



OBJETIVO						
Establecer los lineamientos para la optimización de los procesos y el incremento de la productividad de CISA, alineando la operación a la estrategia y a las iniciativas organizacionales, en articulación con los estándares del SIG, el MIPG y el MSPI.						
PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES		
<ul style="list-style-type: none"> • Todos los procesos • Partes interesadas 		<p>Mejora y optimización de procesos:</p> <ul style="list-style-type: none"> • P. Definir los lineamientos para promover la mejora de los procesos de CISA. • H. Identificar reprocesos, ineficiencias y desperdicios, así como oportunidades de mejora de los procesos, asociadas al cambio solicitado. • H. Realizar levantamiento de información. • H. Estructurar la mejora del proceso alineada a la estrategia de la organización. • H. Realizar Análisis de impacto. • H. Articular mejora con la operatividad de los demás procesos. • H. Realizar la actualización de la documentación de los procesos. • V.A. Proponer la acción correctiva o de mejora, si aplica. <p>Estudios de productividad</p> <ul style="list-style-type: none"> • P. Definir los lineamientos para atender las necesidades de estimaciones y estudios de productividad en la estructuración de soluciones. • P. Definir y establecer lineamientos para los estudios de productividad de los procesos de CISA y los análisis de carga o capacidad de estos. • H. Realizar levantamiento de información de los procesos y procedimientos • H. Identificar reprocesos, ineficiencias y desperdicios, así como oportunidades de mejora de los procesos, asociadas al cambio solicitado. • H. Realizar análisis de cargas de trabajo. • H. Realizar estudio de tiempos y movimientos. • H. Realizar simulaciones de los procesos o soluciones, cuando se requieran. • V. Analizar datos y determinar capacidad del proceso. 	<ul style="list-style-type: none"> • Publicación documento del SIG Actualizado. • Flujos de trabajo. • Socialización de los cambios. • Solicitud elaboración flujos de trabajo en ZEUS • Solicitud de parametrización aplicativo ZEUS • Requerimientos tecnológicos (Software y Hardware) • Requerimientos de personal • Manual de funciones y responsabilidades por cargo • Peligros y riesgos identificados 	<ul style="list-style-type: none"> • Todos los procesos • Jefatura de Operaciones Tecnológicas • Gestión del Talento Humano 		
<ul style="list-style-type: none"> • Soluciones para el Estado 		<ul style="list-style-type: none"> • Oportunidades de optimización de operación • Estructuración de Soluciones 			<ul style="list-style-type: none"> • Todos los procesos • Vicepresidencia de Soluciones para el Estado • Gerencia de Recursos • Administrativa y Suministros • PMO 	



PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES
<ul style="list-style-type: none"> • Procesos Críticos 	<p>Solicitudes de cambios y actualizaciones.</p>	<p>• V. Identificar y establecer recursos necesarios para los procesos o soluciones de nuevos negocios.</p> <p>V.A. Proponer acciones correctivas o de mejora asociadas</p> <p>Continuidad del Negocio</p> <ul style="list-style-type: none"> • P. Planificar las acciones a seguir para el fortalecimiento de las estrategias de continuidad del negocio. • H. Alinear desde los procesos, las solicitudes y cambios frente a continuidad del negocio. • H. A. Actualizar los planes de continuidad del negocio BCP. • H. Brindar acompañamiento a los líderes de los procesos críticos y de apoyo para la realización de actividades enfocadas en continuidad del negocio. • P. Planificar la realización simulacros y pruebas de recuperación de operaciones. • V. Realizar seguimiento a la implementación del BCP. <p>Planeación de la Seguridad de la Información:</p> <ul style="list-style-type: none"> • P: Definir la estrategia de seguridad de la información de la entidad con su alcance, objetivos, metas e indicadores. • P: Definir los planes, programas y proyectos para la implementación de la estrategia de seguridad de la información. • H: Comunicar el plan estratégico de seguridad de la información a todos los interesados. • H: Implementar los planes, programas y proyectos requeridos por la estrategia de seguridad de la información. • V.A: Medir y hacer seguimiento a los indicadores para verificar la consecución de los objetivos de la seguridad de la información de la entidad. • V.A. Identificar e Implementar acciones correctivas o de mejora para la implementación eficaz del plan estratégico de seguridad de la información. <p>Gestión de Activos de información:</p> <ul style="list-style-type: none"> • P: Definir políticas y procedimientos para la identificación, valoración y clasificación de activos de información y protección de datos personales de la entidad. • H: Identificar, valorar y clasificar los activos de información de los procesos de la entidad y asegurar su tratamiento adecuado. 	<ul style="list-style-type: none"> • Plan de continuidad del negocio. • Actualización de Planes de recuperación • Planes de simulacros y pruebas 	<ul style="list-style-type: none"> • Procesos críticos y de apoyo. • Equipo de manejo de crisis. • Líderes funcionales de continuidad del negocio. • Comité de Continuidad del Negocio
<ul style="list-style-type: none"> • Junta directiva y presidencia. • Comité institucional de Gestión y Desempeño. • Organismos del estado. 	<ul style="list-style-type: none"> • Plan estratégico de CISA. • Plan estratégico sectorial. • Políticas y lineamientos de CISA. • Políticas y lineamientos sectoriales. • Modelo integrado de planeación y gestión. • 	<ul style="list-style-type: none"> • Plan estratégico de seguridad de la información. • Informes de avance y desempeño del plan estratégico de seguridad de la información. • Reportes de seguimiento e implementación de ACPM. • 	<ul style="list-style-type: none"> • Presidente de CISA. • Comité institucional de gestión y desempeño. • Todos los procesos de CISA. • Organismos del estado. 	
<ul style="list-style-type: none"> • Todos los procesos de CISA. • Organismos del estado. 	<ul style="list-style-type: none"> • Inventario de activos • Tablas de retención documental. • Caracterización de procesos. • Modelos de gestión, de riesgos y de seguridad de la información del estado colombiano. • 	<ul style="list-style-type: none"> • Inventario de activos de información valorados y clasificados. • Inventario de base de datos que contienen datos personales. • Políticas y procedimientos para la gestión de activos de información. • Reportes de seguimiento e implementación de ACPM. • 	<ul style="list-style-type: none"> • Todos los procesos de CISA. • Organismos del estado. • Comité institucional de gestión y desempeño. • Auditoría Interna. 	



PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES
<ul style="list-style-type: none"> • Todos los procesos de CISA. • Organismos del estado. • Ciudadanos. • Auditoría Interna. • Proveedores 	<ul style="list-style-type: none"> • Eventos de seguridad de la información, seguridad informática o tecnología. • Informes de auditoría interna y externa. • Resultados de análisis de vulnerabilidades. • Resultados de pruebas de ingeniería social. • PQR's de la ciudadanía. 	<p>DESARROLLO DEL PROCESO</p> <ul style="list-style-type: none"> • H: Identificar las bases de datos que contengan datos personales de la entidad y asegurar su tratamiento adecuado. • H: Reportar el estado de la gestión de activos de información y del cumplimiento de la protección de datos personales a las partes interesadas. • V: Asegurar que los activos de información permanecen inventariados, valorados y actualizados. • V: Realizar el seguimiento al cumplimiento de las políticas y metodologías de gestión de activos de información. • V.A: Identificar e Implementar acciones preventivas, correctivas o de mejora para la gestión eficaz de los activos de información. <p>Gestión de Incidentes de seguridad de la información:</p> <ul style="list-style-type: none"> • P: Definir políticas y procedimientos para la gestión de incidentes de seguridad de la información. • H: Identificar, valorar, dar tratamiento y documentar los incidentes de seguridad de la información. • H: Liderar y coordinar las actividades de gestión de los incidentes con los diferentes procesos y partes externas involucradas. • H: Generar reportes de la gestión de incidentes a las partes interesadas. • V: Hacer seguimiento a los incidentes de seguridad de la información para determinar su adecuada contención, erradicación y recuperación. • V.A: Identificar lecciones aprendidas e Implementar acciones preventivas, correctivas o de mejora para la gestión eficaz de los incidentes de seguridad de la información. <p>Seguimiento y medición del desempeño de la seguridad de la información:</p> <ul style="list-style-type: none"> • P: Definir los mecanismos y procedimientos a través de los cuales se le hace medición y seguimiento a la gestión de la seguridad de la información. • H: Recopilar resultados del desempeño de la gestión de la seguridad de la información. • H: Realizar la revisión por la dirección. • V: Verificar el cumplimiento de la estrategia de seguridad de la información. • V.A: Seguimiento al cierre de hallazgos de revisiones y auditorías internas y externas de seguridad de la información. 	<ul style="list-style-type: none"> • Incidentes de seguridad de la información clasificados, valorados, tratados y documentados. • Informes ejecutivos y técnicos de la gestión de incidentes a las partes interesadas. • Reportes de seguimiento e implementación de ACPM. • 	<ul style="list-style-type: none"> • Presidente de CISA. • Comité institucional de gestión y desempeño. • Organismos del estado. • Entes de control. • Auditoría Interna. • Comité asesor de Junta Directiva de Auditoría. •
<ul style="list-style-type: none"> • Todos los procesos de CISA. • Proveedores 	<ul style="list-style-type: none"> • Inventario de activos de información valorados y clasificados. • Matriz de riesgos de seguridad de la información. • Informes de auditoría de seguridad de la información. • Incidentes de seguridad de la información clasificados, valorados, tratados y documentados. • Reportes de seguimiento e implementación de ACPM. 	<p>Seguimiento y medición del desempeño de la seguridad de la información:</p> <ul style="list-style-type: none"> • P: Definir los mecanismos y procedimientos a través de los cuales se le hace medición y seguimiento a la gestión de la seguridad de la información. • H: Recopilar resultados del desempeño de la gestión de la seguridad de la información. • H: Realizar la revisión por la dirección. • V: Verificar el cumplimiento de la estrategia de seguridad de la información. • V.A: Seguimiento al cierre de hallazgos de revisiones y auditorías internas y externas de seguridad de la información. 	<ul style="list-style-type: none"> • Informe de revisión de la seguridad de la información por la dirección de CISA. • Informe de seguimiento y cierre de ACPM. • Informe de medición de avance de la implementación de la estrategia de seguridad de la información • 	<ul style="list-style-type: none"> • Presidente. • Comité institucional de gestión y desempeño. • Organismos del estado. •



PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES
<ul style="list-style-type: none"> Organismos del estado. <p>Todos los procesos de CISA.</p>	<ul style="list-style-type: none"> Constitución política, leyes y decretos. Directivas presidenciales y circulares. Normas, resoluciones y acuerdos, guías, instructivos y requerimientos del estado colombiano. Normatividad interna (Circulares normativas, manuales, políticas, guías, instructivos) Requerimientos contractuales. Aspectos e impactos ambientales Activos de información MIPG 	<p>• V: Verificar el cumplimiento de las metas</p> <p>V. A: Control y seguimiento a la implementación y cierre de acciones correctivas o de mejora relacionadas con la seguridad de la información.</p> <p>Identificación y evaluación de requisitos legales aplicables</p> <ul style="list-style-type: none"> P: Definir el procedimiento requeridos para la gestión del Sistema de gestión ambiental, SST y SGSI. P.H: Identificar los requisitos legales asociados a la gestión ambiental y a la gestión de Seguridad de la Información. H: Asegurar que se comunican a los funcionarios y contratistas la normatividad aplicable a la entidad, con referencia a la gestión ambiental y a la gestión de Seguridad de la Información. H: Realizar análisis de brecha del estado actual de cumplimiento de normas aplicables a la gestión ambiental y a la gestión de Seguridad de la Información. V: Verificar el cumplimiento de las políticas, los procedimientos y controles de seguridad de la información. V: Gestionar la realización de evaluaciones independientes de controles y estado de las vulnerabilidades de seguridad de la información. V: Evaluar el cumplimiento de los requisitos legales y otros suscritos aplicables a la seguridad de la información. V.A: Identificar e implementar acciones preventivas, correctivas o de mejora para mejorar el cumplimiento normativo y legal aplicable a la gestión ambiental y a la gestión de Seguridad de la Información. <p>Control de documentos:</p> <ul style="list-style-type: none"> P. Definir y determinar políticas para el control la documentación del SIG en CISA. H. Realizar levantamiento de información y elaborar procedimiento. H. Realizar Análisis de impacto. H. Actualizar, modificar, elaborar o eliminar documentos del SIG. V. Identificar aspectos e impactos ambientales. V. Identificar peligros y riesgos de SST V. Verificar documentación actualizada con líderes de proceso. A. Adecuar documentación de acuerdo con observaciones. V.A: Asegurar la disponibilidad de documentos vigentes. 	<ul style="list-style-type: none"> Informes de análisis de brecha y evaluaciones en seguridad de la información. Matriz de Requisitos Legales Ambientales y de Seguridad de la Información Acciones correctivas o de mejora 	<ul style="list-style-type: none"> Comité institucional de gestión y desempeño. Organismos del estado. Entes de control. Procesos que implementan control operacional
<ul style="list-style-type: none"> Todos los procesos de CISA 	<ul style="list-style-type: none"> Solicitud para elaborar o modificar documentos del SIG. Solicitud de modificación normograma de proceso Actas de Comités de Junta Directiva, Presidencia o del Negocio Modelo Integrado de Planeación y Gestión Proyectos de mejora de aplicativos 	<ul style="list-style-type: none"> Solicitudes de revisión y aprobación publicación documento Publicación documento del SIG Actualizado. Solicitud revisión cambios documentos del SIG vs. Impactos en aplicativos institucionales. Solicitud Actualización documentación página WEB y otros medios, en los casos que aplique. 	<ul style="list-style-type: none"> Todos los procesos de CISA PMO Dirección de Comunicaciones, Mercado y Relacionamiento 	



PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES
<ul style="list-style-type: none"> Todos los procesos de CISA Otras partes interesadas 	<ul style="list-style-type: none"> No conformidades reales detectadas. Oportunidades de mejora detectadas. Riesgos Modelo Integrado de Planeación y Gestión • 	<p>Acciones Correctivas y de mejora:</p> <ul style="list-style-type: none"> P. Definir y determinar políticas para llevar a cabo las acciones correctivas y/o de mejora en CISA. H. Detección de no conformidades reales y/u oportunidades de mejora. H. Asesorar a los líderes de proceso en la eliminación de la causa raíz y la elaboración del plan de acción. H. Asignar auditores internos del SIG para seguimiento de ACPM y revisión de eficacia. V.A. Control, seguimiento y cierre de Acciones correctivas o de mejora. <p>Control del Producto y/o Servicio No conforme:</p> <ul style="list-style-type: none"> P. Definir y determinar políticas y lineamientos para llevar a cabo el tratamiento del producto y/o servicio No Conforme. H.V. Recopilar información de producto y/o servicio no conforme, para realizar revisión por la dirección. A. Proponer Acciones correctivas y/o de mejora, con respecto al producto no conforme detectado. <p>Seguimiento y Medición del desempeño del SIG:</p> <ul style="list-style-type: none"> P. Definir y determinar políticas para el seguimiento y medición de los procesos del SIG. H. Asesorar a los procesos en la creación de mecanismos de seguimiento y medición. H. Recopilar resultados del desempeño del SIG. V. Verificar cumplimiento de metas de los procesos. V.A. Control, seguimiento y cierre de Acciones correctivas y/o de mejora. <p>Gestión Ambiental</p> <ul style="list-style-type: none"> P. Identificar y/o actualizar los aspectos ambientales provenientes de las actividades de los procesos del SIG. P.H. Realizar la evaluación de los aspectos ambientales. 	<ul style="list-style-type: none"> Asignación de Auditor Interno del SIG. Seguimiento a la implementación y cierre de acciones correctivas y de mejora. Reporte de seguimiento a ACPM para revisión por la dirección. Comunicación Plan de Acción de la Revisión por la Dirección 	<ul style="list-style-type: none"> Todos los procesos de CISA Alta Dirección Todos los procesos de CISA
Procesos Misionales.	<ul style="list-style-type: none"> Identificación de producto y/o servicio no conforme. Reporte del tratamiento del producto y/o servicio no conforme • 		<ul style="list-style-type: none"> Seguimiento a la implementación y cierre de acciones correctivas y de mejora provenientes de Producto o servicio No Conforme. Reporte de seguimiento al producto no conforme para revisión por la dirección. Comunicación Plan de Acción de la Revisión por la Dirección. 	<ul style="list-style-type: none"> Procesos Misionales. Alta Dirección Todos los procesos de CISA
Todos los procesos de CISA	<ul style="list-style-type: none"> Reporte de resultados de indicadores de Gestión del SIG. Aspectos e Impactos Ambientales Peligros y Riesgos SST Riesgos Ánálisis de resultados. Implementación de acciones correctivas y/o de mejora. Resultados de las inspecciones ambientales y SGSSST Incidentes y enfermedades de trabajo Competencia y Formación PQRD Controles de Seguridad de la Información 		<ul style="list-style-type: none"> Seguimiento a la implementación y cierre de acciones correctivas y de mejora. Reporte resultados del desempeño de procesos en la página web de CISA y aplicativo ISOlución. Reporte de seguimiento y medición de los procesos para revisión por la dirección. Comunicación Plan de Acción de la Revisión por la Dirección. 	<ul style="list-style-type: none"> Todos los procesos de CISA Clientes y Partes Interesadas Todos los procesos de CISA Alta Dirección Todos los procesos de CISA •
• Todos los procesos de CISA	<ul style="list-style-type: none"> Actividades y operaciones realizadas por los procesos Estratégicos, Misionales, de Apoyo y de Control. Aspectos ambientales. 		<ul style="list-style-type: none"> Matriz Aspectos e Impactos Ambientales Programas, y controles operacionales aprobados e implementados. Informes de desempeño. Registro de Capacitaciones. 	<ul style="list-style-type: none"> Todos los procesos



PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES
<ul style="list-style-type: none"> • Todos los procesos de CISA • Partes Interesadas • Gerencia de Recursos • Gerencia Inmobiliaria • Gerencia de Cartera Jefatura de Operaciones Tecnológicas 	<ul style="list-style-type: none"> • Comunicaciones o requerimientos internos y externos asociadas aspectos e impactos, programas y controles. • Evaluación y reevaluación de proveedores • Informe de desempeño de proveedores • 	<ul style="list-style-type: none"> • H. Realizar la valoración de los impactos ambientales • P.H. Determinar los controles operacionales necesarios para la mejora del desempeño ambiental. • P.H. Establecer e implementar planes y programas para el control de los impactos ambientales identificados. • H. Comunicar los programas y controles relacionados con los impactos ambientales de las actividades en las que participan. • V. Verificar el cumplimiento eficaz de los programas y planes para el control de los impactos ambientales. • V. Gestionar la realización de evaluaciones, monitoreos e inspecciones requeridos para el seguimiento y evaluación de SGA. • P.H. Establecer plan de Emergencia ambiental. • V.A. Seguimiento a la implementación y al cierre de Acciones correctivas y/o de mejora asociadas. 	<ul style="list-style-type: none"> • Reporte del desempeño ambiental del SIG para revisión por la dirección. • Comunicación Plan de Acción de la Revisión por la Dirección. • 	<ul style="list-style-type: none"> • Alta Dirección • Todos los procesos de CISA.
<ul style="list-style-type: none"> • Auditores Internos del SIG. • Auditoría Interna 	<ul style="list-style-type: none"> • Plan de Auditorías. • Informes de auditoría • Necesidades de cierre de hallazgos. • Programa Anual de Auditorías Internas • 	<p>Auditorías Internas del SIG:</p> <ul style="list-style-type: none"> • P. Definir y determinar políticas para las Auditorías Internas del SIG. • P. Determinar Programa de Auditorías Internas del SIG. • H. Asignar Auditores Internos a los procesos. • V. Realizar seguimiento al cumplimiento del programa de Auditorías. • H.V. Solicitar informes de auditorías y realizar seguimiento a su entrega. • V.A. Seguimiento a la implementación y al cierre de Acciones correctivas y/o de mejora. 	<ul style="list-style-type: none"> • Programa de Auditorías Internas del SIG. • Seguimiento a la implementación y cierre de acciones correctivas preventivas y de mejora provenientes de auditorías internas del SIG. • Reporte resultados de Auditorías Internas del SIG para revisión por la dirección. • Comunicación Plan de Acción de la Revisión por la Dirección. • 	<ul style="list-style-type: none"> • Todos los procesos de CISA • Comité Institucional de Gestión y Desempeño <p>Todos los procesos de CISA</p> <ul style="list-style-type: none"> • Alta Dirección • Todos los procesos •
<ul style="list-style-type: none"> • Dirección de Planeación Estratégica y Sistemas de Información 	<ul style="list-style-type: none"> • Misión, Visión • Objetivos a corto, mediano y largo plazo. • Estrategias • Seguimiento al cumplimiento de los planes de tratamiento de riesgo operativo y de corrupción • Seguimiento al cumplimiento de los planes sectoriales • 		<ul style="list-style-type: none"> • Cumplimiento de los objetivos y del direccionamiento estratégico. • Cumplimiento de los Proyectos del Proceso • 	<ul style="list-style-type: none"> • Dirección de Planeación Estratégica y Sistemas de Información •



PROVEEDORES	ENTRADAS	DESARROLLO DEL PROCESO	SALIDAS	CLIENTES
• Gerencia de Recursos	<ul style="list-style-type: none"> Personal competente para el desempeño de funciones. Desarrollo del talento humano Respuesta de requerimientos de los diferentes procesos. Pago de Nómina. Desarrollo de las políticas y beneficios EFR. Desarrollo del plan de bienestar Ejecución del Sistema de Gestión de Seguridad y Salud en el trabajo, los planes y PVE. Entrega de elementos ergonómicos. Comunicaciones de lecciones aprendidas asociadas a incidentes de salud y seguridad del trabajo. 		<ul style="list-style-type: none"> Necesidades de capacitación Evaluación de competencias y requerimientos generales. Reporte utilización políticas EFR y oportunidades de mejora. Peligros y Riesgos de Seguridad y Salud en el trabajo Reporte de incidentes y condiciones inseguras de trabajo. 	<ul style="list-style-type: none"> Gerencia de Recursos Gestión del Talento COPASST
• Gerencia de Recursos Coordinación de Gestión Documental	<ul style="list-style-type: none"> Sondeos de mercado según los requerimientos Entrega de bienes y servicios Entrega de suministros Infraestructura física en condiciones seguras Entrega de correspondencia Tablas de retención documental Tiquetes 		<ul style="list-style-type: none"> Requerimientos y Justificaciones. Términos de Referencia. Solicitudes de Pedidos de suministros. Solicitudes de Mantenimiento y reparaciones Documentos de Correspondencia Entrega de Documentos para archivo Solicitud de tiquetes 	<ul style="list-style-type: none"> Gerencia de Recursos Coordinación de Gestión Documental
Jefatura de Control Interno Disciplinario	<ul style="list-style-type: none"> Políticas y lineamientos para la aplicación del control disciplinario interno. 		<ul style="list-style-type: none"> Requerimientos, comunicaciones escritas, magnéticas o verbales, sobre hechos que puedan constituir faltas disciplinarias (si aplica) 	<ul style="list-style-type: none"> Jefatura de Control Interno Disciplinario
• Jefatura de Operaciones Tecnológicas	<ul style="list-style-type: none"> Servicios de Tecnología SW y HW (permisos, elementos, licencias, aplicativos, equipo de cómputo y comunicaciones). Servicio de soporte tecnológico 		<ul style="list-style-type: none"> Solicitud de creación de usuarios y autorización de servicios Solicitud de servicios informáticos Solicitud soporte tecnológico 	<ul style="list-style-type: none"> Jefatura de Operaciones Tecnológicas



INDICADORES DE GESTIÓN		DOCUMENTOS A APLICAR
EFICACIA	<ul style="list-style-type: none"> ✓ Acciones correctivas, preventivas y de mejora implementadas oportunamente. ✓ Acciones para Tratamiento de Riesgos S.I. ✓ Gestión de vulnerabilidades Técnicas 	<ul style="list-style-type: none"> • MN011: Código de Buen Gobierno • MN013: Manual del Sistema Integrado de Gestión. • MN015: Manual EFR – Empresa Familiarmente Responsable • MN018: Sistema de Gestión de Seguridad y Salud en el Trabajo • MN022: Manual de Continuidad del Negocio • CN016: Elaboración y control de documentos del SIG. • CN023: Programa de Gestión Documental. • CN093: Políticas y Procedimientos de Infraestructura Tecnológica • CN120: Políticas y procedimiento para Planear y ejecutar Auditorías Internas al SIG. • CN107: Política y procedimientos para la Gestión de Riesgos. • CN128: Políticas y procedimientos de Seguridad de la Información • MN014: Política de Comunicación Institucional • Memorando Circular 056: Procedimiento para el Estudio de Productividad de Soluciones de Cartera • Memorando Circular No. 37: Política de tratamiento de datos personales • Normograma por Procesos Sistema Integrado de Gestión – SIG
EFICIENCIA	<ul style="list-style-type: none"> ✓ Nivel de Consumo de resmas de papel Dirección General ✓ Nivel de Consumo de resmas de papel Agencia Centro ✓ Generación de Residuos Sólidos Inorgánicos ✓ Porcentaje de incidentes de Seguridad de la Información ✓ Gestión de la Cultura en Seguridad de la información 	

REVISÓ	APROBÓ
JEFE DE PROCESOS Y PRODUCTIVIDAD	JEFE DE PROCESOS Y PRODUCTIVIDAD