollo que no cumplen las políticas y requerimientos en seguridad Manipulación intencionada interna o externa de las fuentes de información ocasionando pérdida parcial y/o total del código fuente Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. Indisponibilidad de acceso a los repositorios de información o herramienta donde se resguarda el código fuente Secuestro de la información relacionada con el código fuente efectuado por un tercero a través de un malware Ataques cibernéticos sobre las plataformas desarrolladas internamente
Cambios en los sistemas de información gestionados inadecuadamente	Usuarios y administradores sin conocimiento de las políticas y procedimientos de seguridad de la información

Nota. Elaboración propia

10 Presupuesto

Las acciones definidas en el presente programa se articularán con los programas y proyectos del Plan de Acción 2024-2027 de la Corporación, garantizando así la disponibilidad de los recursos, incluyendo los presupuestales para su ejecución.

Tabla 93 Tabla Presupuesto Iniciativa de Operación

INICIATIVAS DE OPERACION			
Id Iniciativa	**Objetivos de la Iniciativa**	**Prioridad para la Implementación**	**Costo Aproximado de Implementación 2024-2027**
INI_OPE_01	Mejorar la conectividad en los diferentes centros de trabajo (Sede Central, Oficinas Territoriales, Viveros y CAV).	Alta	$ 1,820,000,000
INI_OPE_02	Capacitar al personal de la Corporación en el uso y apropiación de las TIC, sistemas de información, herramientas, licencias y Moodle.	Alta	$ 0
INI_OPE_03	Fortalecer el Modelo de Atención al Ciudadano a través de la implementación de asesores virtuales.	Alta	$ 30,000,000
INI_OPE_04	Actualizar la página web e intranet de la Corporación según la norma técnica NTC 5854 y lineamientos del MinTIC.	Alta	$ 100,000,000
INI_OPE_05	Facilitar el acceso a la información de las bases de datos bibliográficas a los usuarios internos y externos.	Alta	$ 76,000,000

INI_OPE_06	Actualizar el Visor Geográfico de la Corporación, con su respectivo soporte y mantenimiento.	Alta	$ 347,000,000
INI_OPE_07	Actualizar licencias ArcGis, con su respectivo soporte y mantenimiento	Alta	$ 765,000,000
INI_OPE_08	Actualización, soporte y mantenimiento de los módulos del Sistema de Información Administrativo, Financiero, Contable y Fiscal.	Alta	$ 1,693,202,880
INI_OPE_09	Realizar el soporte y mantenimiento de las aplicaciones Sirena y Laboratorio.	Alta	$ 1,500,000,000
INI_OPE_10	Prestar los servicios especializados que garanticen el buen funcionamiento de la Infraestructura Informática y de Telecomunicaciones de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA, que incluya el servicio de Mesa de Ayuda para mejorar la prestación de los servicios tecnológicos de la Corporación.	Alta	$ 2,756,000,000

INI_OPE_11	Realizar el mantenimiento preventivo y correctivo a equipos de cómputo (todo en uno, portátiles y estaciones de trabajo), y tecnológicos y periféricos tales como, impresoras, plotter, escáneres, video proyectores, datamax, accesorios y/o equipos de telecomunicaciones de la Entidad.	Alta	$ 825,000,000
INI_OPE_12	Contar con el licenciamiento necesario para el correcto funcionamiento y disponibilidad de las aplicaciones corporativas.	Alta	$ 7,096,000,000
			$ 17,008,202,880

Tabla 94 Presupuesto Iniciativa de Transformación Digital y Modernización Tecnológica

INICIATIVAS DE TRANSFORMACIÓN DIGITAL Y MODERNIZACIÓN TECNOLÓGICA			
Id Iniciativa	**Objetivos de la Iniciativa**	**Prioridad para la Implementación**	**Costo Aproximado de Implementación 2024-2027**
INI_TMOD_01	Implementar un Sistema de Información en la Administración de los Recursos Naturales, para la Corporación Autónoma Regional del Centro de Antioquia - Corantioquia. (incluye Software como Servicio).	Alta	$ 1,600,000,000
INI_TMOD_02	Migrar la Infraestructura Tecnológica de la Corporación a servicios de nube e híbrida (incluye migración de la infraestructura informática y de telecomunicaciones, sistemas de almacenamiento, sistemas de backups) según los lineamientos del MinTIC y la Directiva Presidencial 03 de 2021.	Alta	$ 4,286,844,564
INI_TMOD_03	Adquirir y renovar equipos tecnológicos de última generación de acuerdo con las necesidades de los procesos.	Media	$ 1,600,000,000

INI_TMOD_04	Implementar tecnología de punta en el ejercicio de la autoridad ambiental y gestión de territorios sostenibles: equipos móviles (GPS, drones, entre otros) y aplicaciones.	Media	$ 270,000,000
INI_TMOD_05	Actualizar e implementar el Modelo de Seguridad y Privacidad de la Información, que incluyan la formulación del Plan de Seguridad y Privacidad de la Información, Plan de Continuidad de TI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Comunicaciones de TI.	Alta	$ 0

INI_TMOD_06	Transformar la experiencia de los ciudadanos con los trámites y servicios por medios electrónicos, asegurando la promoción, la efectividad y la simplicidad (Interoperabilidad de las aplicaciones corporativas de carácter estratégica, misional y de apoyo con otras Entidades del Estado Nacionales y Territoriales), de conformidad con el nuevo el nuevo Modelo de Gestión y Operación de Administración de los Recursos Naturales Renovables.	Alta	$ 300,000,000
INI_TMOD_07	Implementar herramientas tecnológicas para el Teletrabajo.	Baja	$ 100,000,000

INI_TMOD_08	Implementar tecnologías de la IV y V Revolución Industrial (Sistemas de Inteligencia de Negocios, BigData, Analítica de Datos, Machine Learning, IoT, Robótica y Colaboración Abierta) que apoye la toma de decisiones y genere nuevo conocimiento en los procesos corporativos.	Baja	$ 400,000,000
INI_TMOD_09	Implementar el Modelo Operativo de Tecnologías de la Información y las Comunicaciones - Fortalecimiento de la capacidad operativa (Crear la Oficina de TIC).	Media	$ 0
INI_TMOD_10	Implementar sistemas de información y tecnologías enfocadas a las comunidades étnicas jurisdicción de la Corporación.	Alta	$ 500,000,000

INI_TMOD_11	Disponer de las apropiaciones presupuestales necesarias con el fin de modernizar el Data Center de la Corporación de conformidad con la norma ANSI/TIA 942, Telecommunications Infrastructure for Data Centers Standard, ANSI/BICSI 002-2014.	Media	$ 580,000,000
INI_TMOD_12	Realizar la adquisición, instalación, configuración, pruebas, puesta en funcionamiento y soporte de solución para la gestión de requerimientos e incidentes y gestión de inventarios tecnológicos.	Baja	$ 200,000,000
INI_TMOD_13	Realizar la adquisición de equipos y renovación del licenciamiento y acuerdo de soporte de la solución firewall de la Corporación por tres (3) años.	Alta	$ 1,470,000,000

INI_TMOD_14	Realizar la adquisición, instalación, configuración, pruebas, puesta en funcionamiento y soporte de una solución web para firma digital de documentos, con certificados de firma digital y sus respectivos tokens.	Alta	$ 1,600,000,000
INI_TMOD_15	Modernizar el manejo documental de la Corporación, mediante un sistema informático que contenga los componentes de un sistema de gestión documental.	Alta	$ 1,300,000,000
INI_TMOD_16	Diseño e implementación del Centro de Monitoreo Ambiental.	Alta	$ Por definir
		Total del Presupuesto	**$ 14,206,844,564**

Tabla 95 Presupuesto total

Nombre del proyecto	Precio
Presupuesto iniciativas de transformación digital y modernización tecnológica	$ 17,008,202,880
Presupuesto iniciativas de operación	$ 14,206,844,564
Total	$ 31,215,047,444

Nota: Para la valoración del costo de las iniciativas de operación y de transformación digital y modernización tecnológica, se tuvieron en cuenta: Contratos ejecutados por la Corporación, Índice de Precios al Consumidor – IPC y Tasa Representativa del Mercado – TRM.

11 Seguimiento al plan

El PETIC 2024-2027 se diseñó bajo la premisa de dar cumplimiento a los Dominios de TI propuestos en el Modelo de Gestión y Gobierno de TI (MGGTI) del Marco de Referencia de Arquitectura Empresarial del MinTIC (Estrategia de TI, Gobierno de TI, Gestión de Sistemas de Información, Gestión de Información, Gestión de Servicios de TI, Uso y Apropiación de TI); enfoques que sirvieron de insumo para formular las 28 Iniciativas, las cuales están conformadas por 12 de Operación y 16 de Transformación Digital y Modernización Tecnológica, entendidos estos como el conjunto de los proyectos requeridos para dar respuesta a las necesidades en materia de tecnología de la Corporación; para aportar al logro del objetivo del plan, aportando al seguimiento y control del ejercicio de la autoridad ambiental.

El seguimiento y evaluación al PETIC, se realizará conforme al cumplimiento de las metas definidas para cada una de las Iniciativas, las cuales aportarán al cumplimiento de los Dominios de TI, con las cuales están relacionadas; el cumplimiento de estos Dominios previamente ponderados dará como resultado la evaluación del PETIC.

Así pues, el proceso de seguimiento y evaluación permite contar con información objetiva y oportuna de utilidad para: tomar acciones que permitan mejorar la Gestión de TI orientada a la consecución de resultados.

El avance del PETIC se evaluará semestralmente, el cual se alimenta del seguimiento trimestral que se realiza a la ejecución de cada una de las Iniciativas de Operación y Transformación Digital y Modernización Tecnológica, enmarcadas en el comportamiento de la ejecución de los contratos y convenios asociados a TI que la Corporación suscribe,

teniendo en cuenta su articulación con el Plan de Gestión Ambiental Regional, Plan de Acción y con el Presupuesto Anual de Rentas y Gastos.

Estos informes serán presentados al Comité Directivo y serán difundidos al interior de la Corporación.

Como instancias de seguimiento, se tendrá el Comité de Dirección de CORANTIOQUIA, que realizará monitoreo permanente para analizar los avances en la ejecución de las Iniciativas de TI.

El resultado del PETIC y las Iniciativas que lo conforman, se interpretará de conformidad con los siguientes rangos de evaluación:

Nivel de ejecución (N.E) deficiente	Nivel de ejecución (N.E) aceptable	Nivel de ejecución (N.E) sobresaliente
N.E < 75 %	75 % ≤ N.E ≤ 90 %	90 % < N.E ≤ 100 %

Figura 24 Seguimiento al plan -Nivel de ejecución

12 Referencias

Acuerdo Consejo Directivo 575. (diciembre de 2019). por el cual se aprueba el Plan de Gestión Ambiental Regional PGAR 2020-2031. (Corantioquia, Ed.) Medellín, Antioquia, Colombia: Consejo Directivo.

Consejo Directivo. (19 de mayo de 2016). Plan de Acción 2016-2019. Medellín, Antioquia, Colombia: Corantioquia.

Decreto 612. (4 de abril de 2018). Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. Bogotá, D.C., Colombia: Presidencia de la República.

DNP. (2014). Guía metodológica para el Seguimiento y la Evaluación a Políticas Públicas. (D. d. Públicas, Ed.) Bogotá, D.C., Colombia: Departamento Nacional de Planeación.

Función Pública. (agosto de 2019). Valores del servicio público. Código de intedridad. Bogotá, D.C., Colombia: Departamento Administrativo de la Función Pública.

Resolución 040-RES2010-5718. (7 de octubre de 2020). Por medio de la cual se actualiza la política del sistema de gestión integral (SGI) de la Corporación Autónoma Regional del Centro de Antioquia (Corantioquia). Medellín, Antioquia, Colombia: Corantioquia.

Resolución n.° 040-RES1801-405. (31 de enero de 2018). Por la cual se aprueba y adopta el Plan Anticorrupción y de Atención al Ciudadano para el año 2018. Medellín, Antioquia, Colombia: Corantioquia.

Resolución n.° 040-RES2112-9588. (31 de diciembre de 2021). Por la cual se adopta el código de integridad corporativo. Medellín, Antioquia, Colombia: Corantioquia.

SINA. (2018). Plan de Acción Sectorial Ambiental del Mercurio. Bogotá, D.C., Colombia.

13 Anexos

Información de apoyo al plan, tales como tablas, gráficos, diagramas de flujo, etc. Para el diseño de la estructura programática, utilice el siguiente formato:

F-PPO-32_Anexo_plan.xlsx

13.1 Estructura programática

Ver estructura programática en archivo de Excel.

Liliana María Taborda González
Directora General
Corporación Autónoma Regional del Centro de Antioquia

2024-12-26

Aprobado y adoptado mediante Resolución n.° xxx

TABLA DE CONTENIDO

CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

Presentación

La Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA dando alcance al cumplimiento del 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 de la Información" de la Política de Gobierno Digital; así mismo el Decreto 1499 de 2017 determina el cumplimiento institucional de las Políticas de Gobierno y Seguridad Digital en relación con el habilitador "Seguridad de la Información" conforme a la Resolución 500 de 2021 (MinTIC) y la Política de Seguridad Digital acorde con los lineamientos de los documentos CONPES 3701 de 2011 Lineamiento de Políticas de Ciberseguridad y Ciberdefensa, CONPES 3854 de 2016 Política Nacional de Seguridad Digital, CONPES 3975 de 2019 Política Nacional para la Transformación Digital e Inteligencia Digital, CONPES 3995 de 2020 Política Nacional de Confianza y Seguridad Digital.

Por otra parte, La Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA ha implementado la política de protección de datos personales, aprobada mediante resolución 040-RES2411-5277 del 28 de noviembre de 2024, conforme a las disposiciones de la resolución Ley 1581 de 2012 "por la cual se dictan disposiciones generales para la protección de datos personales", atendiendo los lineamientos de la Ley 1712 de 2014; y acoge en sus procesos el marco normativo y regulatorio de la entidad relacionada con la Seguridad y Privacidad de la Información (SPI).

De acuerdo con lo anterior, se define el Plan de Seguridad y Privacidad de la Información para la vigencia 2024-2027, en el marco del Plan de Gestión Ambiental Regional 2020 – 2031 "Un Plan Intergeneracional", y la Resolución 040-RES2010-5756 - Política General de Tecnología, de Seguridad y Privacidad de la Información que se constituyen en instrumentos de planificación que orientan la ruta de acción en materia de seguridad de la información.

1 Elementos estratégicos corporativos

1.1 Misión

Contribuir al logro del desarrollo sostenible, mediante el conocimiento y mejoramiento de la oferta ambiental y la administración del uso de los recursos para responder a su demanda, a través de la construcción de una cultura ambiental del territorio (Consejo Directivo, 2016)

1.2 Visión ambiental para el desarrollo regional

En 2031 los 80 municipios del centro de Antioquia forman un territorio sostenible en el que se protege el patrimonio ambiental biodiverso, se desarrollan actividades económicas en armonía con la madre tierra y sus actores regionales son corresponsables en la conservación de la diversidad biológica, étnica y cultural, y el respeto a la dignidad humana, para el buen vivir de las generaciones presentes y futuras. (Acuerdo Consejo Directivo 575, 2019)

1.3 Política de administración del riesgo

La Corporación Autónoma Regional del Centro de Antioquia - Corantioquia, es una organización de alto desempeño en la administración de los recursos naturales renovables, que tiene como misión contribuir al logro del desarrollo sostenible, comprometida con la satisfacción de las necesidades de la comunidad; asimismo, buscará la eficacia de las acciones formuladas a través del cumplimiento de los requisitos legales, los sistemas de gestión corporativos, transparencia en el acceso de los servicios, manejo adecuado de la información y el fortalecimiento de la cultura organizacional, mediante las relaciones establecidas entre las partes interesadas, con el fin de monitorear y controlar los posibles riesgos (Registro F-PPO-20 Mapa Riesgos y Oportunidades).

1.4 Código de integridad

Mediante Resolución (Resolución n.° 040-RES2112-9588, 2021) se adoptó el Código de Integridad Corporativo como guía, sello e ideal de cómo deben ser y obrar los servidores públicos y todos aquellos colaboradores de la administración que prestan sus servicios en la corporación, con el fin de cumplir con la misión, la visión y los objetivos institucionales dentro del marco de integridad y legalidad.

El Código de Integridad Corporativo reúne los valores de honestidad, respeto, compromiso, diligencia, justicia, servicio y resultados.

a) **Honestidad.** Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia, rectitud y siempre favoreciendo el interés general. (Función Pública, 2019)
b) **Respeto.** Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición. (Función Pública, 2019)

c) **Compromiso.** Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar. (Función Pública, 2019)
d) **Diligencia.** Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos del Estado. (Función Pública, 2019)
e) **Justicia.** Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación. (Función Pública, 2019)
f) **Servicio.** Sirvo y atiendo las necesidades de los ciudadanos, poniendo a disposición mis capacidades y anteponiendo los máximos fines del Estado a cualquier propósito o interés particular.
g) **Resultados.** Tengo claridad frente al rol que desempeño, el empoderamiento individual respecto a los objetivos y la generación de resultados.

El Código de Integridad proporciona el marco ético y de valores que guía la implementación del Plan de Seguridad y Privacidad de la Información para la vigencia 2024-2027.

La relación entre el Código de Integridad y el Plan de Seguridad y Privacidad de la Información 2024-2027 es fundamental para asegurar que las acciones y decisiones tecnológicas de la Corporación se alineen con principios éticos, de transparencia y de manera responsable.

1.5 Política del SGI

Corantioquia es una entidad pública, encargada de administrar el patrimonio ambiental de los 80 municipios de su jurisdicción, enfocada al cumplimiento de los requisitos legales y reglamentarios; la generación de valor público y la satisfacción de los actores del territorio; el mejoramiento continuo del SGI y sus procesos; a la participación de los actores del territorio; el fortalecimiento de la cultura organizacional y ambiental; la prevención de la contaminación y la protección del ambiente; la gestión de los riesgos y oportunidades organizacionales y el bienestar de los servidores públicos, contratistas, subcontratistas, visitantes, participantes en eventos corporativos y actores viales; contribuyendo así al desarrollo sostenible. (Resolución 040-RES2408-3589).

2 Articulación con instrumentos de planificación

2.1 Articulación con el PGAR 2020-2031

El Plan de Seguridad y Privacidad de la Información 2024-2027 está alineado al Plan de Gestión Ambiental Regional 2020-2031 a través del Capítulo 5 “Línea estratégicas del PGAR“, Línea 4 “Fortalecimiento de la cultura ambiental y de las capacidades de los actores para la gestión conjunta y el logro de los resultados”, Objetivo 4 “Generar la gobernanza que permita consolidar el escenario de sostenibilidad ambiental de la jurisdicción” , Componente 13 “Institucionalidad fortalecida para una gestión ambiental corresponsable , Componente 15 “ la gestión de la información y el conocimiento investigación + Desarrollo + Innovación” , Componente 18 ”Incidencia institucional para una eficiente coordinación y cooperación con las autoridades étnicas en materia de gestión ambiental” , Retos : 30, 35, 36, 37 y 49.

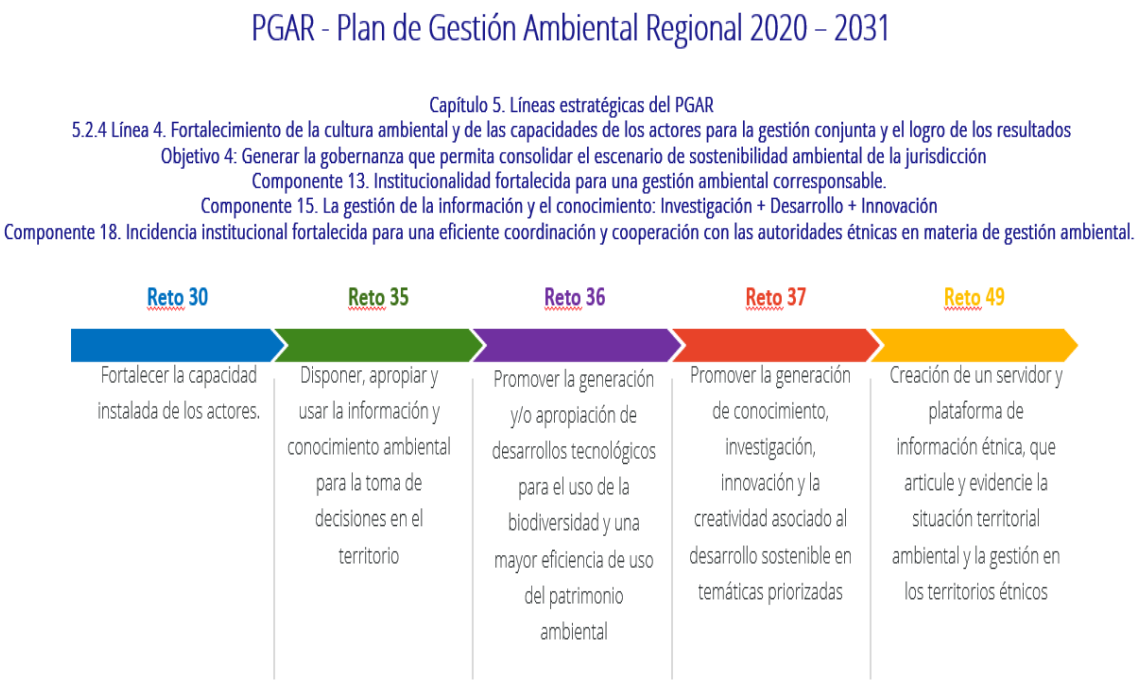


Figura 1 Articulación de la Seguridad y Privacidad de la Información con los retos y Componentes 13, 15 y 18 del PGAR 2020 – 2031

Fuente Elaboración Propia

Nota. Tomado de PGAR 2020-2031 (Acuerdo Consejo Directivo 575, 2019)

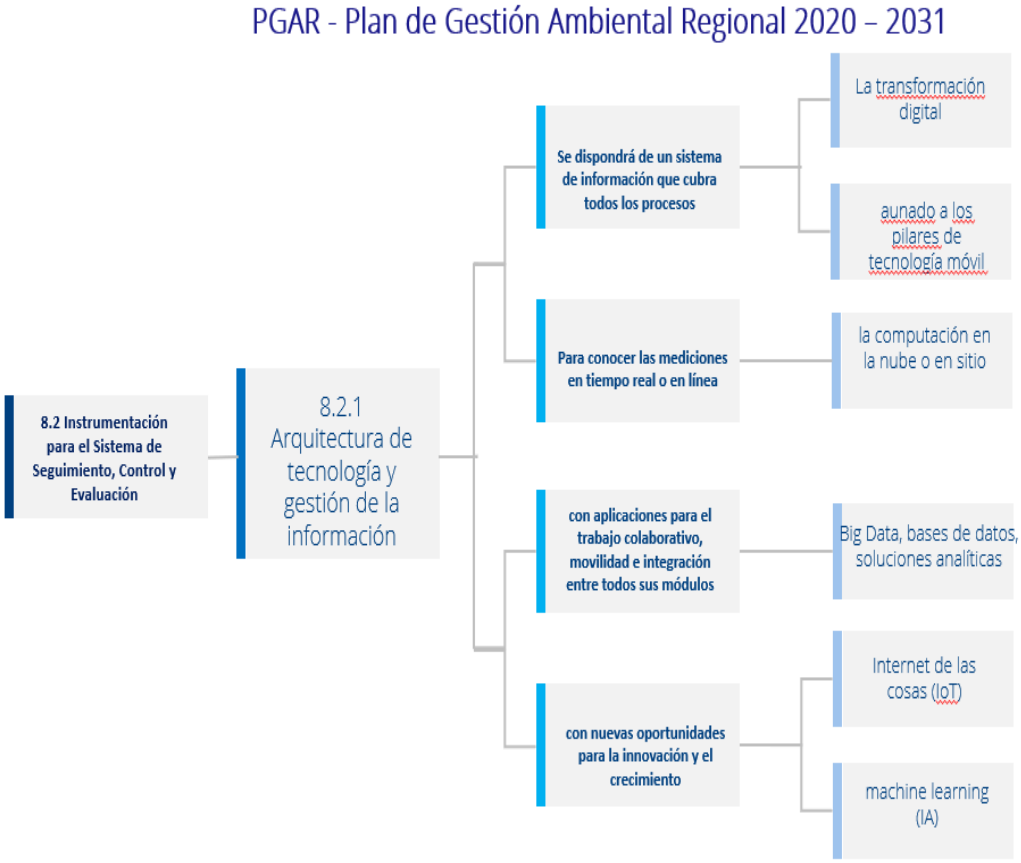


Figura 2 Articulación de la Seguridad y Privacidad de la Información con las tecnologías relacionadas en el instrumento de Planificación PGAR 2020 – 2031

Fuente Elaboración Propia a Partir del PGAR 2020 – 2031

2.2 Articulación con el Plan de Acción 2024-2027

El Plan de Seguridad y Privacidad de la Información 2024-2027 está alineado al Plan de acción 2024-2027 a través del programa 5 “Conexión Institucional “dentro el cual se encuentra el proyecto 5.3 denominado “Gestión de la Información para la toma de decisiones en la gestión ambiental”, dentro de los cuales se encuentra 3 actividades que son:

- **Actividad 5.3.1**. Diseño del Centro de Monitoreo para la administración integral del territorio con énfasis en el recurso agua. (*Indicador: Centro de monitoreo diseñado*).

- **Actividad 5.3.2.** Implementación del Centro de Monitoreo para la administración integral del territorio con énfasis en el recurso agua.
  (***Indicador:*** *Porcentaje de Avance en el levantamiento de los requerimientos, diagnóstico e implementación integral de las plataformas institucionales.*

Indicador: *Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027.*
Indicador: *Porcentaje de avance de la formulación e implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información*
Indicador: *Porcentaje de avance de la formulación e implementación del Plan de Seguridad y Privacidad de la Información.*
Indicador: *Porcentaje de avance en el diagnóstico integral e implementación de soluciones a las necesidades interoperabilidad*
Indicador: *Porcentaje de avance de las actividades priorizadas anualmente para la implementación del Centro de Monitoreo).*

- **Actividad 5.3.3.** Articulación del centro de monitoreo con otras entidades del Sistema Nacional Ambiental – SINA En el marco de Sistema de información para Colombia – SIAC. (*Indicador: % de avance de las actividades priorizadas anualmente para la interoperabilidad del Centro de Monitoreo)*

2.3 Articulación con otros instrumentos de planificación

La Corporación dispone de diferentes Instrumentos de Planificación (Estratégica, Temática o Misional, Institucional o de Gestión y Desempeño), los cuales incorporan diferentes estrategias para el logro de su propósito articuladas con asuntos de las TIC, que requieren en primer lugar ser identificadas y en segundo lugar articuladas con el Plan de Seguridad y Privacidad de la Información 2024-2027:

1. **Planes Temáticos o Misionales:** Corresponden a los planes que se desarrollan en el marco de la sostenibilidad del territorio de la Jurisdicción, los cuales disponen de normativa específica para su formulación, seguimiento y actualización:

    - + Aire Puro.
    - Plan de Ordenación Forestal.
    - Plan Regional de Cambio Climático.
    - Plan de Manejo de Acuíferos.
    - Plan de Manejo de Áreas Protegidas.
    - Planes de Manejo de Microcuencas.
    - Planes de Ordenación y Manejo de Cuencas Hidrográficas.
    - Planes de Ordenamiento del Recurso Hídrico.
    - Plan de Negocio Asociativo en Turismo de Naturaleza.
    - Plan de Conservación y Manejo de Especies Priorizadas de Flora.
    - Plan de Conservación y Manejo de Especies Priorizadas de Fauna.

2. **Planes de Gestión y Desempeño:** Corresponden a los Planes Institucionales y Estratégicos que establece el Decreto 612 de 2018, los cuales se deben actualizar anualmente a más tardar el 31 de enero de cada vigencia e integrar al

Plan de Acción de la Corporación, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión (MIPG):

- Plan Institucional de Archivos de la Entidad -PINAR.
- Plan Anual de Adquisiciones.
- Plan Anual de Vacantes.
- Plan de Previsión de Recursos Humanos.
- Plan Estratégico de Talento Humano.
- Plan Institucional de Capacitación.
- Plan de Incentivos Institucionales.
- Plan de Trabajo Anual en Seguridad y Salud en el Trabajo.
- Programa de Transparencia y Ética Pública (PTEP).
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI.
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Plan de Apertura de datos.

La articulación entre los planes misionales, los Planes de Gestión y Desempeño y el Plan de Seguridad y Privacidad de la Información es esencial para asegurar que las iniciativas transformación digital y modernización tecnológica apoyen directamente los objetivos fundamentales de la Corporación que impactarán la gestión corporativa.

3 Objetivos

3.1 Objetivo general

Definir las medidas, actividades y controles necesarios para adelantar la gestión de la seguridad y privacidad de la información (SPI) de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información, la norma ISO NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad de la operación de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA para asegurar la confidencialidad, integridad y disponibilidad de la información.

3.2 Objetivos específicos

La materialización del Objetivo general del Plan de Seguridad y Privacidad de la Información 2024-2027 se desarrolla a través del cumplimiento de los siguientes objetivos específicos:

1. Identificar y ejecutar actividades asociadas al componente de seguridad y privacidad de la Información, estableciendo productos, responsables y su correspondiente fecha de inicio y fecha final, con el fin de mitigar el impacto de incidentes de seguridad y privacidad de la información en la Corporación.

2. Implementar sesiones de capacitación para funcionarios y profesionales de apoyo a la gestión corporativa sobre prácticas seguras para el manejo y concienciación de la seguridad de la información y políticas de privacidad.

3. Integrar la seguridad de la información en los planes de continuidad del negocio, garantizando que se puedan mantener operaciones críticas ante incidentes.

4. Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios, y a los de las normas técnicas colombianas en materia de seguridad y privacidad de la información.

4 Glosario

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea divulgada a individuos, entidades o procesos no autorizados.

Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos de información.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por los usuarios autorizados cuando lo requieran.

Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema o a la organización.

Análisis de riesgos: Proceso sistemático de utilizar la información disponible para identificar peligros y estimar los riesgos.

Modelo de Seguridad y Privacidad de la Información (MSPI): Marco definido por MINTIC que establece un ciclo de operación para gestionar adecuadamente la seguridad y privacidad de los activos de información.

PHVA: Acrónimo de Planificar, Hacer, Verificar y Actuar, utilizado para la mejora continua de los procesos de seguridad de la información.

Funcionario: Persona con una vinculación laboral con una entidad pública, que ejerce funciones al servicio del estado y de la comunidad.

Cifrado: Técnica utilizada para proteger la confidencialidad de la información mediante la conversión de datos en un formato ilegible para personas no autorizadas.

Control de acceso: Mecanismos que regulan quién puede ver o usar los recursos en un entorno de computación.

4.1 Siglas

GIT TIC. Grupo Interno de Trabajo Tecnologías de la Información y las Comunicaciones.

MSPI. Modelo de Seguridad y Privacidad de la Información.

ODS. Objetivos de Desarrollo Sostenible.

PGAR. Plan de Gestión Ambiental Regional.

SGI. Sistema de gestión integral.

SPI. Seguridad y Privacidad de la Información.

TIC. Tecnologías de la Información y las Comunicaciones.

4.2 Definiciones

Actividades. Son el conjunto de procesos bajo el control del responsable de la intervención pública, que transforma insumos en productos. (DNP, 2014)

Efectividad. Es el grado en el que los resultados deseados se alcanzan a través de los productos». (DNP, 2014)

Eficacia. Es el grado de cumplimiento de las metas y objetivos a nivel de productos y resultados. (DNP, 2014)

Eficiencia. Hace referencia al uso óptimo de recursos en una actividad productiva. Es la máxima cantidad de un producto específico que un nivel dado de costo en insumos puede generar, o alternativamente, es el mínimo costo en insumos que se requiere para generar una cantidad dada de un producto específico. Es decir, la eficiencia compara la productividad observada con una productividad esperada. (DNP, 2014)

Estrategias. Conjunto de directrices coordinadas que ayudan a elegir las acciones adecuadas para alcanzar los objetivos de la planeación estratégica (PGAR y Plan de Acción), orientados a la consecución de resultados. Permiten la definición de condiciones de interés, planes de acción, mecanismos de coordinación, responsables, metas, etc. y orientan el proceso de priorización en la asignación de recursos. (DNP, 2014)

Evaluación. Es la apreciación, lo más sistemática y objetiva posible, de un proyecto, programa o política en curso o concluido, de su diseño, su puesta en práctica y sus resultados. El objetivo es determinar la pertinencia y el logro de los objetivos, así como la eficiencia, la eficacia, el impacto y la sostenibilidad para el desarrollo. (SINA, 2018)

Impacto. Son los efectos exclusivamente atribuibles a la intervención pública. La evaluación del impacto trata de identificar todos estos efectos y centrarse en la determinación de los efectos netos atribuibles a la intervención». (DNP, 2014)

Indicador. Variable o factor cuantitativo o cualitativo que proporciona un medio sencillo y fiable para medir logros, reflejar los cambios vinculados con una intervención o ayudar a evaluar los resultados de un organismo de desarrollo. (DNP, 2014)

Productos. Son los bienes y servicios generados por la intervención pública, que se obtienen mediante los procesos de transformación de los insumos. (DNP, 2014)

Programas. Intervención pública que materializa los objetivos planteados en la planeación a través de la entrega coordinada de productos y la generación de resultados estratégicos a escala territorial con la participación de diferentes actores. Cuenta con una estructura de seguimiento basada en la disposición y el uso de información de desempeño para retroalimentar las decisiones y orientar las decisiones gerenciales. Adaptado de (DNP, 2014)

Resultados. «son los efectos intencionales o no de la intervención pública, una vez se han consumido los productos. (DNP, 2014)

Seguimiento. Es el proceso continuo que debe llevarse a cabo con una periodicidad regular, y que debe centrarse en la evaluación del cumplimiento de los diversos aspectos de la ejecución como por ejemplo la evaluación de los indicadores. Al tratarse de un proceso sistemático y periódico, permite que se recopile y se analice información con el objeto de comparar los avances logrados en función de los planes formulados. Ayuda además a identificar tendencias y patrones, a adaptar las estrategias y a fundamentar las decisiones relativas a la gestión del proyecto o programa. Un seguimiento continuo garantiza que cualquier irregularidad se detecte y corrija a tiempo. Para que resulte verdaderamente eficaz, debe realizarse de forma abierta con una amplia participación de los interesados. (SINA, 2018)

5 Roles y responsabilidades

5.1 Oficial de seguridad o quien haga sus veces

El rol del Oficial de seguridad o Coordinador del proceso Gestión de TIC o quien haga sus veces, es el responsable de:

- Realizar seguimiento al cumplimiento de los lineamientos y políticas del proceso Gestión de TIC.
- Revisar y proponer las políticas, planes, programas, procedimientos en materia de seguridad de la información para la aplicación de controles en el sistema.
- Realizar revisiones periódicas al proceso Gestión de TIC y definir acciones conducentes a la mejora continua.
- Asegurar el cumplimiento de las políticas, normas, procedimientos, y demás lineamientos en materia de seguridad de la información.

5.2 Líder del proceso de Gestión de TIC

El rol del Subdirector Administrativo y Financiero como líder del proceso en la ejecución del plan de revisión y seguimiento al proceso Gestión de TIC, es fundamental dado que es el responsable de:

- Seguimiento a la ejecución del Plan de Seguridad y Privacidad de la Información y del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información.
- Revisión y cumplimiento de los procedimientos, controles y políticas del proceso Gestión de TIC.

5.3 Grupo Interno de Trabajo Tecnologías de la Información y las Comunicaciones (GIT TIC)

El GIT de apoyo informático y sus profesionales serán los responsables de los controles técnicos de seguridad de la información:

- Cierre de vulnerabilidades técnicas.
- Seguimiento al cierre de vulnerabilidades técnicas.
- Seguimiento de indicadores.
- Seguimiento al cierre de eventos e incidentes de seguridad de la información.
- Seguimiento del plan de tratamiento de riesgos de seguridad de la información del proceso Gestión TICs.
- Establecer controles de seguridad de la información con el fin de mitigar los riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información y/o servicios que presta el GIT de apoyo informático.

5.4 Funcionarios y Contratistas

Los funcionarios, contratistas de apoyo a la gestión corporativa, practicantes y colaboradores, serán los responsables de la seguridad y privacidad de la información en los siguientes aspectos:

- Implementar las normas, políticas y procedimientos definidos para el sostenimiento del proceso Gestión de TIC.
- Mantener y garantizar la confidencialidad e integridad de la información que reciben, generan y procesan en la Corporación.
- Hacer buen uso de los activos de información de la entidad.
- Respetar la legislación y regulación vigente.
- Notificar a la cuenta de correo electrónico datacenter@corantioquia.gov.co los eventos o incidentes de seguridad de información, así como cualquier eventualidad sospechosa que pueda poner en riesgo la continuidad de las operaciones de la Corporación.

6 Contexto del plan

6.1 Diagnóstico

6.1.1 Seguridad

Mediante el **Acuerdo del Consejo Directivo número 180-ACU2209-642 del 29 de septiembre de 2022,** se determinó la estructura organizacional de la Corporación.

El Gobierno de TI en Corantioquia está conformado por el Grupo Interno de Trabajo Tecnologías de la Información y las Comunicaciones y el Grupo Interno de Trabajo Gestión de la Información y el Conocimiento.

El Contratista EY (Ernst & Young) mediante el Contrato número 190-CNT1909-110 apoyó a CORANTIOQUIA en la **Formulación del Programa de Seguridad de la Información**. En el proyecto se identificaron múltiples vulnerabilidades y se planteó unas acciones requeridas por parte de la Corporación para cerrar las brechas de seguridad de la información.

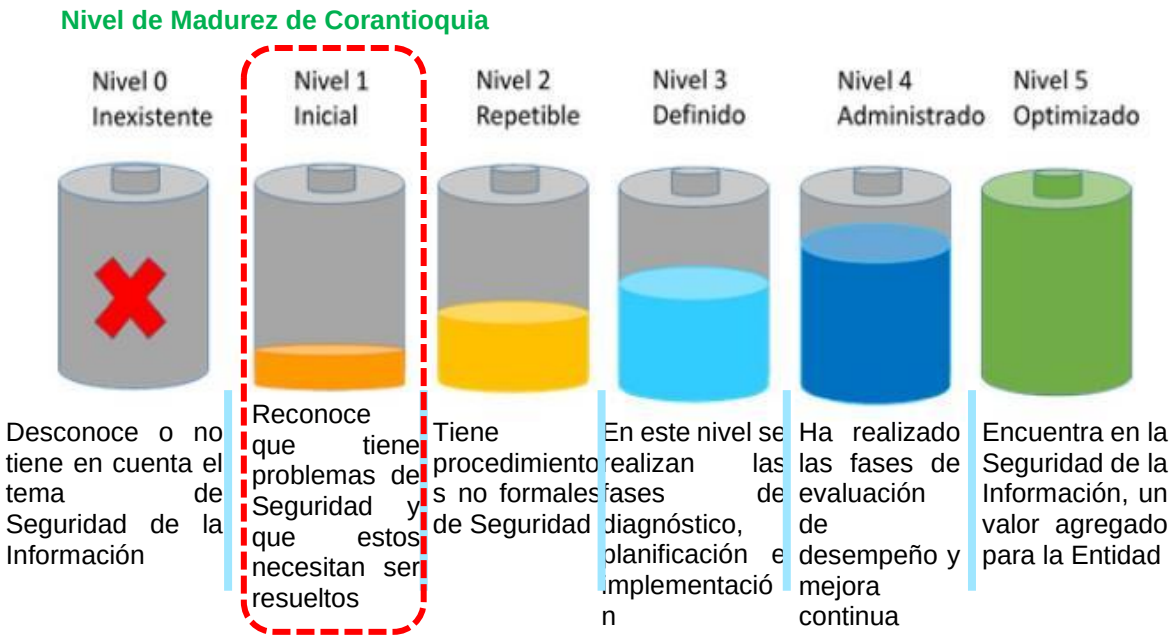


Figura 3 Situación Actual Seguridad de la Información en CORANTIOQUIA

Fuente: Documentación Contrato 190-CNT1909-110

En la Figura 4, el Contratista EY (Ernst & Young) identifica las acciones para la construcción, implementación y administración del Plan de Seguridad y Privacidad de la Información en CORANTIOQUIA, de conformidad con la documentación relacionada en el Contrato 190-CNT1909-110.

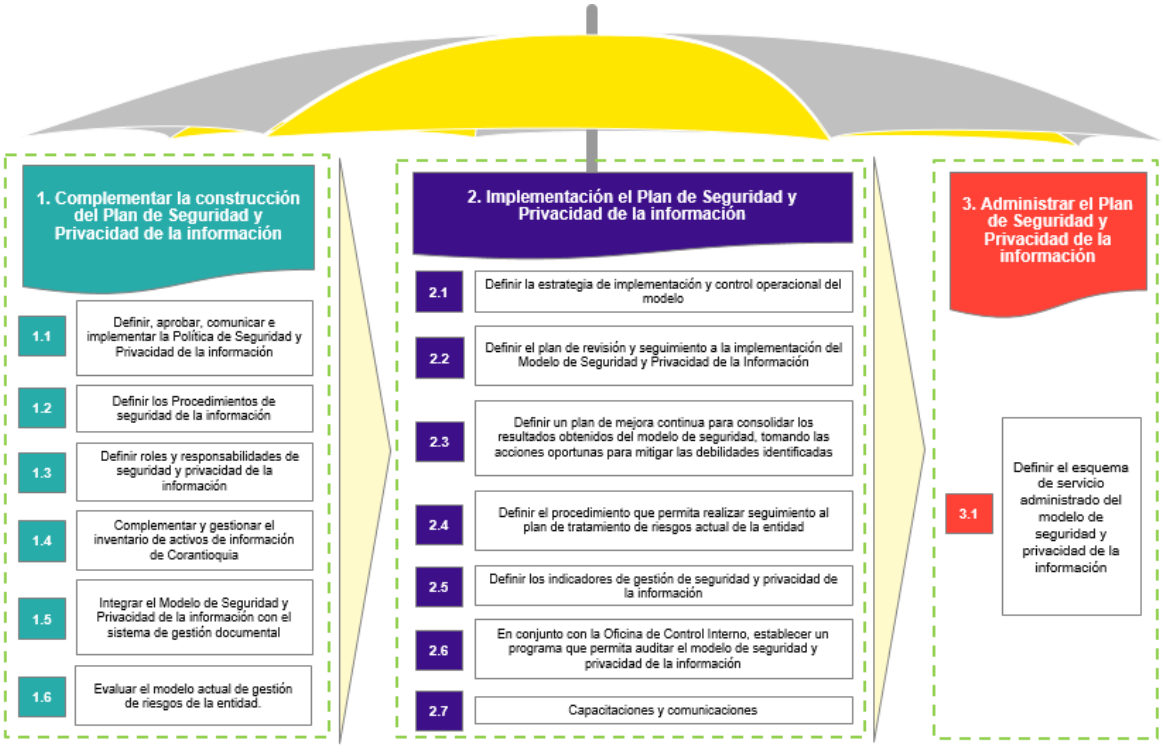


Figura 4 Estructuración Plan de Seguridad y Privacidad de la Información en CORANTIOQUIA

Fuente: Documentación Contrato 190-CNT1909-110

Por otro lado, previo a las actividades por ejecutar del Plan de Seguridad y Privacidad de la Información, se aplicará la herramienta establecida por el Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC) “Instrumento Evaluación del Modelo de Seguridad y Privacidad de la información - MSPI” para autodiagnosticar el nivel de madurez de la entidad en seguridad y privacidad de la información, esto con el propósito de tener un enfoque estructurado y eficiente para cerrar los puntos claves o vulnerables identificados.

6.2 Marco normativo

Tabla 1 Marco Normativo

Marco Normativo	Descripción
Directiva Presidencial 02 del 24 de febrero de 2022	"Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)"
Decreto 338 del 08 de marzo de 2022	Por el cual se adiciona el Titulo 21 a la parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
Resolución 746 del 11 de marzo de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021.
Decreto 767 del 16 de mayo 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.
CONPES 4069 de 2022.	Política Nacional de Ciencia, tecnología e innovación 2022 – 2031.
Resolución 500 del 10 de marzo de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Resolución 1519 del 24 de agosto de 2020	por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos vigente.
CONPES 3995 de 2020.	Confianza y Seguridad Digital.

Marco Normativo	Descripción
Resolución 040-RES2012-7361 del 21 de diciembre de 2020	Por medio de la cual se integra y se establece el reglamento de funcionamiento del Comité Institucional de Gestión y Desempeño de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA
Conpes 3854 del 11 de abril de 2016	Política Nacional de Seguridad Digital Este documento CONPES busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.
Decreto 103 del 20 de enero de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Ley 1712 del 06 de marzo de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decretro 1377 del 23 de junio de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1581 de 17 de octubre de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
CONPES 3701 de 2011.	Lineamientos de Política para Ciberseguridad y Ciberdefensa.

6.3 Logros

A continuación, se relacionan los contratos que ha suscrito la Corporación donde se relacionan los logros alcanzados de cada uno de estos en Seguridad y Privacidad de la Información:

Tabla 1 Contratos suscritos por CORANTIOQUIA que impactan la seguridad y privacidad de la información

Ítem	Nro. Contrato / Orden Compra	Objeto	Valor total contrato incluido IVA	Logros
1	190-CNT2402-18	Actualización, Soporte y mantenimiento de las aplicaciones de Safix.	$ 235,266,841	El Sistema de Información Financiero y Administrativo (SAFIX) y el aplicativo PGAR se actualizan por parte del contratista XENCO S.A de acuerdo con los cambios de Ley y en materia de seguridad informática.
2	190-CNT2407-135	Soporte, mantenimiento y desarrollo en las aplicaciones Sirena/e-Sirena, Laboratorio y Facturación y Cartera.	$ 235,324,215	Las Aplicaciones Sirena/e-Sirena, Laboratorio y Facturación y Cartera se actualizan por parte del contratista CONSERES de acuerdo con los cambio de Ley y en materia de seguridad informática.

3	040-COV2406-8	Aunar esfuerzos financieros, técnicos y humanos para prestar servicios especializados que garanticen el buen funcionamiento de la infraestructura informática y de telecomunicaciones de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA.	$ 347,006,000	A nivel de la infraestructura informática y de telecomunicaciones de la Corporación, donde se encuentran los equipos servidores, sistemas de almacenamiento y solución de backups, el Conveniante ROTORR realiza actividades de mantenimiento periódicos, en las que se instalan y actualizan las versiones que lanza el fabricante HP cada vez que actualiza o emite un nuevo parche de seguridad en sus sistemas operativos o componentes.
4	190-CNT2402-9	Prestar servicios de intercomunicación de datos e internet para la Sede Central y Oficinas Territoriales.	$ 360,488,211	El proveedor de Servicios TIGO - UNE garantiza los servicios de Conectividad a través de la solución SDWAN (servicios de Internet e interconexión de la Sede Central con las Oficinas Territoriales) de conformidad con lo contratado, y agenda ventanas de mantenimiento donde se realizan actualizaciones de seguridad informática a equipos y sistemas de telecomunicaciones.

5	190-OC2402-124782	Renovación del licenciamiento de los productos Microsoft de la Corporación Autónoma Regional del Centro de Antioquia - CORANTIOQUIA hasta el 31 de diciembre de 2024.	$ 1,158,040,962	Se implementó el MFA (Multi-Factor Authentication) donde se habilita la autenticación multifactor, que requiere más de una forma de verificación (por ejemplo, una contraseña y un código enviado al teléfono) para acceder a cuentas y sistemas de la Plataforma Microsoft 365 E3, añadiendo una capa adicional de seguridad al acceso de la información corporativa.
6	190-AO2402-1	Adquirir de certificado SSL (Secure Socket Layer) OV Wilcard Básico por tres (3) años que garantice la seguridad, la autenticidad y confiabilidad en el acceso a la página web y sitios de información (Web) de Corantioquia, desde cualquier navegador de Internet.	$ 4,284,000	El certificado digital SSL (Secure Sockets Layer) autentica la identidad de un sitio web y permite una conexión cifrada entre un servidor Web y un navegador, a través de un sistema de autenticación segura con integridad de los datos, garantizando que estos no sean alterados durante la transmisión.
7	090-AO2406-5	Prestar el servicio de actualización, soporte y mantenimiento al sistema KOHA	$ 8,211,000	El Sistema de Información KOHA se actualiza por parte del contratista DOSSIER SOLUCIONES S.A.S de acuerdo con la normatividad vigente y en materia de seguridad informática.
8	090-OC2402-124287	Licencia ArcGIS para garantizar la transferencia y democratización de la información cartográfica	$ 154,853,253	El fabricante ESRI libera permanentemente nuevos parches de seguridad para el licenciamiento ArcGIS que utiliza la Corporacion en su Sistema de Información Geográfica (SIG).

9	190-AO2404-3	Renovación del licenciamiento de soporte del software de Backup Veeam.	$ 51,066,286	Las copias de seguridad de la información Corporativa se realizan a través del software de Backup Veeam, lo cual representa varias garantías clave para la protección y recuperación de datos en la entidad. Una de ellas es la protección contra amenazas de ransomware. Veeam incluye funcionalidades de seguridad avanzadas, como backups inmutables y detección temprana de amenazas, que ayudan a prevenir y mitigar los ataques de ransomware.
10	190-CNT2411-196	Renovación del licenciamiento y acuerdo de soporte de la solución de Endpoint y protección de correo electrónico de la Corporación.	$ 378,752,176	La solución de seguridad perimetral en la corporación se brinda por medio de la plataforma Sophos, con la renovación del acuerdo de soporte de la solución de Endpoint y protección de correo electrónico de la Corporacióna nivel de Antivirus, AntiSpam, AntiSpyware.

11	190-CNT2312-183	Renovación del contrato de licenciamiento en modalidad tradicional para el soporte y garantía del sistema de comunicaciones unificada Avaya de CORANTIOQUIA, incluyendo las Oficinas Territoriales, propendiendo que las mismas cumplan con su carácter de protección ambiental.	$ 224,605,250	Con la renovación del contrato de licenciamiento, el sistema de comunicaciones unificada existente en la Coproración se actualiza permanentemente por parte del fabricante Avaya garantizando confidencialidad e integridad en las comunicaciones corporativas.
12	190-CNT2310-167	Adopción e implementación del protocolo IPv6 para CORANTIOQUIA	$ 238,000,000	Con la implementación del protocolo IPv6 en la Corporación ganamos en seguridad mejorada: IPv6 fue diseñado con la seguridad como uno de los pilares fundamentales de la transmisión de datos en la red pública Internet, incorporando IPsec (Internet Protocol Security) como una característica obligatoria. Esto permite una comunicación más segura y encriptada entre dispositivos.
13	190-CNT2205-102	Renovar el licenciamiento y acuerdo de soporte de la solución de firewall de la Corporación.	$ 97,000,000	La solución de seguridad perimetral en la corporación se brinda por medio de la plataforma Sophos, a nivel de Firewall, donde el soporte técnico finaliza en marzo de 2025.

14	190-CNT2312-186	Adquisición del servicio de soporte técnico para la infraestructura tecnológica de CORANTIOQUIA.	$ 518,446,336	Disponibilidad y Tiempo de Respuesta: Este Contrato garantiza que los repuestos necesarios para la infraestructura informática y de telecomunicaciones de propiedad de la Corporación, estarán disponibles y se entregarán al siguiente día hábil laboral. Esto minimiza el tiempo de inactividad y asegura que la infraestructura de TI de la Corporación vuelva a estar operativa lo más rápido posible.
		TOTAL	$ 4,011,344,530	

6.4 Retos

Implementar el Plan de Seguridad y Privacidad de la Información en la Corporación presenta varios retos específicos. Aquí se describen los más importantes:

1. **Cumplimiento normativo**: Dar cumplimiento normativo en el marco del Sistema de Gestión de Seguridad de la información y otras como la Ley 1581 de 2012 sobre protección de datos personales.

2. **Gestión de riesgos de terceros**: La Corporación depende de proveedores externos para el soporte técnico, mantenimiento y actualización de sus sistemas de información y aplicativos. Garantizar que estos terceros cumplan con los estándares mínimos de seguridad y privacidad de la información, es crucial para proteger la información Corporativa sensible.

3. **Protección contra amenazas internas**: Las amenazas internas, ya sean intencionales o accidentales, representan un riesgo significativo. Implementar controles de acceso adecuados y educar a los funcionarios, contratistas de apoyo a la gestión y colaboradores, sobre las mejores prácticas de seguridad es esencial.

4. **Seguridad en entornos de nube**: La Corporación está evaluando el proceso de migración a servicios de nube. Garantizar la seguridad de los datos en estos entornos se vuelve esencial. Esto incluye la correcta configuración de los servicios en la nube y la implementación de medidas de seguridad robustas.

5. **Automatización y gestión de incidentes**: La capacidad de detectar y responder rápidamente a incidentes de seguridad es fundamental. La

Corporación debe invertir en tecnologías de automatización y en la formación de equipos especializados para gestionar estos incidentes de manera eficiente.

6. **Cultura de seguridad**: Fomentar una cultura de seguridad dentro de la entidad es vital para el éxito del Plan de Seguridad y Privacidad de la Información. Esto implica la concienciación y formación continua de todos los funcionarios, contratistas de apoyo a la gestión y colaboradores, sobre la importancia de la seguridad y privacidad de la información.

7. **Adopción de nuevas tecnologías**: La rápida evolución de la tecnología presenta tanto oportunidades como desafíos. La Corporación debe evaluar y adoptar nuevas tecnologías de manera segura, asegurándose de que no introduzcan vulnerabilidades adicionales.

Estos retos requieren un enfoque proactivo y multidisciplinario para garantizar la protección de la información y el cumplimiento de la normatividad vigente.

6.5 Actividades del componente de Seguridad y Privacidad de la Información.

Tabla 2 Actividades por Ejecutar

Id	Control	Actividades Por Ejecutar	Producto	Fecha inicial estimada	Fecha final estimada	Responsable
1	Formulación del Modelo de Seguridad y Privacidad de la Información (MSPI)	Formular el MSPI.	MSPI formulado	Ene de 2025	Jun de 2025	GIT TIC
2	Política General de Tecnología, de Seguridad y Privacidad de la Información	Revisar, ajustar y aprobar la Política General de Tecnología, de Seguridad y Privacidad de la Información – Resolución 040-RES2010-5756.	Política General de Tecnología, de Seguridad y Privacidad de la Información actualizada	Ene de 2025	Jun de 2025	Dirección General Subdirección de Planeación - GIT GIC GIT TIC

						Subdirección de Planeación
						Subdirección de Planeación
						Funcionarios de la Corporación
3	Documentos del proceso Gestión de TIC - Procedimiento de seguridad de la información y otros	Revisar y ajustar los documentos del proceso Gestión de TIC implementado en la Corporación, de acuerdo con las actualizaciones definidas y aprobadas por el Comité Institucional de Gestión y Desempeño.	Formatos, Instructivos, Procedimientos de Seguridad y Privacidad de la información indicados en la Guía Nº 3. Min Tic - G3 - Procedimiento de la Seguridad de la información, actualizados	Ene de 2025	Dic de 2027	GIT TIC Todos los procesos del alcance del proceso Gestión de TIC
4	Gestión de activos de Información	Validar, verificar, actualizar y aprobar el inventario de Activos de Información.	Matriz de activos actualizada y aprobada	Ene de 2025	Dic de 2025	GIT TIC
						Subdirección de Planeación – GIT GIC. GIT Gestión Documental
						Todos los procesos del alcance del proceso Gestión de TIC
5	Gestión de vulnerabilidades	Definir lineamientos para ejecutar las pruebas de vulnerabilidades.	Documentación de la gestión de vulnerabilidades y resultados de	Ene de 2025	Dic de 2025	GIT TIC

		Ejecución de pruebas de seguridad (análisis de vulnerabilidades).	pruebas de vulnerabilidades			
		Realizar seguimiento al cierre de vulnerabilidad técnicas de acuerdo con su nivel de criticidad.				
		Verificar la ejecución del re-test de pruebas de seguridad.				
		Documentar las actualizaciones cuando ocurra un cambio importante en los activos de información producto del re-test.				
6	Indicadores de seguridad de la información	Revisar, ajustar y medir los indicadores del Plan de Acción 2024-2027 Programa 5. Conexión Institucional. Actividad 5.3.2. Implementación del Centro de Monitoreo para la administración integral del territorio con	Matriz con indicadores actualizados según periodicidad.	Ene de 2025	Dic de 2027	Subdirección de Planeación – GIT GIC. GIT TIC

		énfasis en el recurso agua.				
7	Plan de Continuidad de Negocio de TI y los Planes de Contingencia	Elaborar y aprobar el Plan de Continuidad de Negocio y los Planes de Contingencia.	Plan de Continuidad de Negocio de TI y Plan de Contingencia.	Ene de 2025	Dic de 2025	GIT TIC
		Validar, verificar, actualizar la identificación y/o valoración de Riesgos de interrupción de la operación de la entidad según corresponda.	Documentación de las pruebas realizadas	Ene de 2025	Dic de 2027	
		Realizar seguimiento y revisión de la ejecución de las pruebas del plan según Cronograma.				
		Realizar seguimiento a la documentación y lecciones aprendidas de los resultados de las pruebas del Plan.				
		Revisión de las acciones de mejora Identificadas en las pruebas del Plan.				
8	Plan de comunicación, socialización y sensibilización	Elaborar y ejecutar el Plan de comunicación en temas relacionados con la seguridad de la información como complemento al	Plan de Sensibilización y toma de conciencia en temas relacionados con seguridad de la Información y Seguridad Digital	Ene de 2025	Dic de 2026	GIT TIC

		Plan Institucional de Ca pacitación de la Corporación.				
		Desarrollar un Plan de sensibilización y toma de conciencia sobre ciberseguridad para ejercer control y protección sobre los entornos digitales.		Ene de 2025	Dic de 2026	Líderes de los procesos de la Corporación, Talento humano, GIT TIC
		Realizar mínimo 3 sesiones de sensibilización en seguridad de la información en las jornadas de inducción y reinducción.		Ene de 2025	Dic de 2027	(Nota: Los lideres podrán realizar socializacion es internas de seguridad de la información cuando sea pertinente mas no es obligatorio)
		Hacer seguimiento a las evidencias de socialización del proceso Gestión de TIC.	Evidencias de socialización y sensibilización	Ene de 2025	Dic de 2027	GIT TIC
9	Auditoria (Internas y/o Externas)	Participar en auditorías internas y/o externas	Informe de auditoría y Plan de Mejoramiento	Ene de 2025	Dic de 2027	Subdirección de Planeación - Grupo Interno de Trabajo Planificación y Gestión Integral

		Realizar seguimiento al cierre de las no conformidades producto de las auditorías internas y externas al proceso Gestión de TIC.				Todos los líderes de los procesos incluyendo al líder del GIT TIC.
		Hacer seguimiento a las evidencias del cierre de las no conformidades por proceso.				
10	Gestión de incidentes de seguridad	Gestionar los incidentes de Seguridad de la Información identificados.	Formatos Registro de Incidentes y/o Eventos de Seguridad de la Información y Soportes gestión	Ene de 2025	Dic de 2027	GIT TIC
		Socializar el procedimiento de respuesta de gestión de incidentes al GIT de Apoyo Informático.	Presentación al GIT TIC	Ene de 2025	Dic de 2027	
		Realizar el seguimiento a la gestión de incidentes de seguridad de la información incl uyendo cierre.	Presentación con los resultados de los incidentes ocurridos en tema d e seguridad y privacidad de la información.	Ene de 2025	Dic de 2027	
		Realizar seguimiento a las lecciones aprendidas producto de la gestión del incidente.				
		Realizar seguimiento de los reportes de eventos de				

		seguridad de la información y tomar acciones.				
		Capacitar a los usuarios internos y partes interesadas sobre los boletines de CSIRT.	Evidencias de sensibilización.	Ene de 2025	Dic de 2027	

7 Metodología empleada para la formulación

La metodología empleada para la formulación del Plan de Seguridad y Privacidad de la Información 2024-2027 para CORANTIOQUIA es, la aportada por el Modelo de Seguridad y Privacidad de la Información (MSPI).

8 Estructura programática

En este capítulo, va lo especificado en el punto 6.5 Actividades del componente de Seguridad y Privacidad de la Información.

9 Líneas de acción para la mitigación del riesgo

Las acciones para la mitigación del riesgo están plasmadas en la matriz de riesgos que se relaciona en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

10 Presupuesto

El presupuesto para el presente Plan de Seguridad y Privacidad de la Información 2024-2027 de la Corporación, está incluido en las Iniciativas de Operación y Transformación Digital y Modernización Tecnológica que se relacionan en el **PETIC** 2024-2027.

11 Seguimiento al plan.

El seguimiento y evaluación al Plan de Seguridad y Privacidad de la Información 2024-2027, se realizará conforme al cumplimiento de las actividades definidas en la estructura programática.

Así pues, el proceso de seguimiento y evaluación permite contar con información objetiva y oportuna de utilidad para: tomar acciones que permitan mejorar la Gestión de TI orientada a la consecución de resultados.

El avance del Plan de Seguridad y Privacidad de la Información 2024-2027 se evaluará semestralmente.

Estos informes serán presentados al Comité Directivo y serán difundidos al interior de la Corporación.

Como instancias de seguimiento, se tendrá el Comité de Dirección de CORANTIOQUIA.

El resultado del Plan de Seguridad y Privacidad de la Información 2024-2027 se interpretará de conformidad con los siguientes rangos de evaluación:

Nivel de ejecución (N.E) deficiente	Nivel de ejecución (N.E) aceptable	Nivel de ejecución (N.E) sobresaliente
N.E < 75 %	75 % ≤ N.E ≤ 90 %	90 % < N.E ≤ 100 %

Figura 3 Seguimiento al plan -Nivel de ejecución

12 Referencias

Acuerdo Consejo Directivo 575. (diciembre de 2019). por el cual se aprueba el Plan de Gestión Ambiental Regional PGAR 2020-2031. (Corantioquia, Ed.) Medellín, Antioquia, Colombia: Consejo Directivo.

Consejo Directivo. (19 de mayo de 2016). Plan de Acción 2016-2019. Medellín, Antioquia, Colombia: Corantioquia.

Decreto 612. (4 de abril de 2018). Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. Bogotá, D.C., Colombia: Presidencia de la República.

DNP. (2014). Guía metodológica para el Seguimiento y la Evaluación a Políticas Públicas. (D. d. Públicas, Ed.) Bogotá, D.C., Colombia: Departamento Nacional de Planeación.

Función Pública. (agosto de 2019). Valores del servicio público. Código de intedridad. Bogotá, D.C., Colombia: Departamento Administrativo de la Función Pública.

Resolución 040-RES2010-5718. (7 de octubre de 2020). Por medio de la cual se actualiza la política del sistema de gestión integral (SGI) de la Corporación Autónoma Regional del Centro de Antioquia (Corantioquia). Medellín, Antioquia, Colombia: Corantioquia.

Resolución n.° 040-RES1801-405. (31 de enero de 2018). Por la cual se aprueba y adopta el Plan Anticorrupción y de Atención al Ciudadano para el año 2018. Medellín, Antioquia, Colombia: Corantioquia.

Resolución n.° 040-RES2112-9588. (31 de diciembre de 2021). Por la cual se adopta el código de integridad corporativo. Medellín, Antioquia, Colombia: Corantioquia.

SINA. (2018). Plan de Acción Sectorial Ambiental del Mercurio. Bogotá, D.C., Colombia.

Liliana María Taborda González
Directora General
Corporación Autónoma Regional del Centro de Antioquia

2024-12-26

Aprobado y adoptado mediante Resolución n.° xxx

TABLA DE CONTENIDO

CONTENIDO

LISTADO DE TABLAS

LISTADO DE FIGURAS

Presentación

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de CORANTIOQUIA relaciona actividades y acciones preventivas para identificar, analizar, evaluar, rastrear y mitigar los riesgos de seguridad y privacidad de la información corporativa en cada uno de sus procesos.

Este plan de tratamiento es la línea estratégica que pretende desarrollar y fortalecer el entendimiento del riesgo y su contexto, comprendiendo las nuevas modalidades de ciberataques dirigidos a entidades públicas, privadas, proveedores de servicios de TI y demás actores que conforman el ecosistema de la información pública, convirtiéndola en un blanco para los ciberdelincuentes que buscan apoderarse de esta, causando traumatismos en la operación, pérdida, robo, destrucción y caída o deterioro de los servicios orientados al ciudadano. Al ser conscientes de los riesgos y vulnerabilidades se adoptan acciones de prevención y el fortalecimiento de las capacidades para evitar los diferentes ataques o incidentes que atenten contra la seguridad y privacidad de la información, implementando la cultura de autoprotección y adecuado resguardo y tratamiento de la información.

Por otra parte, La Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA ha implementado la política de protección de datos personales, aprobada mediante resolución 040-RES2411-5277 del 28 de noviembre de 2024, conforme a las disposiciones de la resolución Ley 1581 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales”, atendiendo los lineamientos de la Ley 1712 de 2014; y acoge en sus procesos el marco normativo y regulatorio de la entidad relacionada con la Seguridad y Privacidad de la Información (SPI).

1 Elementos estratégicos corporativos

1.1 Misión

Contribuir al logro del desarrollo sostenible, mediante el conocimiento y mejoramiento de la oferta ambiental y la administración del uso de los recursos para responder a su demanda, a través de la construcción de una cultura ambiental del territorio (Consejo Directivo, 2016)

1.2 Visión ambiental para el desarrollo regional

En 2031 los 80 municipios del centro de Antioquia forman un territorio sostenible en el que se protege el patrimonio ambiental biodiverso, se desarrollan actividades económicas en armonía con la madre tierra y sus actores regionales son corresponsables en la conservación de la diversidad biológica, étnica y cultural, y el respeto a la dignidad humana, para el buen vivir de las generaciones presentes y futuras. (Acuerdo Consejo Directivo 575, 2019)

1.3 Política de administración del riesgo

La Corporación Autónoma Regional del Centro de Antioquia - Corantioquia, es una organización de alto desempeño en la administración de los recursos naturales renovables, que tiene como misión contribuir al logro del desarrollo sostenible, comprometida con la satisfacción de las necesidades de la comunidad; asimismo, buscará la eficacia de las acciones formuladas a través del cumplimiento de los requisitos legales, los sistemas de gestión corporativos, transparencia en el acceso de los servicios, manejo adecuado de la información y el fortalecimiento de la cultura organizacional, mediante las relaciones establecidas entre las partes interesadas, con el fin de monitorear y controlar los posibles riesgos (Registro F-PPO-20 Mapa Riesgos y Oportunidades).

1.4 Código de integridad

Mediante Resolución (Resolución n.° 040-RES2112-9588, 2021) se adoptó el Código de Integridad Corporativo como guía, sello e ideal de cómo deben ser y obrar los servidores públicos y todos aquellos colaboradores de la administración que prestan sus servicios en la corporación, con el fin de cumplir con la misión, la visión y los objetivos institucionales dentro del marco de integridad y legalidad.

El Código de Integridad Corporativo reúne los valores de honestidad, respeto, compromiso, diligencia, justicia, servicio y resultados.

a) **Honestidad.** Actúo siempre con fundamento en la verdad, cumpliendo mis deberes con transparencia, rectitud y siempre favoreciendo el interés general. (Función Pública, 2019)
b) **Respeto.** Reconozco, valoro y trato de manera digna a todas las personas, con sus virtudes y defectos, sin importar su labor, su procedencia, títulos o cualquier otra condición. (Función Pública, 2019)

c) **Compromiso.** Soy consciente de la importancia de mi rol como servidor público y estoy en disposición permanente para comprender y resolver las necesidades de las personas con las que me relaciono en mis labores cotidianas, buscando siempre mejorar su bienestar. (Función Pública, 2019)
d) **Diligencia.** Cumplo con los deberes, funciones y responsabilidades asignadas a mi cargo de la mejor manera posible, con atención, prontitud, destreza y eficiencia, para así optimizar el uso de los recursos del Estado. (Función Pública, 2019)
e) **Justicia.** Actúo con imparcialidad garantizando los derechos de las personas, con equidad, igualdad y sin discriminación. (Función Pública, 2019)
f) **Servicio.** Sirvo y atiendo las necesidades de los ciudadanos, poniendo a disposición mis capacidades y anteponiendo los máximos fines del Estado a cualquier propósito o interés particular.
g) **Resultados.** Tengo claridad frente al rol que desempeño, el empoderamiento individual respecto a los objetivos y la generación de resultados.

El código de integridad y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información están estrechamente interrelacionados y se complementan para proteger los datos y activos de información de la Corporación.

1.5 Política del SGI

Corantioquia es una entidad pública, encargada de administrar el patrimonio ambiental de los 80 municipios de su jurisdicción, enfocada al cumplimiento de los requisitos legales y reglamentarios; la generación de valor público y la satisfacción de los actores del territorio; el mejoramiento continuo del SGI y sus procesos; a la participación de los actores del territorio; el fortalecimiento de la cultura organizacional y ambiental; la prevención de la contaminación y la protección del ambiente; la gestión de los riesgos y oportunidades organizacionales y el bienestar de los servidores públicos, contratistas, subcontratistas, visitantes, participantes en eventos corporativos y actores viales; contribuyendo así al desarrollo sostenible. (Resolución 040-RES2408-3589).

2 Articulación con instrumentos de planificación

2.1 Articulación con el PGAR 2020-2031

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad 2024-2027está alineado al Plan de Gestión Ambiental Regional 2020-2031 a través del Capítulo 5 “Línea estratégicas del PGAR“, Línea 4 “Fortalecimiento de la cultura ambiental y de las capacidades de los actores para la gestión conjunta y el logro de los resultados”, Objetivo 4 “Generar la gobernanza que permita consolidar el escenario de sostenibilidad ambiental de la jurisdicción” , Componente 13 “Institucionalidad fortalecida para una gestión ambiental corresponsable , Componente 15 “ la gestión de la información y el conocimiento investigación + Desarrollo + Innovación” , Componente 18 ”Incidencia institucional para una eficiente coordinación y cooperación con las autoridades étnicas en materia de gestión ambiental” , Retos : 30, 35, 36, 37 y 49.

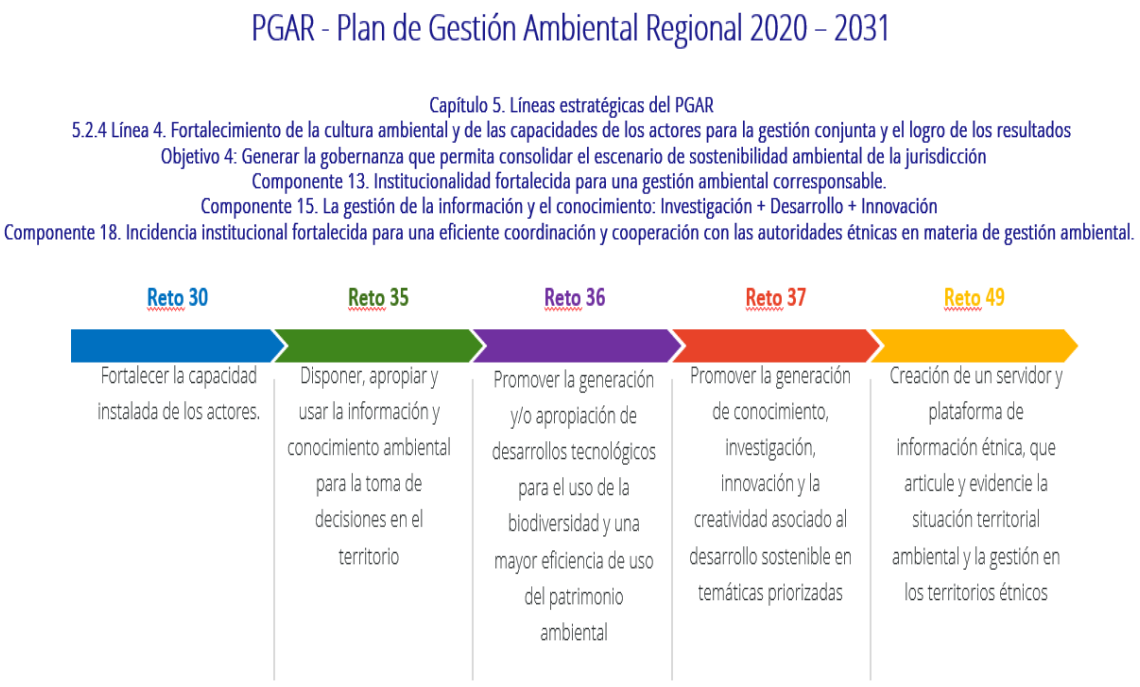


Figura 1 Articulación de la Seguridad y Privacidad de la Información con los retos y Componentes 13, 15 y 18 del PGAR 2020 – 2031

Fuente Elaboración Propia

Nota. Tomado de PGAR 2020-2031 (Acuerdo Consejo Directivo 575, 2019)

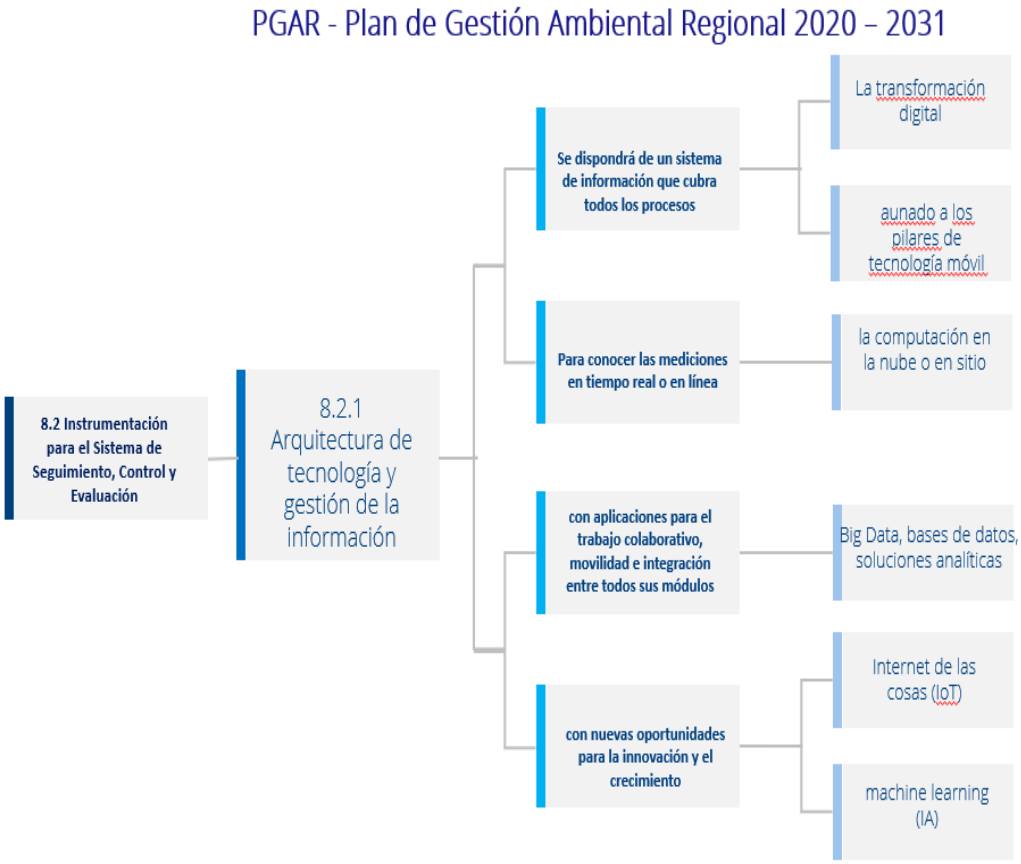


Figura 2 Articulación de la Seguridad y Privacidad de la Información con las tecnologías relacionadas en el instrumento de Planificación PGAR 2020 – 2031

Fuente Elaboración Propia a Partir del PGAR 2020 – 2031

2.2 Articulación con el Plan de Acción 2024-2027

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027 está alineado al Plan de acción 2024-2027 a través del programa 5 “Conexión Institucional “dentro el cual se encuentra el proyecto 5.3 denominado “Gestión de la Información para la toma de decisiones en la gestión ambiental”, dentro de los cuales se encuentra 3 actividades que son:

- **Actividad 5.3.1**. Diseño del Centro de Monitoreo para la administración integral del territorio con énfasis en el recurso agua. (*Indicador: Centro de monitoreo diseñado*).

- **Actividad 5.3.2.** Implementación del Centro de Monitoreo para la administración integral del territorio con énfasis en el recurso agua.

*(**Indicador:** Porcentaje de Avance en el levantamiento de los requerimientos, diagnóstico e implementación integral de las plataformas institucionales.*
***Indicador:** Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027.*
***Indicador:** Porcentaje de avance de la formulación e implementación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información*
***Indicador:** Porcentaje de avance de la formulación e implementación del Plan de Seguridad y Privacidad de la Información.*
***Indicador:** Porcentaje de avance en el diagnóstico integral e implementación de soluciones a las necesidades interoperabilidad*
***Indicador:** Porcentaje de avance de las actividades priorizadas anualmente para la implementación del Centro de Monitoreo).*

- **Actividad 5.3.3.** Articulación del centro de monitoreo con otras entidades del Sistema Nacional Ambiental – SINA En el marco de Sistema de información para Colombia – SIAC. (*Indicador: % de avance de las actividades priorizadas anualmente para la interoperabilidad del Centro de Monitoreo).*

2.3 Articulación con otros instrumentos de planificación

La Corporación dispone de diferentes Instrumentos de Planificación (Estratégica, Temática o Misional, Institucional o de Gestión y Desempeño), los cuales incorporan diferentes estrategias para el logro de su propósito articuladas con asuntos de las TIC, que requieren en primer lugar ser identificadas y en segundo lugar articuladas con el Plan de Seguridad y Privacidad de la Información 2024-2027:

1. **Planes Temáticos o Misionales:** Corresponden a los planes que se desarrollan en el marco de la sostenibilidad del territorio de la Jurisdicción, los cuales disponen de normativa específica para su formulación, seguimiento y actualización:

    - + Aire Puro.
    - Plan de Ordenación Forestal.
    - Plan Regional de Cambio Climático.
    - Plan de Manejo de Acuíferos.
    - Plan de Manejo de Áreas Protegidas.
    - Planes de Manejo de Microcuencas.
    - Planes de Ordenación y Manejo de Cuencas Hidrográficas.
    - Planes de Ordenamiento del Recurso Hídrico.
    - Plan de Negocio Asociativo en Turismo de Naturaleza.
    - Plan de Conservación y Manejo de Especies Priorizadas de Flora.
    - Plan de Conservación y Manejo de Especies Priorizadas de Fauna.

2. **Planes de Gestión y Desempeño:** Corresponden a los Planes Institucionales y Estratégicos que establece el Decreto 612 de 2018, los cuales se deben

actualizar anualmente a más tardar el 31 de enero de cada vigencia e integrar al Plan de Acción de la Corporación, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión (MIPG):

- Plan Institucional de Archivos de la Entidad -PINAR.
- Plan Anual de Adquisiciones.
- Plan Anual de Vacantes.
- Plan de Previsión de Recursos Humanos.
- Plan Estratégico de Talento Humano.
- Plan Institucional de Capacitación.
- Plan de Incentivos Institucionales.
- Plan de Trabajo Anual en Seguridad y Salud en el Trabajo.
- Programa de Transparencia y Ética Pública (PTEP).
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETI.
- Plan de Seguridad y Privacidad de la Información.
- Plan de Apertura de datos.

La articulación entre los planes misionales, los Planes de Gestión y Desempeño y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es esencial para asegurar que las iniciativas transformación digital y modernización tecnológica apoyen directamente los objetivos fundamentales de la Corporación que impactarán la gestión corporativa.

3 Objetivos

3.1 Objetivo general

El objetivo general del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es identificar, evaluar y mitigar los riesgos asociados con la seguridad y privacidad de la información dentro de la Corporación, buscando proteger la confidencialidad, integridad y disponibilidad de la información, cumpliendo con la normatividad del Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC)

3.2 Objetivos específicos

La materialización del Objetivo general del Plan de tratamiento de riesgos de seguridad y privacidad 2024-2027 se desarrolla a través del cumplimiento de los siguientes objetivos específicos:

1. Identificar y actualizar los riesgos de seguridad y privacidad de la información
2. Gestionar los riesgos de seguridad y privacidad de la información, conforme al análisis, evaluación y valoración de estos, para preservar la integridad, disponibilidad y confidencialidad de los activos de información.

3. Sensibilizar y reforzar la protección y adecuado tratamiento de los activos de información y sus riesgos de seguridad y privacidad por medio de charlas y socializaciones con el fin de fortalecer y apropiar conocimiento referente a la gestión de riesgos de seguridad y privacidad de la información.

4 Glosario

Aceptación del riesgo: Decisión informada de asumir un riesgo particular.

Activo: Cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas) que tenga valor para la organización.

Análisis de riesgo: Proceso para comprender la naturaleza del riesgo y determinar su nivel.

Amenaza: Causa potencial de un incidente no deseado que puede resultar en daño a un sistema o a la organización.

Confidencialidad: Propiedad que determina que la información no esté disponible ni sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: Resultado de un evento que afecta los objetivos.

Control de acceso: Mecanismos que regulan quién puede ver o usar los recursos en un entorno de computación.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por los usuarios autorizados cuando lo requieran.

DAFP: Departamento Administrativo de la Función Pública.

DNP: Departamento Nacional de Planeación.

GIT: Grupo Interno de Trabajo.

Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos de información.

Modelo de Seguridad y Privacidad de la Información (MSPI): Marco definido por MINTIC que establece un ciclo de operación para gestionar adecuadamente la seguridad y privacidad de los activos de información.

PGAR: Plan de Gestión Ambiental Regional 2020-2031.

PHVA: Acrónimo de Planificar, Hacer, Verificar y Actuar, utilizado para la mejora continua de los procesos de seguridad de la información.

TIC: Tecnologías de la Información y las Comunicaciones.

4.1 Siglas

ODS. Objetivos de Desarrollo Sostenible.

PGAR. Plan de Gestión Ambiental Regional.

SGI. Sistema de gestión integral.

4.2 Definiciones

Actividades. Son el conjunto de procesos bajo el control del responsable de la intervención pública, que transforma insumos en productos. (DNP, 2014).

Activo. Cualquier recurso valioso para la organización, cuya protección es esencial. Los activos pueden ser físicos, como hardware o instalaciones, o intangibles, como datos, información confidencial o propiedad intelectual.

Amenaza. Cualquier evento o circunstancia que pueda explotar una vulnerabilidad en un activo, con el potencial de causar un daño. Las amenazas pueden ser naturales (como desastres naturales) o humanas (como ataques cibernéticos o errores humanos).

Causa. El origen o factor subyacente que genera una amenaza o contribuye a la existencia de una vulnerabilidad. Es el elemento que desencadena un evento de riesgo o permite que una amenaza explote una vulnerabilidad. Las causas pueden ser de naturaleza técnica, organizativa o humana, como fallos en los controles de seguridad, defectos en el diseño de sistemas, prácticas inadecuadas de gestión, o errores humanos. Identificar la causa es fundamental para implementar medidas efectivas de prevención y mitigación.

Control. Acción, proceso, procedimiento o dispositivo implementado para reducir o mitigar los riesgos, minimizando las probabilidades de que una amenaza explote una vulnerabilidad o disminuyendo el impacto de un evento adverso. Los controles o medidas pueden ser preventivos, detectivos o correctivos, y pueden incluir políticas de seguridad, controles técnicos (como firewalls o cifrado), formación del personal, auditorías regulares, y protocolos de respuesta ante incidentes. La implementación adecuada de controles es crucial para gestionar eficazmente los riesgos de seguridad y privacidad de la información.

Eficacia. Es el grado de cumplimiento de las metas y objetivos a nivel de productos y resultados. (DNP, 2014)

Eficiencia. Hace referencia al uso óptimo de recursos en una actividad productiva. Es la máxima cantidad de un producto específico que un nivel dado de costo en insumos puede generar, o alternativamente, es el mínimo costo en insumos que se requiere para generar una cantidad dada de un producto específico. Es decir, la eficiencia compara la productividad observada con una productividad esperada. (DNP, 2014)

Evaluación. Es la apreciación, lo más sistemática y objetiva posible, de un proyecto, programa o política en curso o concluido, de su diseño, su puesta en práctica y sus

resultados. El objetivo es determinar la pertinencia y el logro de los objetivos, así como la eficiencia, la eficacia, el impacto y la sostenibilidad para el desarrollo. (SINA, 2018)

Impacto. Son los efectos exclusivamente atribuibles a la intervención pública. La evaluación del impacto trata de identificar todos estos efectos y centrarse en la determinación de los efectos netos atribuibles a la intervención». (DNP, 2014).

Probabilidad. La posibilidad de que ocurra un evento de riesgo, basado en el análisis de factores internos y externos. Se mide con base en la frecuencia con la que se ha observado una amenaza en situaciones similares o en la probabilidad de que una vulnerabilidad sea explotada.

Productos. Son los bienes y servicios generados por la intervención pública, que se obtienen mediante los procesos de transformación de los insumos. (DNP, 2014)

Programas. Intervención pública que materializa los objetivos planteados en la planeación a través de la entrega coordinada de productos y la generación de resultados estratégicos a escala territorial con la participación de diferentes actores. Cuenta con una estructura de seguimiento basada en la disposición y el uso de información de desempeño para retroalimentar las decisiones y orientar las decisiones gerenciales. Adaptado de (DNP, 2014)

Resultados. «son los efectos intencionales o no de la intervención pública, una vez se han consumido los productos. (DNP, 2014).

Riesgo. Posibilidad de que un evento o circunstancia adversa afecte de manera negativa los activos de información, comprometiendo su confidencialidad, integridad o disponibilidad. El riesgo se determina por la combinación de la probabilidad de que ocurra un evento y el impacto que tendría si se materializa.

Seguimiento. Es el proceso continuo que debe llevarse a cabo con una periodicidad regular, y que debe centrarse en la evaluación del cumplimiento de los diversos aspectos de la ejecución como por ejemplo la evaluación de los indicadores. Al tratarse de un proceso sistemático y periódico, permite que se recopile y se analice información con el objeto de comparar los avances logrados en función de los planes formulados. Ayuda además a identificar tendencias y patrones, a adaptar las estrategias y a fundamentar las decisiones relativas a la gestión del proyecto o programa. Un seguimiento continuo garantiza que cualquier irregularidad se detecte y corrija a tiempo. Para que resulte verdaderamente eficaz, debe realizarse de forma abierta con una amplia participación de los interesados. (SINA, 2018).

Vulnerabilidad. Debilidad o deficiencia en un sistema, proceso, infraestructura o política que puede ser explotada por una amenaza para causar daño. Las vulnerabilidades pueden surgir por fallos de diseño, configuraciones incorrectas, o falta de controles adecuados.

5 Roles y responsabilidades

5.1 Oficial de seguridad o quien haga sus veces

El rol del Oficial de seguridad o Coordinador del proceso Gestión de TIC o quien haga sus veces, es el responsable de:

- Realizar seguimiento al cumplimiento de los lineamientos y políticas del proceso Gestión de TIC.
- Revisar y proponer las políticas, planes, programas, procedimientos en materia de seguridad de la información para la aplicación de controles en el sistema.
- Realizar revisiones periódicas al proceso Gestión de TIC y definir acciones conducentes a la mejora continua.
- Asegurar el cumplimiento de las políticas, normas, procedimientos, y demás lineamientos en materia de seguridad de la información.
- Realizar el seguimiento a la gestión de los riesgos de seguridad y privacidad de la información, en especial los que se encuentran en la zona de riesgo Extremo, Alto o Moderado. Ver anexo al Plan.

5.2 Líderes de procesos

El rol de los líderes de procesos en la ejecución del plan de revisión y seguimiento al proceso Gestión de TIC, es fundamental dado que es el responsable de:

- Seguimiento a la ejecución de los planes de tratamiento de riesgos en seguridad de la información.
- Actualización de activos de información.
- Revisión y cumplimiento de los procedimientos, controles y políticas del proceso Gestión de TIC.

5.3 Coordinador del Grupo Interno de Trabajo Tecnologías de la Información y las Comunicaciones – GIT TIC

El GIT TIC y sus profesionales serán los responsables de los controles técnicos de seguridad de la información:

- Cierre de vulnerabilidades técnicas.
- Seguimiento al cierre de vulnerabilidades técnicas.
- Seguimiento de indicadores.

- Seguimiento al cierre de eventos e incidentes de seguridad de la información.
- Seguimiento del plan de tratamiento de riesgos de seguridad de la información del proceso Gestión TICs.
- Establecer controles de seguridad de la información con el fin de mitigar los riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información y/o servicios que presta el GIT de apoyo informático.

5.4 Funcionarios y Contratistas

- Implementar las normas, políticas y procedimientos definidos para el sostenimiento del proceso Gestión de TIC.
- Mantener y garantizar la confidencialidad e integridad de la información que reciben, generan y procesan en la Corporación.
- Hacer buen uso de los activos de información de la entidad.
- Respetar la legislación y regulación vigente.
- Notificar a la cuenta de correo electrónico seguridadinformatica@corantioquia.gov.co los eventos o incidentes de seguridad de información, así como cualquier eventualidad sospechosa que pueda poner en riesgo la continuidad de las operaciones de la Corporación.

6 Contexto del plan

6.1 Diagnóstico

La Corporación cuenta con un Mapa de Riesgos asociado al Sistema Integrado de Gestión donde se identifican, evalúan y priorizan los riesgos.

El Plan de Tratamiento de Riesgos de Seguridad de la Información está basado en el Mapa de Riesgos de la Corporación y en las directrices de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitido por el Departamento Administrativo de Función Pública - DAFP (V6) para comprender los riesgos a los que se enfrenta la Corporación y a tomar decisiones informadas sobre cómo gestionarlos.

En el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se definen las actividades encaminadas a gestionar los riesgos de Seguridad de la Información con el fin de lograr prevenir la materialización de los riesgos y cuya valoración sea aceptable, disminuyendo su calificación de Extrema o Alta y lograr en la medida de las posibilidades mantener una calificación Moderada o Baja.

La etapa de implementación se centra en la ejecución y cumplimiento de las actividades y objetivos planteados, teniendo en cuenta los roles y responsabilidades y los tiempos establecidos por la Corporación en la Política de Administración del Riesgo. El resultado esperado de esta fase es la adecuada implementación y cumplimiento de las actividades previstas.

6.2 Marco normativo

Tabla 1 Marco Normativo

Marco Normativo	Descripción
Directiva Presidencial 02	Febrero 24 de 2022, “Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)”.
Decreto 338	Marzo 8 de 2022, "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".
Resolución 746	Marzo 11 de 2022, "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".

Marco Normativo	Descripción
Decreto 767	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”.
Directiva Presidencial 03	Marzo 15 de 2021, “Lineamientos para el uso de Servicios en la Nube, Inteligencia Artificial, Seguridad digital y Gestión de Datos”.
Resolución 500	Marzo 10 de 2021, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital".
Conpes 3995	Julio 1 de 2020, Política Nacional de Confianza y Seguridad Digital “Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías”.
Resolución 1519	Agosto 24 de 2020, “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”.
Guía para la administración del riesgo y el diseño de controles en entidades públicas -V6	Noviembre 2022, “Establece la metodología para la administración del riesgo, los criterios para el análisis de probabilidad e impacto identificado y su respectivo nivel de severidad. En la versión 5 se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo”.
Decreto 612	Abril 4 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”.

Marco Normativo	Descripción
Decreto 1008	Junio 14 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 número 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
Ley 1915	Julio 12 de 2018, “Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos”.
Resolución 2140	Octubre 19 de 2017, "Por la cual adopta el Modelo Integrado de Planeación y Gestión y se crean algunas instancias administrativas al interior del Ministerio de Ambiente y Desarrollo Sostenible y del Fondo Nacional Ambiental, y se dictan otras disposiciones".
Decreto 103 de 2015	Enero 20 de 2015, “Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”.
Decreto 1068	Mayo 26 de 2015, “Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos.
Ley 1712	Marzo 06 de 2014, “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
Decreto 886	Mayo 13 de 2014, “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos”.
Decreto 1377	Junio 23 de 2013, “Por el cual se reglamenta parcialmente la Ley 1581 de 2012”.
Ley 1581	Octubre 17 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013”.
Ley 1273	Enero 05 de 2009. Adiciona al título 7 al código penal. “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

6.3 Logros

La Corporación cuenta con la administración, operación y monitoreo 24/7 de su infraestructura informática y de telecomunicaciones, con los siguientes beneficios:

- Disponibilidad y Continuidad del Servicio: Se garantiza que los servicios críticos están siempre disponibles, minimizando el tiempo de inactividad y asegurando la continuidad operativa.
- Detección y Respuesta Rápida a Incidentes: Se permite la detección inmediata de incidentes de seguridad y fallos técnicos, facilitando una respuesta rápida y efectiva para mitigar posibles daños.
- Optimización de Recursos: Mejoramiento en la eficiencia en el uso de recursos tecnológicos y humanos, permitiendo una gestión más efectiva y reduciendo costos operativos a largo plazo.
- Cumplimiento Normativo: Cumplimiento de las normativas y regulaciones de seguridad y privacidad, evitando sanciones y mejorando la reputación de la entidad.
- Mejora de la Seguridad: Proporciona una vigilancia constante que ayuda a prevenir ataques cibernéticos y otras amenazas, protegiendo la integridad y confidencialidad de la información.
- Monitoreo Proactivo: Facilita el monitoreo proactivo de la infraestructura, identificando y resolviendo problemas potenciales antes de que afecten a los usuarios finales.
- Soporte Técnico Continuo: Asegurando que cualquier problema pueda ser resuelto rápidamente, sin importar la hora del día.
- Escalabilidad y Flexibilidad: Permite una gestión más flexible y escalable de la infraestructura, adaptándose a las necesidades cambiantes de la entidad pública.
- Reducción de Riesgos: Minimiza los riesgos asociados con la gestión de la infraestructura, incluyendo riesgos de seguridad, operativos y de cumplimiento.

6.4 Retos

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información enfrenta varios retos que se detallan a continuación:

- **Cultural de Seguridad Informática**: Fomentar una cultura de seguridad informática dentro de la Corporación
- **Adopción de Nuevas Tecnologías:** La implementación de nuevas tecnologías puede introducir nuevos riesgos que deben ser gestionados adecuadamente.

- **Concienciación y Formación:** Mantener a todo el personal informado y capacitado sobre las mejores prácticas de seguridad y privacidad es un reto continuo.

6.5 Riesgos de Seguridad y Privacidad de la Información identificados.

Ver anexo: Riesgos de Seguridad y Privacidad de la Información

7 Metodología empleada para la formulación

Teniendo en cuenta la aplicabilidad del ciclo PHVA (Planificar, Hacer, Verificar y Actuar) para lograr un ciclo de mejora continua en la gestión y tratamiento de riesgos, se definen las fases y las actividades, así:

- **Planear:** Dentro de esta etapa se desarrollan las actividades definidas en el Análisis de la información para el tratamiento de riesgos..
- **Hacer:** En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en el Desarrollo de las medidas de tratamiento de riesgos de la metodología del tratamiento de riesgos.
- **Verificar:** En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.
- **Actuar:** Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías y revisiones a los riesgos de seguridad y privacidad de la información.

8 Estructura programática

En este capítulo, va lo especificado en el punto 6.5 Riesgos de Seguridad y Privacidad de la Información identificados.

9 Líneas de acción para la mitigación del riesgo

La ejecución del Plan está sujeta a riesgos del entorno las cuales se relacionan en la siguiente tabla:

Tabla 2.*Gestión de riesgos para la ejecución del Plan.*

DESCRIPCIÓN RIESGO	AMENAZA

Incumplimiento de las políticas de seguridad de la información por parte los funcionarios y colaboradores poniendo en riesgo la continuidad de las operaciones, servicios y/o sistemas de la Corporación	Usuarios mal intencionados o por desconocimiento de la seguridad de la información ocasionan pérdida parcial o total de la información.
Acceso no autorizado a sistemas y servicios, o abuso de privilegios de funcionarios o contratistas sobre los sistemas o servicios que están bajo su responsabilidad.	Acciones indebidas de los funcionarios o contratistas con privilegios de acceso (Usuarios mal intencionados o con desconocimiento de los procesos, procedimientos y/o políticas de la Entidad)
Ausencia de requisitos de seguridad de la información en los contratos suscritos con proveedores y contratistas.	Fuga de información Divulgación de procedimientos o información sensible o crítica Configuración por default de componentes tecnológicos

Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnológica.	Incendio, inundación, terremoto, polvo Funcionarios con acceso a Datacenter, inconformes y/o sin conocimientos en seguridad de la información Códigos maliciosos Proveedores tecnológicos Ciberdelincuentes Ataques terroristas Disturbios civiles Interrupción de los servicios de la entidad y página web Indisponibilidad de la plataforma tecnológica Indisponibilidad del fluido eléctrico continuo en el centro de datos y PCs Indisponibilidad de los equipos de protección contra incendios en caso de emergencia

Riesgos de navegación de usuarios, privilegios de descarga e instalación y uso de software en los sistemas operativos de los equipos de cómputo y servidores	Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generado por virus informáticos. Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso
Afectación de equipos informáticos (equipos de cómputo, servidores, equipos de comunicaciones, seguridad, dispositivos móviles) ocasionado por conexiones de dispositivos de medios extraíbles, ejecución de enlaces, o archivos adjuntos, etc.	Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generado por virus informáticos. Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso

Pérdida, alteración o sustracción de Información en medio magnético o físico, dada en custodia al proveedor de Backup's o los usuarios	Funcionarios/contratistas, Proveedores externos, Ciberataques, servicios de suministro, amenazas naturales
Pérdida de la información generada por las actividades propias de la gestión del proceso - Copias de respaldo / restauración	Afectación en la disponibilidad del respaldo de la información Insuficiencia de espacio o almacenamiento para el aseguramiento de la información Pérdida o corrupción de los datos Corrupción de las cintas en el momento de las copias y la restauración del Backups Inexistencia de Backup de la información misional y de gestión

Ataques informáticos internos/externos a la infraestructura tecnológica (páginas web, software misional, hardware, aplicaciones, equipos de comunicación, equipos de seguridad, red interna)	Indisponibilidad de los servicios y/o página web Administradores de tecnología sin conocimientos técnicos de seguridad de la información. Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la plataforma tecnológica Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso
Indisponibilidad del canal de comunicación (internet, intranet)	Falla en el suministro de energía Fallas en los servicios ofrecidos por el proveedor

Gestión y uso inadecuado de las contraseñas	Usuarios sin conocimiento de las políticas, manual y procedimientos de seguridad de la información
Acceso no autorizado a las redes de la entidad (interna y externa)	Red sin protección, sin las herramientas o equipos tecnológicos de comunicación que aseguren al usuarios su correcto funcionamiento Fuga de información debido al acceso de usuarios no autorizados a la infraestructura de red de la entidad. Indisponibilidad del servicio de la red inalámbrica debido a ataques de denegación de servicios (DoS). Suplantación de identidad para acceder a los aplicativos tecnológicos de la entidad que se encuentran disponibles a través de la red de datos. Funcionarios descontentos pueden hacer uso de usuarios y contraseñas de personal que ya no labora en la entidad para visualizar y/o sustraer información confidencial de la entidad.

Acceso no autorizado a información enviada mediante mensajería electrónica	Fuga y/o pérdida de información Divulgación no autorizada de información debido a acceso de terceros Secuestro de información generado por una aplicación ramsomware.
Interceptación de información en tránsito provocada por una pérdida de la confidencialidad	Usuarios mal intencionados, Atacantes, Códigos maliciosos
Alteración, suplantación, divulgación y/o uso mal intencionado de la información sensible para la Entidad.	Funcionarios y/o Contratistas inconformes Atacantes externos,
Incumplimiento de la legislación y procedimientos vigentes	Funcionarios con desconocimiento en temas de contratación de personal Cambios en las regulaciones y lineamientos del gobierno que puedan impactar las operaciones de la Corporación Insuficiente protección y privacidad de información personal

Pérdida de la confidencialidad, integridad y disponibilidad de la información cifrada	Robo o hurto de información catalogada como sensible por falta de implementación de herramientas que aseguren el transporte de la información por la red Acceso a información privada, reservada o sensible sin la debida autorización.
Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia	Funcionarios con roles de seguridad de la información sin conocimiento Interrupción completa en la continuidad del negocio (Daño en Data Center, Servicios Tecnológicos y pérdida de la Información) Los usuarios realizan trabajo en casa, manipulan información, acceden a los sistemas de información desde las conexiones establecidas en el hogar Practicas inapropiada que afecten la disponibilidad de la información y la plataforma tecnológica
Indisponibilidad de los recursos tecnológicos ocasionada por una inadecuada gestión a la capacidad (procesamiento, almacenamiento, memoria)	Ausencia de revisiones periódicas por parte de los administradores de los recursos de la infraestructura tecnológica

Perdida de confidencialidad, integridad de la información en la ejecución de proyectos relacionados con la adquisición de bienes o servicios por parte del GIT Apoyo informático	Filtración y manipulación de la información para beneficio de un tercero
Perdida de confidencialidad, integridad y disponibilidad durante el ciclo de desarrollo en los sistemas de información ya sean nuevos o existentes - Acceso no autorizado a los códigos fuente y ambientes de desarrollo	Proveedores de sistemas de información, funcionarios con roles de desarrollo que no cumplen las políticas y requerimientos en seguridad Manipulación intencionada interna o externa de las fuentes de información ocasionando pérdida parcial y/o total del código fuente Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. Indisponibilidad de acceso a los repositorios de información o herramienta donde se resguarda el código fuente Secuestro de la información relacionada con el código fuente efectuado por un tercero a través de un malware Ataques cibernéticos sobre las plataformas desarrolladas internamente
Cambios en los sistemas de información gestionados inadecuadamente	Usuarios y administradores sin conocimiento de las políticas y procedimientos de seguridad de la información

Tratamiento no autorizado de datos personales	El desconocimiento del marco normativo relacionado con la protección de datos personales y los ataques informáticos podrían generar un tratamiento no autorizado de los datos personales generando demandas y sanciones, y pérdida de reputación.

Nota. Elaboración propia

10 Presupuesto

El presupuesto para el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027 de la Corporación, está incluida en las Iniciativas de Operación y Transformación Digital y Modernización Tecnológica que se relacionan en el PETIC 2024-2027.

11 Seguimiento al plan.

El seguimiento y evaluación al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027, se realizará conforme al cumplimiento de las actividades definidas en el numeral 6.5 Riesgos de Seguridad y Privacidad de la Información identificados.

Así pues, el proceso de seguimiento y evaluación permite contar con información objetiva y oportuna de utilidad para: tomar acciones que permitan mejorar la Gestión de TI orientada a la consecución de resultados.

El avance del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027 se evaluará semestralmente.

Estos informes serán presentados al Comité Directivo y serán difundidos al interior de la Corporación.

Como instancias de seguimiento, se tendrá el Comité de Dirección de CORANTIOQUIA.

El resultado del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024-2027 se interpretará de conformidad con los siguientes rangos de evaluación:

Nivel de ejecución (N.E) deficiente	Nivel de ejecución (N.E) aceptable	Nivel de ejecución (N.E) sobresaliente
N.E < 75 %	75 % ≤ N.E ≤ 90 %	90 % < N.E ≤ 100 %

Figura 3 Seguimiento al plan Nivel de ejecución

12 Referencias

Acuerdo Consejo Directivo 575. (diciembre de 2019). por el cual se aprueba el Plan de Gestión Ambiental Regional PGAR 2020-2031. (Corantioquia, Ed.) Medellín, Antioquia, Colombia: Consejo Directivo.

Consejo Directivo. (19 de mayo de 2016). Plan de Acción 2016-2019. Medellín, Antioquia, Colombia: Corantioquia.

Decreto 612. (4 de abril de 2018). Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. Bogotá, D.C., Colombia: Presidencia de la República.

DNP. (2014). Guía metodológica para el Seguimiento y la Evaluación a Políticas Públicas. (D. d. Públicas, Ed.) Bogotá, D.C., Colombia: Departamento Nacional de Planeación.

Función Pública. (agosto de 2019). Valores del servicio público. Código de intedridad. Bogotá, D.C., Colombia: Departamento Administrativo de la Función Pública.

Resolución 040-RES2010-5718. (7 de octubre de 2020). Por medio de la cual se actualiza la política del sistema de gestión integral (SGI) de la Corporación Autónoma Regional del Centro de Antioquia (Corantioquia). Medellín, Antioquia, Colombia: Corantioquia.

Resolución n.° 040-RES1801-405. (31 de enero de 2018). Por la cual se aprueba y adopta el Plan Anticorrupción y de Atención al Ciudadano para el año 2018. Medellín, Antioquia, Colombia: Corantioquia.

Resolución n.° 040-RES2112-9588. (31 de diciembre de 2021). Por la cual se adopta el código de integridad corporativo. Medellín, Antioquia, Colombia: Corantioquia.

SINA. (2018). Plan de Acción Sectorial Ambiental del Mercurio. Bogotá, D.C., Colombia.

DOMINIO ARQUITECTURA DE TI	PONDERACIÓN	OBJETIVO	INICIATIVA
Estrategia de TI	5%	Definir e implementar la estrategia de TI bajo el modelo de gestión IT4+ para contribuir al mejoramiento de la gestión.	Implementar tecnologías de la IV y V Revolución Industrial (Sistemas de Inteligencia de Negocios, BigData, Analítica de Datos, Machine Learning, IoT, Robótica y Colaboración Abierta) que apoye la toma de decisiones y genere nuevo conocimiento en los procesos corporativos.
Estrategia de TI		Actualizar el Modelo de Seguridad y Privacidad de la Información, alineado al Plan de Seguridad y Privacidad de la Información y al Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Planes Institucionales y Estratégicos de Tecnología alineados al PETIC.
Gobierno de TI	5%	Alinear la estrategia de TI definida en el PETIC con el PGAR y Plan de Acción de la Corporación.	Implementar el Modelo Operativo de Tecnologías de la Información y las Comunicaciones - Fortalecimiento de la capacidad operativa (Crear la Oficina de TIC).
Gestión de Información	10%	Diseñar los servicios de información para el análisis y desarrollo de capacidades para su uso estratégico que apoye la toma de decisiones.	Actualizar la página web e intranet de la Corporación según la norma técnica NTC 5854 y lineamientos del MINTIC.
Gestión de Información		Mantener el Portal Geográfico de la Corporación actualizado, que incluye soporte tecnico y mantenimiento.	Actualizar el Portal Geográfico de la Corporación, con su respectivo soporte y mantenimiento.
Gestión de Sistemas de Información	25%	Garantizar el correcto funcionamiento de los sistemas de información de la Corporación para contribuir al mejoramiento de la gestión.	Transformar la experiencia de los ciudadanos con los trámites y servicios por medios electrónicos, asegurando la promoción, la efectividad y la simplicidad (Interoperabilidad de las aplicaciones corporativas de carácter estratégica, misional y de apoyo con otras Entidades del Estado Nacionales y Territoriales), de conformidad con el nuevo el nuevo Modelo de Gestión y Operación de Administración de los Recursos Naturales Renovables.

Gestión de Sistemas de Información		Garantizar el correcto funcionamiento de los sistemas de información de la Corporación para contribuir al mejoramiento de la gestión.	Modernizar el Sistema de Información en la Administración de los Recursos Naturales, para la Corporación Autónoma Regional del Centro de Antioquia - Corantioquia. Incluye Software como Servicio (SaaS)
Gestión de Sistemas de Información		Garantizar el correcto funcionamiento de los sistemas de información de la Corporación para contribuir al mejoramiento de la gestión.	Implementar sistemas de información y tecnologías enfocadas a las comunidades étnicas jurisdicción de la Corporación.
Gestión de Sistemas de Información		Garantizar el correcto funcionamiento de los sistemas de información de la Corporación para contribuir al mejoramiento de la gestión.	Fortalecer el Modelo de Atención al Ciudadano a través de la implementación de asesores virtuales.
Gestión de Sistemas de Información		Facilitar el acceso a la información de las bases de datos bibliográficas a los usuarios internos y externos.	Prestar el servicio de actualización, soporte y mantenimiento al Sistema Koha.
Gestión de Sistemas de Información		Garantizar el correcto funcionamiento de los sistemas de información de la Corporación para contribuir al mejoramiento de la gestión.	Actualizar licencias ArcGis, con su respectivo soporte y mantenimiento.
Gestión de Sistemas de Información		Garantizar el correcto funcionamiento de los sistemas de información de la Corporación para contribuir al mejoramiento de la gestión.	Actualización, soporte y mantenimiento de los módulos del Sistema de Información Administrativo, Financiero, Contable y Fiscal.
Gestión de Sistemas de Información		Garantizar el correcto funcionamiento de los sistemas de información de la Corporación para contribuir al mejoramiento de la gestión.	Realizar el soporte y mantenimiento de las aplicaciones Sirena, Facturación y Cartera y Laboratorio.
Gestión de Sistemas de Información		Garantizar el correcto funcionamiento de los sistemas de información de la Corporación para contribuir al mejoramiento de la gestión.	Realizar la adquisición, instalación, configuración, pruebas, puesta en funcionamiento y soporte de solución para la gestión de requerimientos e incidentes y gestión de inventarios tecnológicos.
Gestión de Sistemas de Información		Garantizar el correcto funcionamiento de los sistemas de información de la Corporación para contribuir al mejoramiento de la gestión.	Realizar la adquisición de equipo, renovación del licenciamiento y acuerdo de soporte de la solución firewall de la Corporación por tres (3) años.

Gestión de Sistemas de Información		Modernizar el manejo documental de la Corporación, mediante un sistema informático que contenga los componentes de un sistema de gestión documental.	Adquisición e implementación de un software de gestión documental.
Gestión de Servicios de TI	25%	Garantizar el correcto funcionamiento de la Infraestructura Tecnológica y de Telecomunicaciones de la Corporación para contribuir al mejoramiento de la gestión.	Implementar tecnología de punta en el ejercicio de la autoridad ambiental y gestión de territorios sostenibles: equipos móviles (tablets, GPS, drones, entre otros) y aplicaciones.
Gestión de Servicios de TI		Garantizar el correcto funcionamiento de la Infraestructura Tecnológica y de Telecomunicaciones de la Corporación para contribuir al mejoramiento de la gestión.	Mejorar la conectividad en los diferentes centros de trabajo (Sede Central, Oficinas Territoriales, Sedes locales, Viveros y CAV).
Gestión de Servicios de TI		Garantizar el correcto funcionamiento de la Infraestructura Tecnológica y de Telecomunicaciones de la Corporación para contribuir al mejoramiento de la gestión.	Migrar la Infraestructura Tecnológica de la Corporación a servicios de nube e híbrida (incluye migración de la infraestructura informática y de telecomunicaciones, sistemas de almacenamiento, sistemas de backups) según los lineamientos del MINTIC y la Directiva Presidencial 03 de 2021.
Gestión de Servicios de TI		Garantizar el correcto funcionamiento de la Infraestructura Tecnológica y de Telecomunicaciones de la Corporación para contribuir al mejoramiento de la gestión.	Adquirir y renovar equipos tecnológicos de última generación de acuerdo con las necesidades de los procesos.
Gestión de Servicios de TI		Garantizar el correcto funcionamiento de la Infraestructura Tecnológica y de Telecomunicaciones de la Corporación para contribuir al mejoramiento de la gestión.	Disponer de las apropiaciones presupuestales necesarias con el fin de modernizar el Data Center de la Corporación de conformidad con la norma ANSI/TIA 942, Telecommunications Infrastructure for Data Centers Standard, ANSI/BICSI 002-2014.
Gestión de Servicios de TI		Garantizar el correcto funcionamiento de la Infraestructura Tecnológica y de Telecomunicaciones de la Corporación para contribuir al mejoramiento de la gestión.	Implementar herramientas tecnológicas para el Teletrabajo.

Gestión de Servicios de TI		Garantizar el correcto funcionamiento de la Infraestructura Tecnológica y de Telecomunicaciones de la Corporación para contribuir al mejoramiento de la gestión.	Prestar los servicios especializados que garanticen el buen funcionamiento de la Infraestructura Informática y de Telecomunicaciones de la Corporación Autónoma Regional del Centro de Antioquia – CORANTIOQUIA, que incluya el servicio de Mesa de Ayuda para mejorar la prestación de los servicios tecnológicos de la Corporación.
Gestión de Servicios de TI		Garantizar el correcto funcionamiento de la Infraestructura Tecnológica y de Telecomunicaciones de la Corporación para contribuir al mejoramiento de la gestión.	Realizar el mantenimiento preventivo y correctivo a equipos de cómputo (todo en uno, portátiles y estaciones de trabajo), y tecnológicos y periféricos tales como, impresoras, plotter, escáneres, video proyectores, datamax, accesorios y/o equipos de telecomunicaciones de la Entidad.
Uso y Apropiación de TI	30%	Promover la cultura de las Tecnologías de la Información y las Comunicaciones a las partes interesadas de la Corporación con el fin de lograr participación, sensibilización y liderazgo en las iniciativas de TI.	Capacitar al personal de la Corporación y al equipo TIC en el uso y apropiación de las TIC, sistemas de información, herramientas, licencias y Moodle.
Uso y Apropiación de TI		Formular e implementar el Modelo de Seguridad y Privacidad de la Información contribuyendo al desarrollo y ejecución del Plan de Acción de la Corporación.	Realizar la adquisición, instalación, configuración, pruebas, puesta en funcionamiento y soporte de una solución web para firma digital de documentos, con certificados de firma digital y sus respectivos tokens.
Uso y Apropiación de TI		Formular e implementar el Modelo de Seguridad y Privacidad de la Información contribuyendo al desarrollo y ejecución del Plan de Acción de la Corporación.	Contar con el licenciamiento necesario para el correcto funcionamiento del software Corporativo.

TIPO DE INICIATIVA	PRIORIDAD	PROYECTO - ACTIVIDAD PLAN DE ACCIÓN	INDICADOR	META 2024	META 2025
Transformación Digital y Modernización Tecnológica	3. Baja	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Implementación de Tecnologías de la IV y V Revolución Industrial.	0	0
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Modelo actualizado de Seguridad y Privacidad de la Información	0%	100%
Transformación Digital y Modernización Tecnológica	2. Media	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Modelo Operativo de Tecnologías de la Información y las Comunicaciones implementado.	0%	0%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Página Web actualizada según NTC 5854.	100%	100%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Portal Geográfico actualizado.	100%	100%
Transformación Digital y Modernización Tecnológica	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Implementación de Trámites en Línea.	0%	100%

Transformación Digital y Modernización Tecnológica	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Modernizar el Sistema de Información en la Administración de los Recursos Naturales.	0%	100%
Transformación Digital y Modernización Tecnológica	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Implementación Sistema de Información Comunidades Étnicas.	0%	0%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Implementación de Asesores Virtuales.	0%	100%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Bases de Datos bibliográgicas con acceso abierto.	100%	100%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Licencias ArcGis actualizadas.	100%	100%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Actualización, soporte y mantenimiento del Sistema de Información Administrativo, Financiero, Contable y Fiscal.	100%	100%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Actualización, soporte y mantenimiento de las aplicaciones Sirena, Facturación y Cartera y Laboratorio.	100%	100%
Transformación Digital y Modernización Tecnológica	3. Baja	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Implementación de solución para gestión de requerimientos e incidentes.	0%	0%
Transformación Digital y Modernización Tecnológica	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Soporte y licenciamiento del Firewall.	100%	100%

Transformación Digital y Modernización Tecnológica	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Software de gestion documental implementando.	0%	100%
Transformación Digital y Modernización Tecnológica	2. Media	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Implementación de tecnología en el ejercicio de la Autoridad Ambiental.	0%	100%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Mejora de la conectividad en centros de trabajo.	100%	100%
Transformación Digital y Modernización Tecnológica	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Implementación de sistemas de almacenamiento en la nube.	0%	100%
Transformación Digital y Modernización Tecnológica	2. Media	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Renovación de equipos tecnológicos.	0%	100%
Transformación Digital y Modernización Tecnológica	2. Media	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Modernización física del Data Center.	100%	100%
Transformación Digital y Modernización Tecnológica	3. Baja	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Implementación de herramientas tecnológicas para el Teletrabajo.	0%	100%

Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Soporte, monitoreo y administración de la Infraestructura Informática y de Telecomunicaciones.	100%	100%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Mantenimiento de Equipos de Cómputo, Tecnológicos y Periféricos.	100%	100%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan estratégico de tecnologías de la información y las comunicaciones - PETIC 2024-2027	Capacitación al personal de la Corporacion y al equipo TIC.	0	1
Transformación Digital y Modernización Tecnológica	1. Alta	Porcentaje de avance de la formulación e implementación del Plan de Seguridad y Privacidad de la Información	Implementación de Firma Digital.	100%	100%
Operación	1. Alta	Porcentaje de avance de la formulación e implementación del Plan de Seguridad y Privacidad de la Información	Licenciamiento del software corporativo que mejore la seguridad informática.	100%	100%

TOTAL	

META 2026	META 2027	META 2024-2027	VIGENCIA DE EJECUCIÓN	DISTRIBUCIÓN EJECUCIÓN 2024	DISTRIBUCIÓN EJECUCIÓN 2025	DISTRIBUCIÓN EJECUCIÓN 2026	DISTRIBUCIÓN EJECUCIÓN 2027
1	1	2	2026-2027	$ -	$ -	$ 200,000,000	$ 200,000,000
0%	0%	1	2025	$ -	$ -	$ -	$ -
0%	100%	1	2027	$ -	$ -	$ -	$ -
100%	100%	4	2024-2025-2026-2027	$ 25,000,000	$ 25,000,000	$ 25,000,000	$ 25,000,000
100%	100%	4	2024-2025-2026-2027	$ 86,750,000	$ 86,750,000	$ 86,750,000	$ 86,750,000
100%	100%	3	2025-2026-2027	$ -	$ 100,000,000	$ 100,000,000	$ 100,000,000

0%	0%	1	2025	$ -	$ 1,600,000,000	$ -	$ -
100%	100%	2	2026-2027	$ -	$ -	$ 250,000,000	$ 250,000,000
0%	0%	1	2025	$ -	$ 30,000,000	$ -	$ -
100%	100%	4	2024-2025-2026-2027	$ 19,000,000	$ 19,000,000	$ 19,000,000	$ 19,000,000
100%	100%	4	2024-2025-2026-2027	$ 191,250,000	$ 191,250,000	$ 191,250,000	$ 191,250,000
100%	100%	4	2024-2025-2026-2027	$ 320,000,000	$ 457,734,293	$ 457,734,293	$ 457,734,293
100%	100%	4	2024-2025-2026-2027	$ 375,000,000	$ 375,000,000	$ 375,000,000	$ 375,000,000
100%	0%	1	2026	$ -	$ -	$ 200,000,000	$ -
0%	100%	3	2024-2025-2027	$ 397,000,000	$ 600,000,000	$ -	$ 473,000,000

100%	100%	3	2025-2026-2027	$ -	$ 433,333,333	$ 433,333,333	$ 433,333,333
100%	100%	3	2025-2026-2027	$ -	$ 90,000,000	$ 90,000,000	$ 90,000,000
100%	100%	4	2024-2025-2026-2027	$ 360,488,931	$ 486,503,690	$ 486,503,690	$ 486,503,690
100%	100%	3	2025-2026-2027	$ -	$ 1,428,948,188	$ 1,428,948,188	$ 1,428,948,188
100%	100%	3	2025-2026-2027	$ -	$ 600,000,000	$ 600,000,000	$ 400,000,000
100%	100%	4	2024-2025-2026-2027	$ 145,000,000	$ 145,000,000	$ 145,000,000	$ 145,000,000
0%	0%	1	2025	$ -	$ 100,000,000	$ -	$ -

100%	100%	4	2024-2025-2026-2027	$ 333,006,000	$ 807,664,667	$ 807,664,667	$ 807,664,667
100%	100%	4	2024-2025-2026-2027	$ 180,000,000	$ 215,000,000	$ 215,000,000	$ 215,000,000
1	1	3	2025-2026-2027	$ -	$ -	$ -	$ -
100%	100%	4	2024-2025-2026-2027	$ 400,000,000	$ 400,000,000	$ 400,000,000	$ 400,000,000
100%	100%	4	2024-2025-2026-2027	$ 1,774,000,000	$ 1,774,000,000	$ 1,774,000,000	$ 1,774,000,000
				$ 4,606,494,931	$ 9,965,184,171	$ 8,285,184,171	$ 8,358,184,171

TOTAL	Seguimiento 2024-I	Seguimiento 2024-II	Seguimiento 2024-III	Seguimiento 2024-IV	Resultado semestre I 2024
$ 400,000,000					
$ -					
$ -					
$ 100,000,000					
$ 347,000,000					
$ 300,000,000					

$ 1,600,000,000					
$ 500,000,000					
$ 30,000,000					
$ 76,000,000					
$ 765,000,000					
$ 1,693,202,880					
$ 1,500,000,000					
$ 200,000,000					
$ 1,470,000,000					

$ 1,300,000,000					
$ 270,000,000					
$ 1,820,000,000					
$ 4,286,844,564					
$ 1,600,000,000					
$ 580,000,000					
$ 100,000,000					

$ 2,756,000,000					
$ 825,000,000					
$ -					
$ 1,600,000,000					
$ 7,096,000,000					

$ 31,215,047,444	Total PETIC	0

% cumplimiento semestre I 2024	Evaluación por dominio semestre I 2024	Resultado semestre II 2024	% cumplimiento semestre II 2024	Evaluación por dominio semestre II 2024	Seguimiento 2025-I	Seguimiento 2025-II

0%	0%	0	0	0%

Seguimiento 2025-III	Seguimiento 2025-IV	Resultado semestre I 2025	% cumplimiento semestre I 2025	Evaluación por dominio semestre I 2025	Resultado semestre II 2025	% cumplimiento semestre II 2025

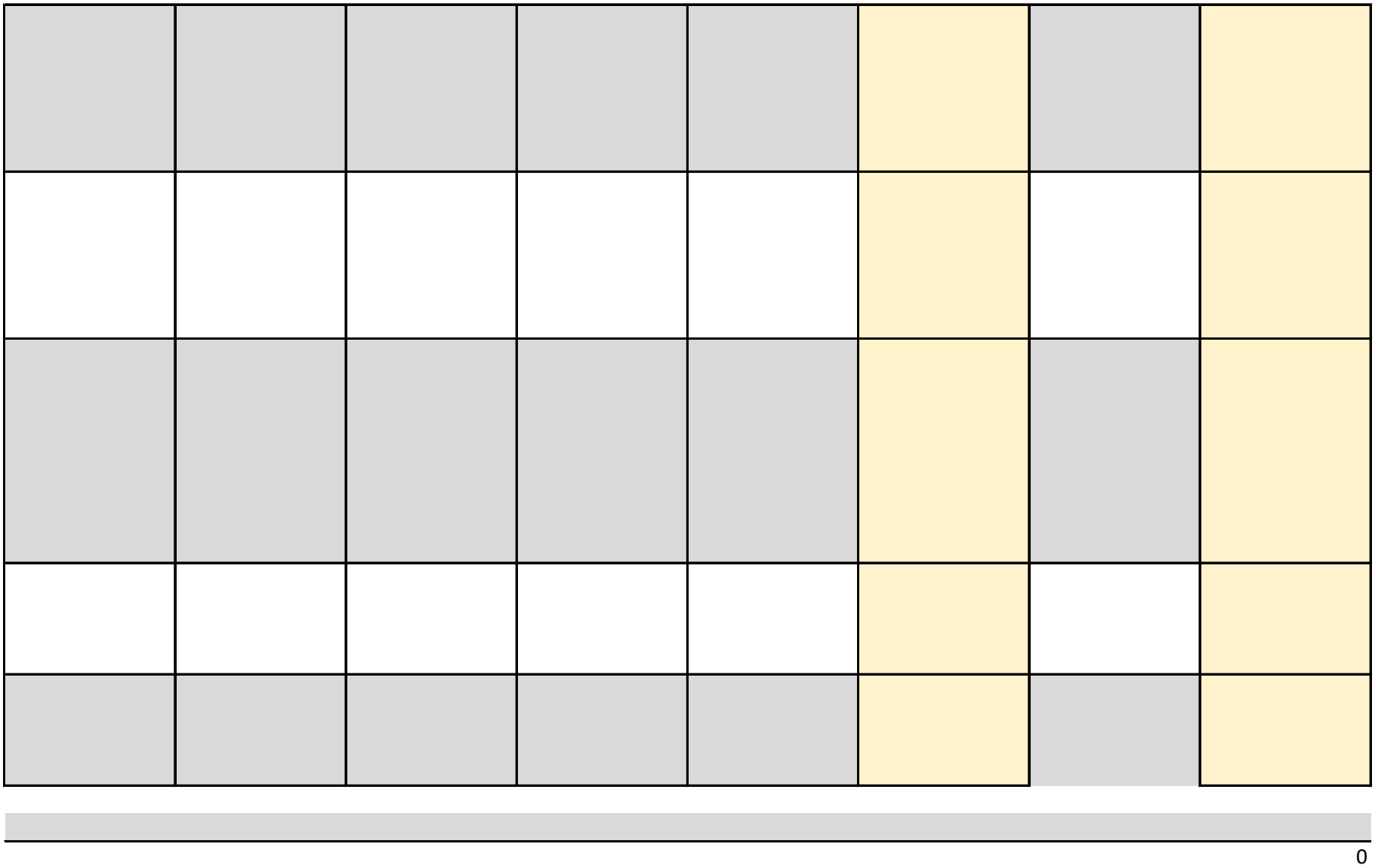
Total PETIC		0	0	0%	0%	0%

Evaluación por dominio semestre II 2025	Seguimiento 2026-I	Seguimiento 2026-II	Seguimiento 2026-III	Seguimiento 2026-IV	Resultado semestre I 2026	% cumplimiento semestre I 2026	Evaluación por dominio semestre I 2026

0%

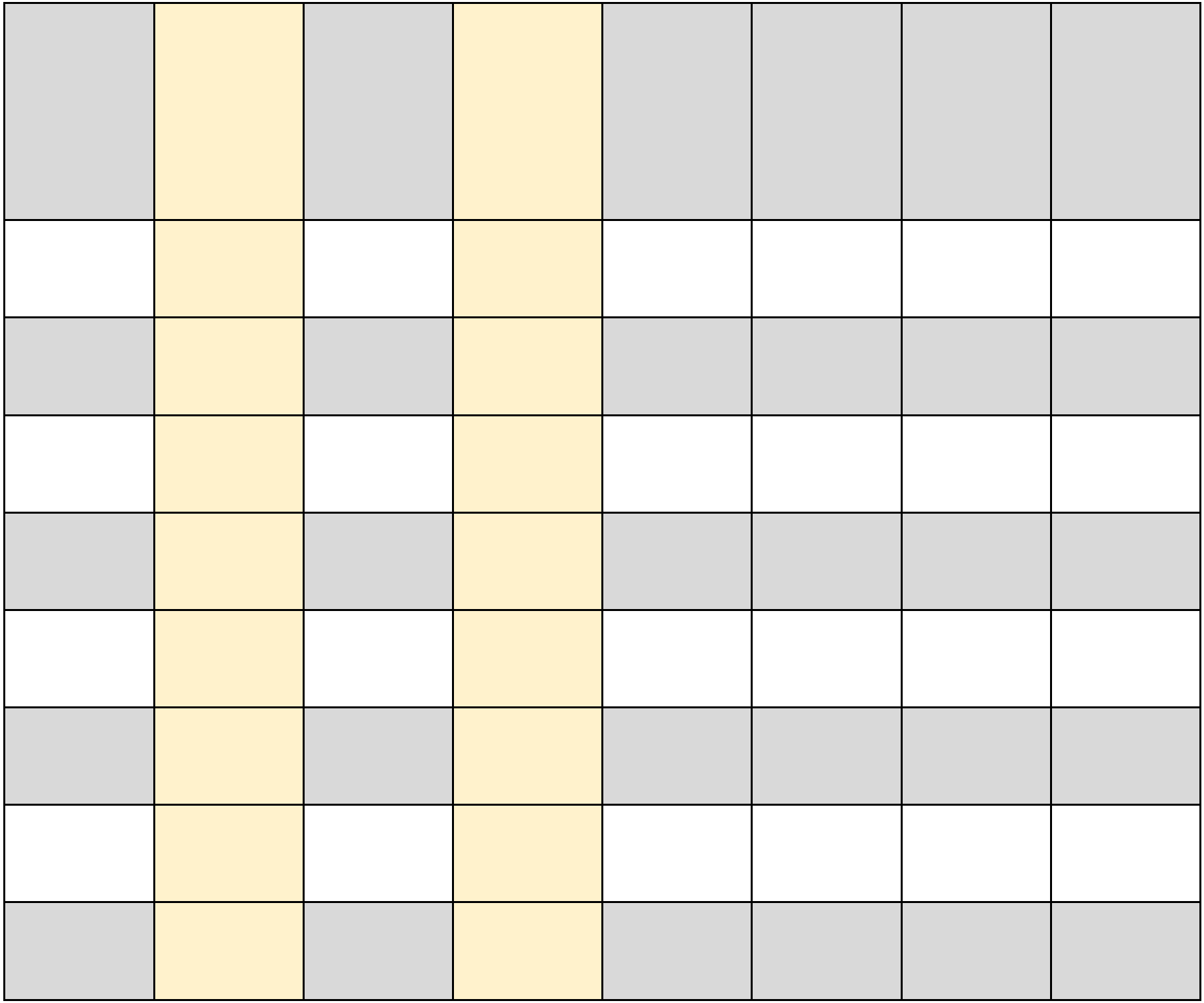
Resultado semestre II 2026	% cumplimiento semestre II 2026	Evaluación por dominio semestre II 2026	Seguimiento 2027-I	Seguimiento 2027-II	Seguimiento 2027-III	Seguimiento 2027-IV	Resultado semestre I 2027

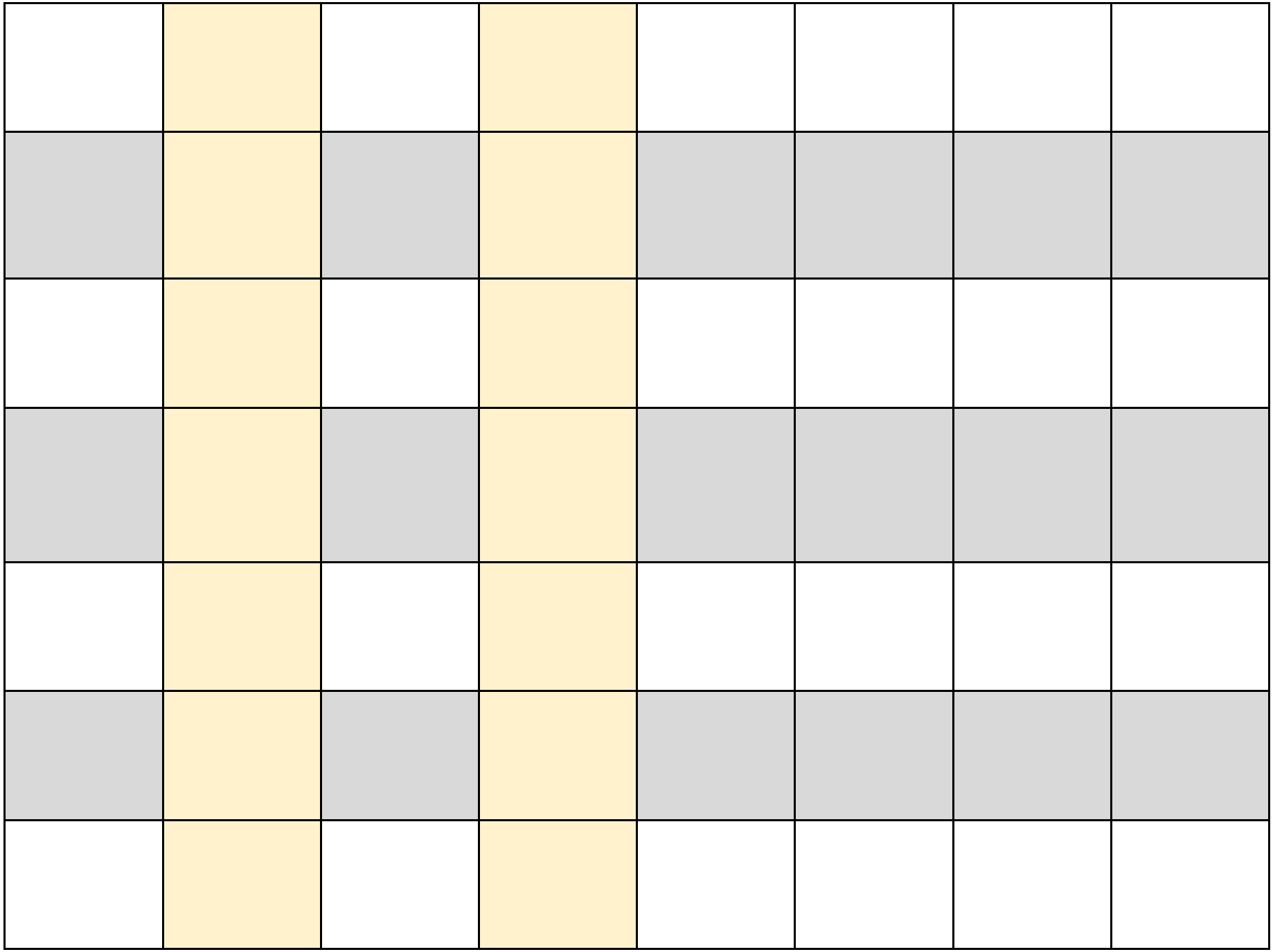
% cumplimiento semestre I 2027	Evaluación por dominio semestre I 2027	Resultado semestre II 2027	% cumplimiento semestre II 2027	Evaluación por dominio semestre II 2027	Ejecución financiera semestre I 2024	% ejecución financiera semestre I 2024	Ejecución financiera semestre II 2024



0

% ejecución financiera semestre II 2024	Ejecución financiera semestre I 2025	% ejecución financiera semestre I 2025	Ejecución financiera semestre II 2025	% ejecución financiera semestre II 2025	Ejecución financiera semestre I 2026	% ejecución financiera semestre I 2026	Ejecución financiera semestre II 2026



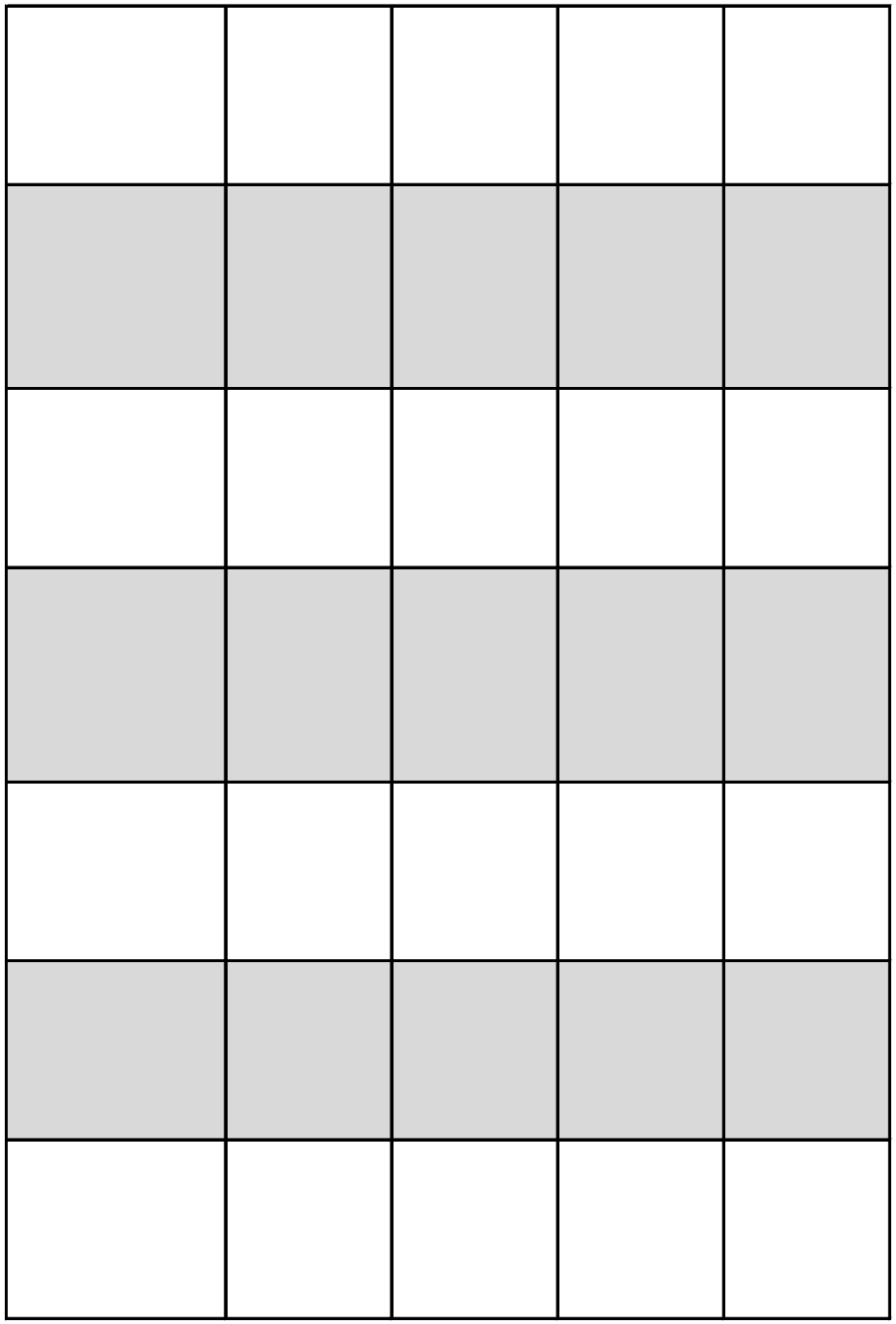


#¡DIV/0!	0	#¡DIV/0!	0	#¡DIV/0!

% ejecución financiera semestre II 2026	Ejecución financiera semestre I 2027	% ejecución financiera semestre I 2027	Ejecución financiera semestre II 2027	% ejecución financiera semestre II 2027	Ejecución financiera 2024	% ejecución financiera 2024	Ejecución financiera 2025

0	#¡DIV/0!	0

% ejecución financiera 2025	Ejecución financiera 2026	% ejecución financiera 2026	Ejecución financiera 2027	% ejecución financiera 2027



#¡DIV/0!

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024-2027 - CORANTIOQUIA

FORMATO DE DESCRIPCIÓN DEL RIESGO

Nro.	ACTIVOS	RIESGO	DESCRIPCIÓN RIESGO	AMENAZA	TIPO	CAUSA / VULNERABILIDAD	CONSECUENCIA	PROCESO AL QUE APLICA	RIESGO INICIAL O INHERENTE		
									CALIFICACIÓN		EVALUACIÓN
									PROBABILIDAD	IMPACTO	
1	TALENTO HUMANO	Pérdida de Confidencialidad	Incumplimiento de las políticas de seguridad de la información por parte los funcionarios y colaboradores poniendo en riesgo la continuidad de las operaciones, servicios y/o sistemas de la Corporación	Usuarios mal intencionados o por desconocimiento de la seguridad de la información ocacionan pérdida parcial o total de la información.	Seguridad de la Información	Desconocimiento de los lineamientos sobre la seguridad de la información institucionales Desactualización de la Política y Manual de seguridad de la información Uso y apropiación insuficiente de las políticas, manual y procedimientos de seguridad de la información Falta de competencias del personal a cargo del cumplimiento de las responsabilidades de la seguridad de la información asignadas Falta o insuficiente descripción de los roles y responsabilidades sobre seguridad de la información en los documentos de contratación	Incumplimiento de políticas de seguridad de la información Indisponibilidad de los servicios	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	CASI SEGURO	MAYOR	EXTREMO
2	TALENTO HUMANO INFORMACION	Pérdida de Confidencialidad	Acceso no autorizado a sistemas y servicios, o abuso de privilegios de funcionarios o contratistas sobre los sistemas o servicios que estan bajo su responsabilidad.	Acciones indebidas de los funcionarios o contratistas con privilegios de acceso (Usuarios mal intencionados o con desconocimiento de los procesos, procedimientos y/o políticas de la Entidad)	Seguridad de la Información	Ausencia de implementación de procedimientos en la gestión de usuarios que incluya registro de usuarios, cancelacion de usuarios, asignación y anulación de derechos de acceso. Ausencia de gestión sobre las vulnerabilidades técnicas Trabajo no supervisado de personal externo o de limpieza	Afectación a la disponibilidad de acceso a los sistemas y servicios de la Corporación	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	IMPROBABLE	MAYOR	ALTO
3	INFORMACIÓN	Pérdida de Disponibilidad	Ausencia de requisitos de seguridad de la información en los contratos suscritos con proveedores y contratistas.	Fuga de información Divulgación de procedimientos o información sensible o crítica Configuración por default de componentes tecnológicos	Seguridad de la Información	Falta de implementación de procedimientos o políticas adecuadas en seguridad de la información en las actividades, servicios o procesos aplicadas a los proveedores y/o contratistas en la labor contratada	Perdida de confidencialidad y disponibilidad de la información y posibles Ataques a la integridad de los datos	GESTIÓN DE TIC	RARA VEZ	MODERADO	MODERADO
4	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Disponibilidad	Daño de información y/o físico en las instalaciones de procesamiento de datos (Datacenter) o Interrupción de la Operación de la Plataforma Tecnológica.	Incendio, inundación, terremoto, polvo Funcionarios con acceso a Datacenter, inconformes y/o sin conocimientos en seguridad de la información Códigos maliciosos Proveedores tecnológicos Ciberdelincuentes Ataques terroristas Disturbios civiles Interrupción de los servicios de la entidad y página web Indisponibilidad de la plataforma tecnológica Indisponibilidad del fluido eléctrico continuo en el centro de datos y PCs Indisponiobilidad de los equipos de protección contra incendios en caso de emergencia	Seguridad de la Información	Ausencia de planes de emergencia y pruebas al mismo. Ausencia de redes contra incendio, condiciones inadecuadas de temperatura y humedad que generan daños sobre la infraestructura física Acciones fortuitas o malintencionados en el centro de computo, ocasionando pérdida parcial o total de la información alojada en los equipos. Conexión de equipos a corriente no regulada Debilidad en la infraestructura tecnológica, ausencia de un sistema de control de acceso. Falta de mantenimiento a equipos de usuarios y a la plataforma tecnologíca Hardware y software obsoletos y sin garantía Encargado del componente no se encuentra disponible y no existe un rol de respaldo de éste. Gestión inadecuada de la capacidad de los equipos, falla en las UPS o aires acondicionados. Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos) Ausencia de redundancias para los servicios críticos	Interrupción completa de los servicios ofrecidos por la Corporación Perdida de información que puede poner en riesgo la continuidad de las operaciones de la Corporación Hurto y/o daño de la infraestructura tecnológica (Servidores, Dispositivos de red, etc.) que se encuentra alojada en el datacenter debido a la ausencia de controles de acceso Pérdida de credibilidad de las partes interesadas	GESTIÓN DE TIC	IMPROBABLE	MAYOR	ALTO
5	HARDWARE SOFTWARE Y SERVICIOS	Perdida de Integridad	Riesgos de navegación de usuarios, privilegios de descarga e instalación y uso de software en los sistemas operativos de los equipos de cómputo y servidores	Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generado por virus informáticos. Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso	Seguridad de la Información	Ausencia de políticas y controles restrictivos para la instalación de software no autorizado Uso e instalación de software con vulnerabilidades Perfiles y privilegios no asignados Descarga de virus informáticos maliciosos (Spiware, troyanos, virus, gusanos)	Interrupción de las operaciones y/o afectación en la prestación del servicio Suspencion temporal, parcial o permanentes de las actividades a desarrollar por parte de los funcionarios Afectación de la continuidad del negocio debido al secuestro de la información ocasionado por código malicioso. Sustracción no autorizada de información confidencial de la organización, afectando la continuidad del negocio. Daño de hardware ocasionado por código malicioso, provocando en la entidad la asignación de presupuesto extra para la reposición del hardware.	GESTIÓN DE TIC	IMPROBABLE	MAYOR	ALTO
6	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Perdida de Integridad	Afectación de equipos informáticos (equipos de cómputo, servidores, equipos de comunicaciones, seguridad, dispositivos móviles) ocasionado por conexiones de dispositivos de medios extraibles, ejecución de enlaces, o archivos adjuntos, etc.	Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generado por virus informáticos. Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso	Seguridad de la Información	Base de datos de antivirus desactualizada. Usuarios con privilegios de uso de medios removibles Equipos informaticos sin licencia o con software desactualizados	Posibles fallos de seguridad o vulnerabilidades en los equipos informáticos y/o perdida de información sensible y confidencial de la Corporación Afectación de la continuidad del negocio debido al secuestro de la información ocasionado por código malicioso. Sustracción no autorizada de información confidencial de la organización, afectando la continuidad del negocio. Daño de hardware ocasionado por código malicioso, provocando en la entidad la asignación de presupuesto extra para la reposición del hardware.	GESTIÓN DE TIC	IMPROBABLE	MODERADO	MODERADO
7	INFORMACIÓN TALENTO HUMANO	Pérdida de Disponibilidad	Pérdida, alteración o sustracción de Información en medio magnético o físico, dada en custodia al proveedor de Backup's o los usuarios	Funcionarios/contratistas, Proveedores externos, Ciberataques, servicios de suministro, amenazas naturales	Seguridad de la Información	Manipulación, transporte y almacenamiento inadecuado a las cintas de backups. Ausencia de pruebas regulares a las copias de respaldo. Incumplimiento al acuerdo de confidencialidad Manipulación inadecuada de la documentación recepcionada por el personal de la Entidad. Falta de valores y compromiso con la Entidad Intereses a favor de terceros Incumplimiento de los Roles y Responsabilidades para la seguridad de la Información.	Perdida de la información y posibles ataques a la integridad de los datos.	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	POSIBLE	CATASTROFICO	EXTREMO

8	INFORMACIÓN TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Disponibilidad	Pérdida de la información generada por las actividades propias de la gestión del proceso - Copias de respaldo / restauracion	Afectación en la disponibilidad del respaldo de la información Insuficiencia de espacio o almacenamineto para el aseguramiento de la informacion Pérdida o corrupción de los datos Corrupción de las cintas en el momento de las copias y las restauración del Backups Inexistencia de backup de la información misional y de gestión	Seguridad de la Información	Ausencia de medidas para evitar la pérdida de datos, por ejemplo copias de respaldo. Falta de pruebas regulares a las copias de respaldo. Ausencia de manuales para la administración de las herramientas de aplicaciones. Administrador de servidores sin conocimiento de las políticas de seguridad de la información. El respaldo de backup está ubicado en los mismos servidores a los cuáles se les realiza las copias de respaldo	Perdida de confidencialidad y disponibilidad de la información para los usuarios internos y externos.	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	IMPROBABLE	MAYOR	ALTO
9	TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Integridad	Ataques informáticos internos/externos a la infraestructura tecnológica (páginas web, software misional, hardware, aplicaciones, equipos de comunicación, equipos de seguridad, red interna)	Indisponibilidad de los servicios y/o página web Administradores de tecnología sin conocimientos técnicos de seguridad de la información. Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la plataforma tecnológica Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso	Seguridad de la Información	Vulnerabilidades técnicas sin conocer, uso de software desactualizado Intrusión de personal no autorizado a la plataforma tecnológica Acceso sin autorización locales, remotos y a los centros de cableado o de la UPS Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos) Falta de políticas, controles de seguridad, no existen procedimientos establecidos para la restricción de acceso a la infraestructura física de la organización Falta de socializacion acerca de las diferentes modalidades de ciberataques	Perdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos. Afectación a toda la Entidad Suplantacion de identidad Afectación de la continuidad del negocio debido al secuestro de la información ocasionado por código malicioso. Sustracción no autorizada de información confidencial de la organización, afectando la continuidad del negocio. Daño de hardware ocasionado por código malicioso, provocando en la entidad la asignación de presupuesto extra para la reposición del hardware. Pérdida de la buena imágen de la Entidad por fallas en sus servicios o página web, ocasionado por un ataque de denegación de servicios	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	IMPROBABLE	MAYOR	ALTO
10	HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Disponibilidad	Indisponibilidad del canal de comunicación (internet, intranet)	Falla en el suministro de energía Fallas en el servicios ofrecidos por el proveedor	Seguridad de la Información	Ausencia de canal de respaldo, acuerdos de nivel de servicio con el proveedor sin establecer. Falta de respaldo de los servicios de suministro (aire, energía, entre otros).	Afectación a la disponibilidad de los servicios de la Corporación	GESTIÓN DE TIC	PROBABLE	MAYOR	EXTREMO
11	INFORMACIÓN TALENTO HUMANO	Pérdida de Confidencialidad	Gestión y uso inadecuado de las contraseñas	Usuarios sin conocimiento de las políticas, manual y procedimientos de seguridad de la información	Seguridad de la Información	Ausencia de políticas para la gestión y uso de contraseñas Falta de sensibilización y capacitación en el manejo y uso de contraseñas Personal inconforme al interior de la Entidad o poco compromiso ante las políticas de Seguridad de la Información. Robo o usurpación de contraseñas	Incumplimiento de las políticas de seguridad de la información Ingresos no autorizados en los sistema de informacion, plataforma tecnologica, etc Robo de informacion	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	POSIBLE	MAYOR	EXTREMO
12	TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Confidencialidad	Acceso no autorizado a las redes de la entidad (interna y externa)	Red sin protección, sin las herramientas o equipos tecnologicos de comunicacion que aseguren al usuarios su correcto funcioanmiento Fuga de información debido al acceso de usuarios no autorizados a la infraestructura de red de la entidad. Indisponibilidad del servicio de la red inalámbrica debido a ataques de denegación de servicios (DoS). Suplantación de identidad para acceder a los aplicativos tecnológicos de la entidad que se encuentran disponibles a través de la red de datos. Funcionarios descontentos pueden hacer uso de usuarios y contraseñas de personal que ya no labora en la entidad para visualizar y/o sustraer información confidencial de la entidad.	Seguridad de la Información	Ausencia de controles que protejan la información transferida y las instalaciones de procesamiento de información de soporte No hay un proceso establecido para la administración y gestión de usuarios al interior de la entidad. Ausencia de procesos que establezcan los procedimientos para habilitar o deshabilitar las cuentas de usuario. No existe un registro actualizado de los usuarios que tienen acceso a los aplicativos y servicios ni se identifica su estado (Activo, Bloqueado, Deshabilitado). Deficiencias en las configuraciones de seguridad de la red, incluida la inalámbrica, empleando un cifrado débil. Ausencia de un administrador de red que configure, administre y gestione la red bajo criterios de seguridad de la información. No se aplican políticas de seguridad de la información.	Perdida de disponibilidad, integridad y confidencialidad de la información de la entidad, generando un impacto negativo en la continuidad del negocio Indisponibilidad de los servicios que se brindan a través de la red ocasionando tiempos no productivos para los funcionarios Desprestigio de la imagen corporativa de la entidad, debido a la divulgación no autorizada de información confidencial por parte del personal interno y/o externo de la entidad.	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	IMPROBABLE	MODERADO	MODERADO
13	INFORMACIÓN TALENTO HUMANO	Pérdida de Confidencialidad	Acceso no autorizado a información enviada mediante mensajería electrónica	Fuga y/o pérdida de información Divulgación no autorizada de información debido a acceso de terceros Secuestro de información generado por una aplicación ramsomware.	Seguridad de la Información	Controles de acceso al correo electrónico inadecuados, uso de contraseñas débiles, uso de cifrados débiles	Perdida de confidencialidad e integridad de la información	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	RARA VEZ	MODERADO	MODERADO
14	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Confidencialidad	Interceptación de información en tránsito provocada por una pérdida de la confidencialidad	Usuarios mal intencionados, Atacantes, Códigos maliciosos	Seguridad de la Información	Ausencia de controles adecuados para la transferencia de información Cifrados débiles Ausencia de herramientas que permitan asegurar el transporte de la información	Perdida de confidencialidad e integridad de la información	GESTIÓN DE TIC	RARA VEZ	MAYOR	ALTO
15	INFORMACIÓN	Pérdida de Confidencialidad Pérdida de Disponibilidad	Alteración, suplantación, divulgación y/o uso mal intencionado de la información sensible para la Entidad.	Funcionarios y/o Contratistas inconformes Atacantes externos,	Seguridad de la Información	Accesos lógicos sin retirar, novedades de funcionarios y/o contratistas sin reportar, ausencia de acuerdos de confidencialidad Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos) y/o ataque informático interno por parte de un funcionario o contratista con acceso, a la plataforma tecnológica Incumplimiento del procedimiento de clasificacion y etiquetado documental Ausencia de implementacion de procesos, procedimiento y políticas que permitan preservar y mantener los pilares referentes a Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad)	Incumplimiento de la política de seguridad de la información en el acuerdo de confidencialidad de la información	GESTIÓN DE TIC	RARA VEZ	MODERADO	MODERADO
16	INFORMACIÓN TALENTO HUMANO	Pérdida de Disponibilidad	Incumplimiento de la legislación y procedimientos vigentes	Funcionarios con desconocimiento en temas de contratación de personal Cambios en las regulaciones y lineamientos del gobierno que puedan impactar las operaciones de la Corporación Insuficiente protección y privacidad de información personal	Seguridad de la Información	Desconocimiento de la legislación Colombiana y de los procedimientos internos de la Entidad Incomprensión de las nuevas leyes y reglamentos y la identificación de la legislación aplicable Procedimientos inadecuados de contratación de personal. Procedimiento insuficiente para el cumplimiento de los requisitos de propiedad intelectual	Incumplimiento legal de obligaciones con causales disciplinarias, fiscales o penales	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	RARA VEZ	MODERADO	MODERADO
17	INFORMACIÓN	Pérdida de la confidencialidad, integridad	Pérdida de la confidencialidad, integridad y disponibilidad de la información cifrada	Robo o hurto de informacion catalogada como sensible por falta de implementacion de herramientas que aseguren el tranporte de la informacion por la red Acceso a información privada, reservada o sensible sin la debida autorización.	Seguridad de la Información	Uso de controles criptográficos débiles, protección inadecuada a llaves criptográficas, ausencia de políticas para asegurar el uso apropiado de controles criptográficos Protocolos de certificacion para paginas seguras sin licencia o vencidos Desconocimiento de Políticas sobre teletrabajo y trabajo remoto Falta de Monitoreo de tráfico de red a través de la VPN. Falta de parches de seguridad del sistema operativo del equipo conectado. Falta de actualización de firmas del software antivirus	Perdida, robo o mala utilización de la información.	GESTIÓN DE TIC	PROBABLE	MAYOR	ALTO

18	INFORMACIÓN	Pérdida de Disponibilidad,, integridad	Pérdida de la continuidad de la seguridad de la información en situaciones de contingencia	Funcionarios con roles de seguridad de la información sin conocimiento Interrupción completa en la continuidad del negocio (Daño en Data Center, ServiciosTecnológicos y pérdida de la Información) Los usuarios realizan trabajo en casa, manipulan informacion, acceden a los sistemas de informacion desde las conexiones establecidas en el hogar Practicas inapropiada que afecten la disponibilidad de la informacion y la plataforma tecnologica	Seguridad de la Información	Exclusión de la seguridad de la información en la planificación de la continuidad del negocio Obsolescencia Tecnológica Plan de contingencia y guias desactualizadas Eventos catastróficos: inundaciones, incendios, terremotos, ataques terroristas, disturbios civiles, pandemia La entidad no tiene el control sobre las medidas de protección utilizadas por el usuario para salvaguardar los datos y evitar perdida de intregidad y confidencialidad de la infomacion a la que accede desde trabajo en casa.	Perdida de la continuidad del negocio, servicios afectados para los usuarios internos y externos. Afectación a toda la Entidad Interrupción completa de los servicios ofrecidos en la entidad Pérdida de la imágen corporativa frente a las partes interesadas	GESTIÓN DE TIC	IMPROBABLE	CATASTROFICO	EXTREMO
19	HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Disponibilidad	Indisponibilidad de los recursos tecnológicos ocasionada por una inadecuada gestión a la capacidad (procesamiento, almacenamiento, memoria)	Ausencia de revisiones periodicas por parte de los administradores de los recursos de la infraestructura tecnológica	Seguridad de la Información	Falta de identificación de rangos críticos Saturación de capacidad de almacenamiento. Falta de reporte de alarmas en los arreglos de discos	Interrupción de los servicios tecnológicos ofrecidos por la Corporación Perdida de informacion crítica	GESTIÓN DE TIC	POSIBLE	MAYOR	EXTREMO
20	INFORMACIÓN	Pérdida de la confidencialidad, integridad	Perdida de confidencialidad, integridad de la información en la ejecución de proyectos relacionados con la adquision de bienes o servicios por parte del GIT Apoyo informático	Filtración y manipulación de la información para beneficio de un tercero	Seguridad de la Información	No se realiza una valoración de los riesgos de seguridad de la información en una etapa temprana del proyecto con el fin de identificar los controles necesarios . Falta de integración de la seguridad de la información en la gestión de proyectos. Inadecauda gestion de estudio de mercado, viabilidad o especificacion tecnica del producto o servicio que permita dar cumplimiento del requerimiento	Afectación en la seguridad aplicada al proyecto, directamente relacionado con costo, tiempo y alcance	GESTIÓN DE TIC	RARA VEZ	MAYOR	ALTO
21	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Pérdida de la confidencialidad, integridad	Perdida de confidencialidad, integridad y disponibilidad durante el ciclo de desarrollo en los sistemas de información ya sean nuevos o existentes - Acceso no autorizado a los códigos fuente y ambientes de desarrollo	Proveedores de sistemas de información, funcionarios con roles de desarrollo que no cumplen las politicas y requerimientos en seguridad Manipulación intencionada interna o externa de las fuentes de información ocasionando pérdida parcial y/o total del código fuente Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. Indisponibilidad de acceso a los repositorios de información o herramienta donde se resguarda el codigo fuente Secuestro de la información relacionada con el código fuente efectuado por un tercero a través de un malware Ataques cibernéticos sobre las plataformas desarrolladas internamente	Seguridad de la Información	Falta de políticas que exijan la inclusión de requisitos de seguridad de la información para la adquisición, desarrollo y mantenimiento de sistemas Ausencia de una metodología de desarrollo de software seguro. No se realiza la gestion documental y/o actualizacion de control de version para el desarrollo de nuevas funcionalidades del software permaneciendo de manera local en el equipo del desarrollador y no en el repositorio documental No se encuentra documentado los lineamientos de seguridad implementados en el desarrollo de software No hay definido un plan detallado de pruebas de seguridad a efectuar en las etapas del desarrollo de software. No se realizan pruebas de seguridad sobre el software que permitan detectar vulnerabilidades de seguridad. El aplicativo no encripta la información para su transmisión a través de la red. Ausencia de controles en el acceso al código fuente	Afectación en la confidencialidad, integridad y disponibilidad de los sistemas de información Eliminación de codigo fuente afectando la disponibilidad y ejecucion del desarrollo de software Divulgación de información no autorizada por terceros por asignación excesiva de permisos sobre un rol. Manipulación de información no autorizada por terceros, que favorezcan a las partes interesadas, afectando la imagen corporativa de la entidad.	GESTIÓN DE TIC	RARA VEZ	MAYOR	ALTO
22	TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Pérdida de Integridad	Cambios en los sistemas de información gestionados inadecuadamente	Usuarios y administradores sin conocimiento de las políticas y procedimientos de seguridad de la información	Seguridad de la Información	Ausencia de procedimientos formales para el control de cambios. Ausencia de políticas para el control de cambios en los sistemas. Ausencia de transferencia de conocimiento y falta de capacitación tecnica	Incumplimiento de los procedimientos de control de cambios en los sistemas de información	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	PROBABLE	MENOR	ALTO
	OPORTUNIDADES										
1	TALENTO HUMANO INFORMACIÓN		Asesoría y documentación brindada por Entidades del Estado en temas de seguridad de la información, por ejemplo guías que provee MinTIC, DAFP, Archivo General de la Nación	No Aplica	Seguridad de la Información	No Aplica	No Aplica	GESTIÓN DE TIC GESTIÓN DEL TALENTO HUMANO	No Aplica	No Aplica	No Aplica

MAPA Y PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024-2027 - CORANTIOQUIA

Nro.	RIESGO	ACTIVOS	TIPO	AMENAZA	CAUSA / VULNERABILIDAD	RIESGO RESIDUAL CALIFICACIÓN			OPCION DE TRATAMIENTO	ACCIONES	ACTIVIDAD DE CONTROL	SOPORTE	INDICADOR
						PROBABILIDAD	IMPACTO	EVALUACIÓN					
1	Pérdida de Confidencialidad	TALENTO HUMANO	Seguridad de la Información	Usuarios mal intencionados o por desconocimiento de la seguridad de la información ocasionan pérdida parcial o total de la información.	Desconocimiento de los lineamientos sobre la seguridad de la información institucionales Desactualización de la Politica y Manual de seguridad de la información Uso y apropiación insuficiente de las políticas, manual y procedimientos de seguridad de la información Falta de competencias del personal a cargo del cumplimiento de las responsabilidades de la seguridad de la información asignadas Falta o insuficiente descripción de los roles y responsabilidades sobre seguridad de la información en los documentos de contratación	CASI SEGURO	MODERADO	EXTREMO	Reducir el riesgo	Revisiones periódicas y actualización de la política general y el manual de políticas de seguridad de la información cuando aplique.	Políticas para la seguridad de la información Revisión de la política	Política general de seguridad de la información aprobada por la alta dirección	Evidencia de seguimiento
										Dar cumplimiento con el diligenciamiento del acuerdos de confidencialidad para todos los funcionarios públicos de la Entidad		Cláusula de confidencialidad en los contratos de prestación de servicios Acuerdos de confidencialidad firmados	Evidencia de seguimiento
										Validar el cumplimiento de la política general y el manual de las políticas específicas de seguridad de la información.		Manual de políticas específicas de seguridad de la información aprobado por el Comité Directivo.	Cumplimiento de políticas y manual de seguridad de la información **# Políticas satisfactorias / # Políticas medibles**
										Definir y diligenciar el plan anual de capacitación, educación (formal y no formal). Formación en seguridad de la información (formal y no formal).	Toma de conciencia, educación y formación en la seguridad de la información	Plan anual de capacitación de la entidad Invitaciones y asistencia a foros, talleres y charlas relacionadas con seguridad de la información	Evidencia de seguimiento
										Socializar la política general y manual de seguridad de la información aprobada por la alta dirección, por medio de: Correo electrónico, Intranet, Pagina Web, Sensibilizaciones. (Dejar evidencia documentada)		Plan de medios de comunicación de seguridad de la información (Información, tips, recomendación y temas generales en seguridad)	
2	Pérdida de Confidencialidad	TALENTO HUMANO INFORMACIÓN	Seguridad de la Información	Acciones indebidas de los funcionarios o contratistas con privilegios de acceso (Usuarios mal intencionados o con desconocimiento de los procesos, procedimientos y/o políticas de la Entidad)	Ausencia de implementación de procedimientos en la gestión de usuarios que incluya registro de usuarios, cancelación de usuarios, asignación y anulación de derechos de acceso. Ausencia de gestión sobre las vulnerabilidades técnicas	RARA VEZ	MENOR	BAJO	Reducir el riesgo	Hacer seguimiento a la implementación de las políticas de control de acceso lógico	Gestión de derechos de acceso privilegiado	Perfiles y privilegios de administración asignados para ciertos administradores de las plataformas	Evidencia de seguimiento
										Hacer seguimiento de las políticas de suministro de acceso formal de usuarios para asignar o revocar derechos de acceso			
										Revisión periódica de la política de los derechos de acceso	Política de control de acceso	Política para el control de acceso definida	
										Revisión y seguimiento a la solución de las vulnerabilidades de cada componente.		Archivo de seguimiento a la remediación de las vulnerabilidades	
3	Pérdida de Disponibilidad	INFORMACIÓN	Seguridad de la Información	Fuga de información Divulgación de procedimientos o información catalogada como reservada o clasificada Configuración por default de componentes tecnologicos	Falta de implementación de procedimientos o políticas adecuadas en seguridad de la información en las actividades, servicios o procesos aplicadas a los proveedores y/o contratistas en la labor contratada	RARA VEZ	MODERADO	MODERADO	Reducir el riesgo	Seguimiento y control a los proveedores en la aplicación de los requisitos de seguridad en los sistemas de información, dando cumplimiento a la norma. Realizar seguimiento a las conexiones de los proveedores de acuerdo al objeto contractual (Validación de servidores, recursos, VPNs, etc)	Política de seguridad de la información para las relaciones con proveedores	Se establecerá que el proveedor debe cumplir con las políticas de seguridad de la información de la entidad.	Evidencia de seguimiento
											Tratamiento de la seguridad dentro de los acuerdos con proveedores	Clausula de confidencialidad en los contratos suscritos con proveedores y contratistas Acuerdo de confidencialidad para proveedores	
										Seguimiento y control de las licencias adquiridas por la entidad y las que se encuentren en uso en los equipos. Controlar y asegurar que no se exceda el numero de licencias asignadas a usuarios. Adquirir software de fuentes conocidas y confiables para asegurar que no se violen los derechos de autor.	Derechos de propiedad intelectual	Clausula de derechos de propiedad intelectual en los contratos suscritos con proveedores y contratistas.	Evidencia de seguimiento
4	Pérdida de Disponibilidad	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información	Incendio, inundación, terremoto, polvo Funcionarios con acceso a Datacenter, inconformes y/o sin conocimientos en seguridad de la información Códigos maliciosos Proveedores tecnológicos Ciberdelincuentes Ataques terroristas Disturbios civiles Interrupción de los servicios de la entidad y página web Indisponibilidad de la plataforma tecnológica	Ausencia de planes de emergencia y pruebas al mismo. Ausencia de redes contra incendio, condiciones inadecuadas de temperatura y humedad que generan daños sobre la infraestructura fisica Acciones fortuitas o malintencionados en el centro de computo, ocasionando pérdida parcial o total de la información alojada en los equipos. Conexión de equipos a corriente no regulada Debilidad en la infraestructura tecnológica, ausencia de un sistema de control de acceso. Falta de mantenimiento a equipos de usuarios y a la plataforma tecnológica Hardware y software obsoletos y sin garantía Encargado del componente no se encuentra disponible y no existe un rol de respaldo de éste. Gestión inadecuada de la capacidad de los equipos, falla en las UPS o aires acondicionados. Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos) Ausencia de redundancias para los servicios críticos No se registra un monitoreo constante de los eventos y registro de logs que permitan detectar posibles intrusiones y/o debilidades de seguridad. El antivirus instalado en los servidores no se encuentra activo o desactualizado	RARA VEZ	MODERADO	MODERADO	Reducir el riesgo	Actualizar plan de continuidad del negocio	Protección contra amenazas externas y ambientales	Sistema de detección y prevención de incendios. Plan de continuidad del negocio para montar servicios en centro de datos alterno.	Evidencia de seguimiento
										Verificar el cumplimiento del control de acceso al centro de datos	Ubicación y protección de los equipos	Bitácora de acceso al Datacenter	
										Establecer plan de mantenimientos preventivos a los equipos de la infraestructura tecnológica para el periodo		Mantenimientos a aire acondicionado, switches, cuchillas, servidores, etc.	
										Realizar inspecciones periódicas de los equipos tecnológicos y de respaldo (servidores, UPS, planta eléctrica) para verificar su funcionamiento y ejecutar las correcciones necesarias	Servicios de suministro	Sistema de Alimentación Ininterrumpida (UPS) con autonomía de 16 minutos. Planta Eléctrica con autonomía de 10 horas	Evidencia de seguimiento
										Validar y poner a prueba sistemas de redundancia suficiente para los servicios y arquitectura crítica usados para el procesamiento de información	Implementación de la continuidad de la seguridad de la información Disponibilidad de instalaciones de procesamiento de información.	Pruebas realizadas a los planes de contingencia de los servicios críticos	
5	Perdida de Integridad	HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información	Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generado por virus informáticos. Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso	Ausencia de políticas y controles restrictivos para la instalación de software no autorizado Uso e instalación de software con vulnerabilidades Perfiles y privilegios no asignados Descarga de virus informáticos maliciosos (Spiware, troyanos, virus, gusanos)	RARA VEZ	MODERADO	MODERADO	Reducir el riesgo	Verificar el cumplimiento de las políticas de teletrabajo y trabajo remoto establecidos por la Corporación	Teletrabajo Gestión de derechos de acceso privilegiado Restricciones sobre la instalación de software	Cumplimiento de la política general de seguridad de la información aprobada por la alta dirección y el Manual de Políticas de Seguridad de la Información.	Monitoreo de logs Evidencia de seguimiento
										Verificar el cumplimiento de las políticas para la gestión de vulnerabilidades técnicas y para la restricción de instalación de software en sistemas operativos		Formato -Administración de cambios a TI	Detección de vulnerabilidades # Test ejecutados / # Total test programados
										Verificar la aplicación del procedimiento para la restricción de la instalación de software en sistemas operativos		Perfiles y privilegios de administración asignados para ciertos usuarios	Evidencia de seguimiento
6	Perdida de Integridad	INFORMACIÓN HARDWARE SOFTWARE Y	Seguridad de la Información	Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la información generado por virus informáticos.	Base de datos de antivirus desactualizada. Usuarios con privilegios de uso de medios removibles	IMPROBABLE	MENOR	BAJO	Reducir el riesgo	Verificar la pertinencia y aplicación de las reglas para el manejo de la gestión de los medios removibles.	Controles contra códigos maliciosos	Se monitorea con la consola de antivirus Sophos.	Evidencia de seguimiento
										Cumplimiento de las políticas para la protección contra código		Al conectar dispositivos USB el antivirus automáticamente realiza un escaneo el cual no se puede cancelar por parte del usuario.	Evidencia de seguimiento

		SERVICIOS		Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso	Equipos informaticos sin licencia o con software desactualizados				malicioso en servidores y equipos de cómputo.		Se controlan desde la consola las actualizaciones de las bases de datos de virus.	Evidencia de seguimiento
7	Pérdida de Disponibilidad	INFORMACIÓN TALENTO HUMANO	Seguridad de la Información	Funcionarios/contratistas, Proveedores externos, Ciberataques, servicios de suministro, amenazas naturales	Manipulación, transporte y almacenamiento inadecuado a las cintas de Backup. Ausencia de pruebas regulares a las copias de respaldo. Incumplimiento al acuerdo de confidencialidad Manipulación inadecuada de la documentación recepcionada por el personal de la Entidad. Falta de valores y compromiso con la Entidad Intereses a favor de terceros Incumplimiento de los Roles y Responsabilidades para la seguridad de la Información.	IMPROBABLE	MAYOR	ALTO	Reducir el riesgo	Realizar pruebas de restauración de las copias de respaldo de la información, software e imágenes de los sistemas para este periodo. Verificar el almacenamiento adecuado de las copias de respaldo. Monitores y seguimiento de la ejecución de las copias de respaldo con el fin de asegurar el correcto procedimiento (Completitud de los datos y registros) durante la gestión.	Respaldo de información	Restauración de copias de respaldo de información	Evidencia de seguimiento
										Validar los requisitos de seguridad en la custodia de cintas al proveedor (Transporte, instalaciones, manipulación, etc.).	Cadena de suministro de tecnología de información y comunicación	Protocolos y procedimientos de seguridad de la información del proveedor	
8	Pérdida de Disponibilidad	INFORMACIÓN TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información	Afectación en la disponibilidad del respaldo de la información Insuficiencia de espacio o almacenamiento para el aseguramiento de la información Pérdida o corrupción de los datos Corrupción de las cintas en el momento de las copias y las restauración del Backup Inexistencia de Backup de la información misional	Ausencia de medidas para evitar la pérdida de datos, por ejemplo copias de respaldo. Falta de pruebas regulares a las copias de respaldo. Ausencia de manuales para la administración de las herramientas de aplicaciones. Administrador de servidores sin conocimiento de las políticas de seguridad de la información. El respaldo de Backup está ubicado en los mismos servidores a los cuáles se les realiza las copias de respaldo	RARA VEZ	MENOR	BAJO	Reducir el riesgo	Dar cumplimiento con la política y procedimientos para la realización de backups a software, imágenes de los sistemas operativos, e información crítica Verificación de las copias de respaldo por medio de pruebas de restauración	Respaldo de información	Evidencia de respaldo y restauración Diligenciamiento del formato -Seguimiento y control de seguridad de la información	Cumplimiento de la política de copias de respaldo a servidores **# Reportes ejecutados / # Reportes programados**
9	Pérdida de Integridad	TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información	Indisponibilidad de los servicios y/o página web Administradores de tecnología sin conocimientos técnicos de seguridad de la información. Fuga y/o pérdida de información generada por código malicioso. Divulgación no autorizada de información debido a acceso de terceros a través del uso de malware. Indisponibilidad de la plataforma tecnológica Secuestro de información generado por una aplicación ramsomware. Daño de hardware ocasionado por código malicioso	Vulnerabilidades técnicas sin conocer, uso de software desactualizado Intrusión de personal no autorizado a la plataforma tecnológica Acceso sin autorización locales, remotos y a los centros de cableado o de la UPS Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos) Falta de políticas, controles de seguridad, no existen procedimientos establecidos para la restricción de acceso a la infraestructura física de la organización Falta de socialización acerca de las diferentes modalidades de ciberataques	RARA VEZ	MODERADO	MODERADO	Reducir el riesgo	Establecer contacto con grupos de interés, especializados en seguridad de la información	Contacto con grupos de interés especial	Cierre de puertos. Monitoreo de Logs	Evidencia de seguimiento
										Desarrollar pruebas de vulnerabilidades periódicas	Gestión de las vulnerabilidades técnicas	Pruebas de vulnerabilidad periódicas	Detección de vulnerabilidades **# Test ejecutados / # Total test programados**
										Instalación de nuevas versiones de software		Actualización de software para mitigar riesgos de seguridad.	
10	Pérdida de Disponibilidad	HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información	Falla en el suministro de energía, servicios ofrecidos por el proveedor	Ausencia de canal de respaldo, acuerdos de nivel de servicio con el proveedor sin establecer. Falta de respaldo de los servicios de suministro (aire, energía, entre otros).	POSIBLE	MODERADO	ALTO	Reducir el riesgo	Establecer redundancia en los servicios críticos de la Entidad	Seguridad de los servicios de red	Software de monitoreo.	Evidencia de seguimiento
										Solicitar al proveedor principal activación de una comunidad SNMP para monitoreo interno.	Disponibilidad de instalaciones de procesamiento de información	Eventos y alarmas de los componentes de infraestructura tecnológica	
										Seguimiento a los acuerdos de nivel de servicio con los Proveedores de los servicios críticos.		Línea de soporte del proveedor de internet para reporte de indisponibilidad del servicio.	
11	Pérdida de Confidencialidad	INFORMACIÓN TALENTO HUMANO	Seguridad de la Información	Usuarios sin conocimiento de las políticas, manual y procedimientos de seguridad de la información	Ausencia de políticas para la gestión y uso de contraseñas Falta de sensibilización y capacitación en el manejo y uso de contraseñas Personal inconforme al interior de la Entidad o poco compromiso ante las políticas de Seguridad de la Información. Robo o usurpación de contraseñas	IMPROBABLE	MODERADO	MODERADO	Reducir el riesgo	Dar cumplimiento a las políticas de seguridad de la información relacionadas con el uso adecuado de contraseñas por parte de los usuarios.	Sistema de gestión de contraseñas	Políticas de control de contraseñas en el servidor de dominio.	Evidencia de seguimiento
										Validar el cumplimiento de las políticas de asignación de contraseñas temporales seguras cuando se crean usuarios		Configuración en el servidor de dominio para cambio de contraseñas	
										Verificar el cumplimiento de la política de cambio de contraseña de cuentas de administración genéricas cada vez que expire el tiempo de acceso concedido a un funcionario, exfuncionario, contratista y/o proveedor.		Se realizan sensibilizaciones por medio de los Tips de seguridad de la información a través de Corantioquia al día.	
										Validar el funcionamiento de la herramienta para gestión de contraseñas			
										Incluir en el plan de sensibilización y capacitación temas asociados al uso adecuado de contraseñas para este periodo.			
12	Pérdida de Confidencialidad	TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información	Red sin protección, sin las herramientas o equipos tecnológicos de comunicación que aseguren al usuarios su correcto funcionamiento Fuga de información debido al acceso de usuarios no autorizados a la infraestructura de red de la entidad. Indisponibilidad del servicio de la red inalámbrica debido a ataques de denegación de servicios (DoS). Suplantación de identidad para acceder a los aplicativos tecnológicos de la entidad que se encuentran disponibles a través de la red de datos. Funcionarios descontentos pueden hacer uso de usuarios y contraseñas de personal que ya no labora en la entidad para visualizar y/o sustraer información confidencial de la entidad.	Ausencia de controles que protejan la información transferida y las instalaciones de procesamiento de información de soporte No hay un proceso establecido para la administración y gestión de usuarios al interior de la entidad. Ausencia de procesos que establezcan los procedimientos para habilitar o deshabilitar las cuentas de usuario. No existe un registro actualizado de los usuarios que tienen acceso a los aplicativos y servicios ni se identifica su estado (Activo, Bloqueado, Deshabilitado). Deficiencias en las configuraciones de seguridad de la red, incluida la inalámbrica, empleando un cifrado débil. Ausencia de un administrador de red que configure, administre y gestione la red bajo criterios de seguridad de la información.	RARA VEZ	MENOR	BAJO	Reducir el riesgo	Verificar que a nivel de Switch se deshabilitan los puertos que no están en uso	Controles de redes Seguridad de los servicios de red Separación en las redes	A nivel de Switch se deshabilitan los puertos que no están en uso	Evidencia de seguimiento
										Verificar el funcionamiento de la autenticación en redes Wi-Fi mediante los protocolos seguros (WPA2)		Autenticación a la Wifi a través del directorio activo para la red inalámbrica corporativa	Evidencia de Seguimiento
										Verificar el uso de protocolos de comunicación seguros (HTTPS)		En la red de invitados se cuenta con seguridad (WPA2)	Evidencia de Seguimiento
										Hacer seguimiento a la implementación de servicios y/o equipos que brinden seguridad perimetral			Evidencia de Seguimiento
										Verificar la separación de la red de la entidad mediante VLANS			
13	Pérdida de Confidencialidad	INFORMACIÓN TALENTO HUMANO	Seguridad de la Información	Fuga y/o pérdida de información Divulgación no autorizada de información debido a acceso de terceros Secuestro de información generado por una aplicación ramsomware.	Controles de acceso al correo electrónico inadecuados, uso de contraseñas débiles, uso de cifrados débiles	RARA VEZ	INSIGNIFICANTE	BAJO	Reducir el riesgo	Socialización a los usuarios en medios de comunicación sobre los riesgos a los cuales están expuestos por medio del correo electrónico para este periodo	Protección de transacciones de los servicios de las aplicaciones	Envío de mensajería electrónica mediante HTTPS Encriptación estándar (TLS)	Evidencia de Seguimiento
14	Pérdida de Confidencialidad	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información	Usuarios mal intencionados, Atacantes, Códigos maliciosos	Ausencia de controles adecuados para la transferencia de información Cifrados débiles Ausencia de herramientas que permitan asegurar el transporte de la información	RARA VEZ	MENOR	BAJO	Reducir el riesgo	Validar o realizar mantenimiento a los procedimientos y controles para la transferencia de información durante el transito de la misma, además de los niveles aceptables de control de acceso.	Política de desarrollo seguro	Uso de certificados digitales para servicios críticos	Evidencia de Seguimiento
										Establecer acuerdos para intercambio de información con entes de control	Procedimientos de control de cambios en sistemas	Uso de protocolos de comunicación SFTP Uso de VPN con certificados y autenticación Conexiones de la VPN bien asignadas reglas de conexión dentro del firewall	Evidencia de Seguimiento
15	Pérdida de Confidencialidad	INFORMACIÓN	Seguridad de la Información	Funcionarios y/o Contratistas inconformes Atacantes externos,	Accesos lógicos sin retirar, novedades de funcionarios y/o contratistas sin reportar, ausencia de acuerdos de confidencialidad Interrupción de los servicios prestados por terceros. (redes eléctricas, comunicaciones de voz y datos) y/o ataque informático interno por parte de un funcionario o contratista con acceso, a la plataforma tecnológica Incumplimiento del procedimiento de clasificación y etiquetado documental Ausencia de implementación de procesos, procedimiento y políticas que permitan preservar y mantener los pilares referentes a Seguridad de la Información (Confidencialidad, Integridad y Disponibilidad)	RARA VEZ	MENOR	BAJO	Reducir el riesgo	Verificar el control y seguimiento a la gestión de usuarios	Teletrabajo Terminación o cambio de responsabilidades de empleo	Diligenciamiento de cada uno de los formatos de gestión de acceso, de acuerdo a los diferentes sistemas de información de la Entidad.	Evidencia de seguimiento
										Verificar el cumplimiento de las políticas de teletrabajo y trabajo remoto establecidos por la Corporación		Cumplimiento de la política general de seguridad de la información aprobada por la alta dirección y el Manual de Políticas de Seguridad de la Información.	
										Dar cumplimiento con el diligenciamiento del acuerdos de confidencialidad para todos los funcionarios públicos de la Entidad		Acuerdo de confidencialidad firmado por todos los funcionarios públicos. Cláusula de confidencialidad en los contratos de prestación de servicios	
										Verificación del procedimiento en el proceso de cambio o terminación de empleo		Procedimiento de novedades	
16	Pérdida de Disponibilidad	INFORMACIÓN	Seguridad de la Información	Funcionarios con desconocimiento en temas de contratación de personal Cambios en las regulaciones y lineamientos del gobierno que puedan impactar las operaciones de la Corporación	Desconocimiento de la legislación Colombiana y de los procedimientos internos de la Entidad Incomprensión de las nuevas leyes y reglamentos y la identificación de la legislación aplicable Procedimientos inadecuados de contratación de personal.	RARA VEZ	MENOR	BAJO	Reducir el riesgo	Verificar la aplicación de protocolos de verificación sobre los antecedentes de los funcionarios que estén acorde a las funciones u obligaciones laborales	Selección Términos y condiciones del empleo Proceso disciplinario	Normograma y demás lineamientos que aplican	Evidencia de seguimiento
												Manual de contratación, Ley 80 y sus decretos	

		TALENTO HUMANO		Insuficiente protección y privacidad de información personal	Procedimiento insuficiente para el cumplimiento de los requisitos de propiedad intelectual					Validar procedimiento de vinculación y retiro laboral desde las áreas pertinentes (Gestión administrativa y Talento humano).	Terminación o cambio de responsabilidades de empleo	Procedimiento de vinculación y retiro laboral	Evidencia de seguimiento
17	Pérdida de la confidencialidad, integridad	INFORMACIÓN	Seguridad de la Información	Robo o hurto de información catalogada como sensible por falta de implementación de herramientas que aseguren el transporte de la información por la red Acceso a información privada, reservada o sensible sin la debida autorización.	Uso de controles criptográficos débiles, protección inadecuada a llaves criptográficas, ausencia de políticas para asegurar el uso apropiado de controles criptográficos Protocolos de certificación para paginas seguras sin licencia o vencidos Desconocimiento de Políticas sobre teletrabajo y trabajo remoto Falta de Monitoreo de tráfico de red a través de la VPN. Falta de parches de seguridad del sistema operativo del equipo conectado. Falta de actualización de firmas del software antivirus	POSIBLE	MODERADO	MODERADO	Reducir el riesgo	Hacer seguimiento a la Implementación de controles criptográficos y gestión de llaves criptográficas para este periodo Divulgación de Políticas sobre teletrabajo y trabajo remoto	Teletrabajo Política sobre el uso de controles criptográficos	Cumplimiento de la política general de seguridad de la información aprobada por la alta dirección y el Manual de Políticas de Seguridad de la Información. Monitoreo de Logs Implementación de sistema de autenticación de doble factor (tokens) y certificados SSL	Evidencia de seguimiento
18	Pérdida de Disponibilidad	INFORMACIÓN	Seguridad de la Información	Funcionarios con roles de seguridad de la información sin conocimiento Interrupción completa en la continuidad del negocio (Daño en Data Center, Servicios Tecnológicos y pérdida de la Información) Los usuarios realizan trabajo en casa, manipulan información, acceden a los sistemas de información desde las conexiones establecidas en el hogar Practicas inapropiada que afecten la disponibilidad de la información y la plataforma tecnológica	Exclusión de la seguridad de la información en la planificación de la continuidad del negocio Obsolescencia Tecnológica Plan de contingencia y guías desactualizadas Eventos catastróficos: inundaciones, incendios, terremotos, ataques terroristas, disturbios civiles pandemia La entidad no tiene el control sobre las medidas de protección utilizadas por el usuario para salvaguardar los datos y evitar perdida de integridad y confidencialidad de la información a la que accede desde trabajo en casa.	IMPROBABLE	MAYOR	ALTO	Reducir el riesgo	Realizar seguimiento periódico del plan de continuidad del negocio para asegurar e incorporar los aspectos derivados de la gestión de Seguridad de Información. Monitoreo de conexiones de red o Análisis de tráfico de red Firewall para protegerse ante amenazas y minimizar los riesgos que comprometan la información Conexiones seguras a través de la VPN	Planificación de la continuidad de la seguridad de la información Implementación de la continuidad de la seguridad de la información Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Backup de las aplicaciones y bases de datos de las aplicaciones misionales Plan de Contingencia de la Entidad Plan de continuidad del negocio Centro de datos ubicado en sitio alterno Reporte de amenazas Reporte de VPN Reporte de usuarios conectado	Evidencia de seguimiento Evidencia de seguimiento
19	Pérdida de Disponibilidad	HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información	Ausencia de revisiones periódicas por parte de los administradores de los recursos de la infraestructura tecnológica	Falta de identificación de rangos críticos Saturación de capacidad de almacenamiento. Falta de reporte de alarmas en los arreglos de discos	POSIBLE	MAYOR	ALTO	Reducir el riesgo	Seguimiento y monitoreo periódico de los componentes de la plataforma tecnológica	Gestión de capacidad	Implementación de scripts para el monitoreo a los recursos de los servidores y notificación por correo electrónico del estado al administrador	Evidencia de seguimiento
20	Pérdida de la confidencialidad, integridad	INFORMACIÓN	Seguridad de la Información	Filtración y manipulación de la información para beneficio de un tercero	No se realiza una valoración de los riesgos de seguridad de la información en una etapa temprana del proyecto con el fin de identificar los controles necesarios . Falta de integración de la seguridad de la información en la gestión de proyectos. Inadecuada gestión de estudio de mercado, viabilidad o especificación técnica del producto o servicio que permita dar cumplimiento del requerimiento	RARA VEZ	MODERADO	MODERADO	Reducir el riesgo	Validar la aplicabilidad de la metodología de proyectos y la inclusión de requisitos sobre la seguridad de la información. Aplicar la valoración de riesgos de seguridad de la información en una etapa temprana del proyecto para identificar los controles necesarios. Realizar seguimiento a los riesgos identificados y a los controles implementados para tratar los riesgos durante las fases del proyecto.	Seguridad de la información en la gestión de proyectos	En el formato de ESPECIFICACIONES TECNICAS se establece un ítem de requerimientos mínimos obligatorios de ESPECIFICACIONES DE SEGURIDAD INFORMÁTICA DE PRODUCTO Y/O SERVICIO	Evidencia de seguimiento
21	Pérdida de la confidencialidad, integridad	INFORMACIÓN HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información	Proveedores de sistemas de información, funcionarios con roles de desarrollo que no cumplen las políticas y requerimientos en seguridad Manipulación intencionada interna o externa de las fuentes de información ocasionando pérdida parcial y/o total del código fuente Hurto o pérdida de información causada por parte de un empleado descontento de la entidad. Indisponibilidad de acceso a los repositorios de información o herramienta donde se resguarda el código fuente	Falta de políticas que exijan la inclusión de requisitos de seguridad de la información para la adquisición, desarrollo y mantenimiento de sistemas Ausencia de una metodología de desarrollo de software seguro. No se realiza la gestión documental y/o actualización de control de versión para el desarrollo de nuevas funcionalidades del software permaneciendo de manera local en el equipo del desarrollador y no en el repositorio documental No se encuentra documentado los lineamientos de seguridad implementados en el desarrollo de software	RARA VEZ	MODERADO	MODERADO	Reducir el riesgo	Establecer e implementar políticas para la protección de ambientes de desarrollo. Verificar la aplicación de las metodologías en desarrollo seguro. Implementación de herramientas actualizadas a la última versión estable.	Seguridad en los procesos de desarrollo y de soporte Ambiente de desarrollo seguro	Formato Orden de cambio Formato -Documento de especificación	Evidencia de seguimiento
22	Pérdida de Integridad	TALENTO HUMANO HARDWARE SOFTWARE Y SERVICIOS	Seguridad de la Información	Usuarios y administradores sin conocimiento de las políticas y procedimientos de seguridad de la información	Ausencia de procedimientos formales para el control de cambios. Ausencia de políticas para el control de cambios en los sistemas. Ausencia de transferencia de conocimiento y falta de capacitación técnica	POSIBLE	INSIGNIFICANTE	BAJO	Reducir el riesgo	Verificar la pertinente o actualización de los procedimientos de gestión de cambios adoptados	Procedimientos de control de cambios en sistemas	Formato Administración de cambios a TI	Evidencia de seguimiento
					OPORTUNIDADES								
1	Asesoría y documentación brindada por Entidades del Estado en temas de seguridad de la información, por ejemplo guías que provee MinTIC, DAFP, Archivo General de la Nación	TALENTO HUMANO INFORMACIÓN	Seguridad de la Información	No Aplica	No Aplica	No Aplica	No Aplica		No Aplica	Revisión de documentación generada por el Min Tic y relacionada con seguridad de la información. Asesoría en seguridad de la información dada por personal de Min Tic. Implementación de guías generadas por el Min Tic-MSPI.	No Aplica		No Aplica