

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA
INFORMACIÓN 2022
AGENCIA NACIONAL DE HIDROCARBUROS - ANH
Versión 1.0

Bogotá D.C., enero de 2022

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información

CONTENIDO

	Pág.
1. ALCANCE	3
2. OBJETIVOS.....	4
2.1. Objetivo General.....	4
2.2. Objetivos Específicos.....	4
3. CONTEXTO ORGANIZACIONAL.....	4
4. MARCO NORMATIVO.....	6
5. SITUACIÓN ACTUAL.....	6
6. ACTIVIDADES Y RECURSOS.....	7
7. SEGUIMIENTO Y MEDICIÓN.....	10
8. BIBLIOGRAFÍA	10
9. REGISTROS.....	10
10. CONTROL DE CAMBIOS.....	10
11. DEFINICIONES.....	11

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información

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

INTRODUCCIÓN

El Plan de tratamiento de riesgos de seguridad y privacidad de la información de la ANH busca gestionar los riesgos de manera adecuada para salvaguardar la confidencialidad, integridad, disponibilidad y no repudio de la información de la Agencia Nacional de Hidrocarburos -ANH y así generar valor público en un entorno de confianza digital.

El plan comprende las directrices emanadas en Seguridad y Privacidad de la Información como habilitador transversal de la Política de Gobierno Digital¹, los lineamientos y estándares para la estrategia de seguridad digital, el Modelo de Seguridad y Privacidad de la Información – MSPI² y, el Modelo Nacional de Gestión de Riesgos de Seguridad Digital - MGRSG, establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, alineado con las buenas prácticas descritas en la norma ISO 27001:2013.

A nivel estratégico, el plan aporta al objetivo estratégico que busca “*Contar con una entidad innovadora, flexible y con capacidad de adaptarse al cambio*”; así mismo, su planteamiento se alinea con las políticas del gobierno nacional en materia de seguridad y privacidad de la información, seguridad digital y protección de datos personales, buscando gestionar “*las amenazas y vulnerabilidades a las que la entidad pueda estar expuesta desde la perspectiva del entorno cibernético, con el fin de fortalecer el ambiente de control, intensificar la confianza de las múltiples partes interesadas en el medio digital e impulsar la prosperidad económica, social de la Entidad y, por ende, del país*”³

El presente plan se formular para la vigencia 2022 y se desarrolla desde la Oficina de Tecnologías de la Información. Las actividades propuestas se ejecutarán conforme los recursos disponibles y se formulan para ser realizadas de manera virtual teniendo en cuenta la actual emergencia sanitaria⁴.

1. ALCANCE

El plan fijado para la vigencia 2022, comprende la fijación de actividades que permitan la gestión de los riesgos de seguridad de la información y seguridad digital conforme los lineamientos y directrices gubernamentales vigentes⁵, alineado con las buenas prácticas descritas en la norma ISO 27001:2013.

¹ 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”.

² Resolución 00500 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”

³ Tomado del Modelo de Gestión de Riesgos de Seguridad Digital Sector Público

⁴ Resolución 1913 de 2021 “Por la cual se proroga la emergencia sanitaria por el coronavirus COVID-19”

⁵ Guía para la administración del riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital, versión 4-2018 Función Pública, Modelo Nacional de Riesgos de Seguridad Digital MINTIC. Guía No.7 de gestión de riesgos versión 3-2016 MSPI MINTIC, principalmente

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información

2. OBJETIVOS

2.1. Objetivo General.

Promover las medidas que permitan mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital, preservando la confidencialidad, integridad, disponibilidad y no repudio de la información, para generar valor público, en un entorno de confianza digital.

2.2. Objetivos Específicos.

- ✓ Optimizar el nivel de madurez de ANH en materia de gestión de riesgos de seguridad de la información y seguridad digital a través de la ejecución de actividades alineadas al MSPI, al MGRSD, buenas prácticas y demás lineamientos asociados.
- ✓ Promover la implementación y seguimiento de controles para disminuir la probabilidad y/o el impacto de ocurrencia de los riesgos de seguridad de la información y de seguridad digital identificados
- ✓ Proponer la inclusión de la gestión de riesgos de seguridad de la información y de seguridad digital en la metodología de gestión de riesgos de ANH

3. CONTEXTO ORGANIZACIONAL

LA ANH es una Agencia Estatal del Sector descentralizado adscrita al Ministerio de Minas y Energía, en la Rama Ejecutiva Nacional, que tiene como objeto administrar integralmente las reservas y recursos hidrocarbuníferos de propiedad de la Nación, promover el aprovechamiento óptimo y sostenible de los recursos hidrocarbuníferos y contribuir a la seguridad energética nacional⁶, lo cual se traslada a su misión institucional incluyendo la armonía con los intereses de la sociedad, el Estado y las empresas del sector. De igual forma, para 2025 ANH busca ser reconocida como una entidad modelo en el mundo por el conocimiento del potencial del subsuelo colombiano y el logro de su aprovechamiento, la eficiencia y transparencia en la administración de hidrocarburos y el trabajo conjunto con la industria y la comunidad; por el profesionalismo de su equipo de trabajo, el alto nivel tecnológico y la eficiencia y agilidad en procesos clave.

ANH ha definido como objetivos estratégicos:

- Contribuir al desarrollo de la seguridad energética y en la generación de excedentes de exportación de hidrocarburos.
- Armonizar los intereses del Gobierno Nacional y Territorial, de los ciudadanos y las empresas del sector en el desarrollo de la industria de hidrocarburos.
- Contar con una entidad innovadora, flexible y con capacidad de adaptarse al cambio.
- Asegurar la funcionalidad del Sistema de Gestión Integrado y de Control, alcanzando la mejora continua de los procesos.

⁶ Tomado del Manual de Estructura del Estado, Sector Minas y Energía. Recuperado de <http://www.funcionpublica.gov.co/eva/gestornormativo/manual-estado/ejecutiva-orden-nacional.php> el 6 de julio de 2018

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información

Mediante el Decreto 714 de 2012 se establece la estructura de la ANH, así:

1. Consejo Directivo.
2. Presidente.
- 2.1 Oficina Asesora Jurídica.
- 2.2 Oficina de Control Interno.
- 2.3 Oficina de Tecnologías de la Información.
3. Vicepresidencia Administrativa y Financiera.
4. Vicepresidencia Técnica.
5. Vicepresidencia de Promoción y Asignación de Áreas.
6. Vicepresidencia de Contratos de Hidrocarburos.
7. Vicepresidencia de Operaciones, Regalías y Participaciones.
8. Órganos de Asesoría y Coordinación.
 - 8.1 Comité de Dirección.⁷
 - 8.2 Comité de Coordinación del Sistema de Control Interno.
 - 8.3 Comisión de Personal.

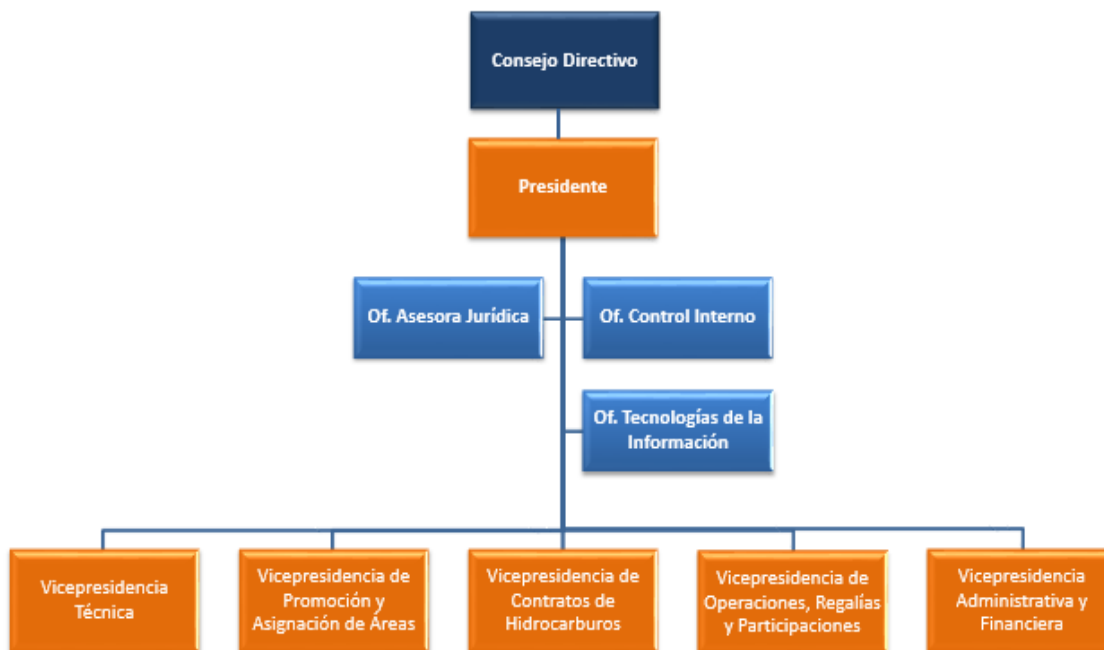


Imagen 1. Organigrama ANH

Para la organización de la seguridad de la información, la ANH ha venido trabajando en la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información – SGSI para establecer un marco de confianza en el ejercicio de sus deberes con el Estado, la sociedad

⁷ El Decreto 1499 de 2017 establece los Comités Institucionales de Gestión y Desempeño, el cual sustituye los demás comités que tengan relación con el Modelo Integrado de Planeación y Gestión-MIPG

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información

y las empresas del sector, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con su misión y visión.

Así las cosas, en aras de cumplir con este compromiso, las directrices, normas y buenas prácticas en la materia, la ANH adoptó el Sistema de Gestión de Seguridad de la Información - SGSI⁸, la Política General de Seguridad y Privacidad de la Información, el Manual de Políticas Específicas de Seguridad y Privacidad de la Información y, la Política de Protección de Datos Personales, entre otros instrumentos. De igual manera cuenta con una metodología general de gestión de riesgos aplicada a todos los procesos de ANH.

La Seguridad Digital y Gobierno Digital hacen parte de las políticas de la dimensión “*Gestión con valores para resultados*” de MIPG, ya que incide en el logro de los resultados propuestos y materialización de la planeación institucional.

4. MARCO NORMATIVO

Interno:

- ✓ Política General de Seguridad y Privacidad de la Información de ANH V3-2018.
- ✓ Manual de Políticas Específicas de Seguridad y Privacidad de la Información de ANH V1-2017
- ✓ Resolución 266 de 2018 – Adopción del Sistema de Gestión de Seguridad de la Información.
- ✓ Guía para la Administración del Riesgo y Oportunidades ANH.

Externo:

- ✓ Directrices y Guía PESI (no oficial) emitida por el Ministerio de las Tecnologías de la Información y las Comunicaciones – Mintic.
- ✓ Resolución 00500 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” - MINTIC
- ✓ Documento Maestro Modelo de Seguridad y Privacidad de la información V4-2021 y Guía 7 de Gestión de Riesgos V1 - MINTIC
- ✓ Modelo de Gestión de Riesgos de Seguridad Digital Sector Público y sus anexos MINTIC
- ✓ Guía para la administración del riesgo y el diseño de controles en entidades públicas, Riesgos de Gestión, Corrupción y Seguridad Digital, versión 4-2018 - Función Pública
- ✓ Decreto 612 de 2018 Integración Planes Institucionales - Función Pública
- ✓ Decreto 1008 de 2018 Política de Gobierno Digital – Gobierno Nacional
- ✓ Norma ISO 27001:2013
- ✓ Resolución 1581 de 2012 y Decreto Reglamentario 1377 de 2013 – Protección de Datos Personales.
- ✓ Buenas prácticas y normatividad vigente sobre la materia.

5. SITUACIÓN ACTUAL

Conforme la traza de diagnósticos del estado de la implementación del Modelo de Seguridad y Privacidad de la Información en la ANH, se han venido planteando las acciones para reducir la

⁸ Resolución ANH 266 de 2018

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información

brecha, estableciendo en el Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información aquellas acciones que por disponibilidad de tiempo y/o recursos no se lograron avanzar en vigencias anteriores, así como las propuestas para continuar la implementación acorde con la realidad de la Entidad, priorizando los dominios con más oportunidad de mejora.

Así las cosas, a pesar que en la vigencia 2021 continuaron presentes varios factores como la emergencia sanitaria, y la rotación de personas en varias dependencias, con el apoyo del funcionario de la OTI encargado de los temas asociados a activos de información y tratamiento de riesgos de seguridad de la información por procesos en la Entidad se presentaron avances en los dominios de la norma ISO 27001 entre 2020-2021 según Instrumento de Evaluación MSPI, destacando incrementos respecto al año anterior principalmente en *Aspectos de la seguridad de la información de la gestión de la continuidad del negocio (+27)*, *Criptografía (+20)*, *Gestión de Activos (+23)*, *Relaciones con los Proveedores y Políticas de Seguridad de la Información (+10)*, entre otros, pasando de un promedio de calificación de **77 a 86**.

En 2021 se enfocaron los esfuerzos en la identificación y clasificación de activos de información, así como se inició la identificación de Riesgos de Seguridad Digital por proceso, aportando en la mejor evaluación de los dominios con controles y aspectos relacionados a estos temas. Los temas mencionados son necesarios para consolidar una metodología de Gestión de Riesgos de Seguridad Digital, por ende algunas actividades planteadas en 2021 se trasladan a 2022 como continuación al trabajo que se viene realizando.

Como factores que inciden en la gestión, se consideran la aún vigente emergencia sanitaria y la rotación de personal clave en los procesos lo cual incide en la curva de aprendizaje y apropiación de los temas a trabajar; así las cosas, el presente plan se ajusta a esta nueva realidad y se enfocará en los aspectos más relevantes, alcanzables y realizables bajo estas condiciones, con la salvedad que para el éxito de las acciones propuestas se requiere la anuencia, concurso y colaboración de personal de otras áreas cuando sean convocados, que permita solventar tareas diarias, adicionales, emergentes y las propuestas en el presente plan.

6. ACTIVIDADES Y RECURSOS

Actualmente en ANH, cuenta con un (1) servidor público de planta con la dedicación y funciones asociadas a la seguridad de la información.

Respecto a Infraestructura tecnológica, ANH cuenta con esquema de seguridad perimetral administrada por un tercero, quien abarca lo relativo a seguridad informática y redes.

Teniendo en cuenta estos aspectos, se plantean las acciones que se consideran alcanzables para el sostenimiento y la mejora continua del SGSI enfocado en la gestión de riesgos de seguridad de la información y seguridad digital.

Formulación de actividades

Se establece el siguiente cronograma, detallando en el plan de trabajo las acciones propuestas para apuntar al logro de los objetivos para la presente vigencia con enfoque en los aspectos más relevantes.

(ver cronograma en la siguiente página)

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2022						
Objetivo estratégico asociado		<i>Contar con una entidad innovadora, flexible y con capacidad de adaptarse al cambio</i>				
Dimensión de MIPG Asociada		<i>Gestión con valores para resultados</i>				
Nombre del Plan	Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información 2022	Fecha inicio	03/01/2022			
Responsable	Oficina de Tecnologías de la Información	Fecha fin	20/12/2022			
Objetivo general	Promover las medidas que permitan mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital, preservando la confidencialidad, integridad, disponibilidad y no repudio de la información, para generar valor público, en un entorno de confianza digital.	Presupuesto total				
Actividad	Responsable	Producto o servicio	Recursos con los que se cuenta	Meta	Fecha de Inicio	Fecha de Fin
Asesorar en la identificación, evaluación y tratamiento de riesgos de seguridad de la información/digital de los procesos de la ANH	Líderes de Proceso/Facilitadores Gestión de TIC's	Asesorías realizadas	Facilitadores por proceso Material y reglamentación expedida por Función Pública y MINTIC	Asesorías al 100% de los procesos de ANH	03/01/2022	30/06/2022
Validar y/o ajustar declaración de aplicabilidad propuesta del CTO 634-2019 conforme controles aplicados en identificación de riesgos de seguridad de la información/digital de los procesos de la ANH	Líderes de Proceso/Facilitadores Gestión de TIC's	Propuesta para aprobación de la Declaración de aplicabilidad de ANH	Documento entregado por contratista CTO 634-2019 Información de Matriz de riesgos de seguridad de la información/digital por proceso	Declaración de aplicabilidad para aprobación	01/07/2022	30/09/2022

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información

Proponer integración riesgos de seguridad de la información en metodología de gestión de riesgos ANH (alineado a modelo de gestión de riesgos de seguridad digital)	Gestión de TIC's Planeación ANH	Propuesta para aprobación de metodología de gestión de riesgos ANH incluyendo de riesgos de seguridad de la información/digital	Metodología de Gestión de Riesgos ANH Material y reglamentación expedida por Función Pública	Propuesta para aprobación de Riesgos de Seguridad de la Información incluidos en metodología de gestión de riesgos ANH	15/02/2022	20/12/2022
Campañas de sensibilización y refuerzo en temas de gestión de riesgos digitales	Gestión de TIC's Comunicaciones	Campañas ejecutadas	Material CTO 634-2019 Material de referencia y buenas prácticas	Servidores y colaboradores sensibilizados	Permanente	Permanente

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información

7. SEGUIMIENTO Y MEDICIÓN

Se realizarán seguimiento semestral durante la vigencia para validar el cumplimiento en cada una de las actividades planteadas, con sus correspondientes productos y/o grado de avance, dejando las observaciones respectivas.

El presente Plan podrá ser actualizado o ajustado conforme cambios en las metas, la operación, nuevas directrices, normativas y/o lineamientos de Gobierno, condiciones emergentes o necesidades del servicio. En caso de imposibilidad del logro de las actividades total o parcialmente se dejará constancia en el seguimiento y ajuste realizado de las razones.

Para conocer el avance en a la ejecución del plan, se establece un indicador de gestión que mide la cantidad de acciones, procesos, procedimientos y operaciones realizadas durante el periodo a evaluar.

Nombre del Indicador	Descripción	Tipo	Unidad de Medida	Periodicidad	Responsable	Fecha de creación
Avance del plan	Grado de avance porcentual de ejecución del plan: Actividades ejecutadas en el periodo / Actividades a ejecutar en el periodo	Gestión	Porcentaje	Según periodo a evaluar (semestral)	Proceso de Gestión de TIC's	Enero de 2021

8. BIBLIOGRAFÍA

- ✓ Manual de Gobierno Digital
- ✓ Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información ANH 2021
- ✓ Autodiagnóstico MSPI 2021
- ✓ Matriz Gobierno Digital 2021

9. REGISTROS

Para el presente plan no se utilizarán registros oficiales, sin embargo, se dejará plasmado el seguimiento en un documento tipo Excel con las observaciones para cada actividad.

10. CONTROL DE CAMBIOS

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información

FECHA	MOTIVO DEL CAMBIO	VERSIÓN
Enero 7 de 2022	Creación del documento	1

11. DEFINICIONES

Confidencialidad: Propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados⁹.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada¹⁰.

Información: Se refiere a un conjunto organizado de datos que los sujetos obligados generen, obtengan, adquieran, transformen o controlen¹¹.

Integridad: Propiedad de la información relativa a su exactitud y completitud¹².

MSPI: Modelo de Seguridad y Privacidad de la Información. Ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información¹³

No repudio: Es la garantía de que no puedan ser negados los mensajes en una comunicación electrónica. Esto permite vincular al autor con la responsabilidad derivada de sus actuaciones y certificar que los datos o información provienen de la fuente que dice ser¹⁴.

Política: Documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información¹⁵.

SGSI - Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.¹⁶

Seguridad de la información: La protección de la información y los sistemas de información contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados para proporcionar confidencialidad, integridad y disponibilidad¹⁷.

⁹ Ibidem

¹⁰ ISO 27000:2018

¹¹ Ley 1712 de 2014

¹² ISO/IEC 27000

¹³ MINTIC

¹⁴ MINTIC, Guía 3 Cero papel

¹⁵ MINTIC, Modelo de Seguridad y Privacidad de la Información, Guía 2 Elaboración de la Política General de Seguridad y Privacidad de la Información

¹⁶ ISO/IEC 27000

¹⁷ Ibidem

Elaborado por:	Revisado por:	Aprobado por:
Sandra Mireya Ramírez	Planeación	Martha Lucía Torres Giraldo
Experto G3-5 Asesor	Planeación	Jefe Oficina de Tecnologías de la Información