1. INTRODUCCIÓN

Un entorno digital se define como un ambiente, tanto físico como virtual sobre el cual se soporta la economía digital[1]. Los ciudadanos acceden a diferentes tramites y servicios que presta el Instituto Geográfico Agustín Codazzi - IGAC a través de estos entornos digitales, por lo cual surge la necesidad de identificar y gestionar los diferentes riesgos asociados a la seguridad digital.

Bajo el decreto 1008 de 2018 se establecen los lineamientos generales de la política de Gobierno Digital y se describen los principios que rigen la función y los procedimientos administrativos. Uno de estos principios es el de Seguridad de la Información, el cual soporta su implementación en el Modelo de Seguridad y Privacidad de la Información – MSPI definido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, dicho modelo contempla un ciclo de operación que consta de cinco (5) fases: Diagnóstico, Planificación, Implementación (Hacer), Evaluación de desempeño (verificar) y Mejora Continua (Actuar), un ciclo PHVA, lo cual lo enmarca dentro de un sistema de gestión en correlación con la norma ISO 27001.

El IGAC establece bajo la resolución 1840 de 2018 la política del Sistema de Gestión Integrado del IGAC donde incorpora los requisitos de cada uno de los sistemas de gestión y control que lo conforman y en el cual se incluye la del Sistema de Gestión de Seguridad de la Información; de otro lado también se asigna al Jefe de la Oficina de Informática y Telecomunicaciones como el responsable de liderar la implementación y seguimiento a la política de seguridad de la información y quien será el enlace sectorial de seguridad digital. Para el presente documento cuando se enuncie la política de seguridad de la información, se entenderá que es la política de seguridad digital.

Así mismo, bajo la resolución 993 del 2017 se implementa la Política Pública de Protección de datos Personales en el IGAC, donde se dan los lineamientos a seguir para la creación, tratamiento y cierre de las bases de datos que posean datos personales.

De otro lado, bajo la resolución 320 de 2018 se crea y conforma el Comité Institucional de Gestión y Desempeño del IGAC, el cual dentro de sus funciones se encuentra la de "Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad digital y de la información"; por consiguiente, desde dicho comité se articularán los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la presente política.

2. OBJETIVO

Fortalecer los lineamientos para el cumplimiento de los objetivos de seguridad de la información en entornos digitales, a través de la identificación, valoración, tratamiento y mitigación de los riesgos de seguridad digital del IGAC en un marco de cooperación, colaboración y asistencia.

3. ALCANCE

Es aplicable a todas las sedes, los procesos, actividades, servicios, unidades móviles y demás escenarios donde se desarrollen las actividades del instituto incluyendo al personal vinculado de forma directa e indirecta al IGAC, así como a los visitantes.

4. ROLES Y RESPONSABILIDADES

La asignación de roles y responsabilidades para la seguridad de la información se define a continuación.

[1] Conpes 3854 - POLÍTICA NACIONAL DE SEGURIDAD DIGITAL. Ver https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf al 2020-07-31.

4.1 COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO-ALTA DIRECCIÓN

- Asegurar la implementación y desarrollo de políticas de gestión y directrices en materia de seguridad digital y de la información.
- Lo anterior, mediante el cumplimiento de las siguientes actividades:
- Aprobar y hacer seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad de la información.
- Socializar la importancia de adoptar la cultura de seguridad de la información a los procesos de la entidad.
- Aprobar acciones y mejores prácticas que contribuyan en la implementación del SGSI.
- Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.

4.2 OFICINA DE INFORMÁTICA Y TELECOMUNICACIONES

- Liderar la planificación e implementación del SGSI.
- Integrar el Sistema de Gestión de Seguridad de la Información – SGSI con el Sistema de Gestión Integrado- SGI.
- Brindar apoyo en los temas que requiera el Comité Institucional de Gestión y Desempeño de la entidad, en materia de seguridad de la información y proponer acciones de mejora del SGSI.
- Definir y elaborar los procedimientos que sean de su competencia para la operación del SGSI.
- De acuerdo con las solicitudes realizadas por los proyectos y/o procesos, realizar el acompañamiento correspondiente en materia de seguridad de la información.
- Incluir en el procedimiento de administración de riesgo los aspectos de seguridad de la información de la entidad.
- Liderar y brindar acompañamiento a los procesos de la entidad en la gestión de riesgos de seguridad de la información y seguimiento al plan de tratamiento de riesgos.
- Proponer la formulación de políticas y lineamientos de seguridad de la información.
- Definir e implementar socializaciones de seguridad de la información para servidores públicos y contratistas.
- Apoyar a los procesos en los planes de mejoramiento para dar cumplimiento a las recomendaciones en materia de seguridad de la información.
- Presentar los resultados de los indicadores del SGSI al Comité Institucional de Gestión y Desempeño.
- Actualizar manuales, procedimientos, metodologías y documentación del SGSI que sea de su competencia.
- Definir e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la entidad.
- Efectuar acompañamiento a los procesos en la implementación de las Políticas de Seguridad de la Información en la entidad.
- Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad de la información.

4.3 OFICINA ASESORA JURÍDICA

- Brindar asesoría a la Oficina de Informática y Telecomunicaciones en materia de temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad de la información.
- Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad de la información.
- Verificar que los contratos o convenios de ingreso que por competencia deban suscribir los procesos de la Sede Central y Territoriales, cuenten con cláusulas de derechos de autor, de confidencialidad y no divulgación de la información según sea el caso.

- Representar a la Entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad de la información.
- Apoyar a los procesos en la elaboración del índice de información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.
- Implementar los controles de seguridad definidos por la Oficina Asesora Jurídica, con el acompañamiento de la Oficina de Informática y Telecomunicaciones cuando sea solicitado.

4.4 GIT GESTIÓN CONTRACTUAL (SEDE CENTRAL) O EL PROFESIONAL CON FUNCIONES DE ABOGADO EN LAS DIRECCIONES TERRITORIALES

- Incluir acuerdos de confidencialidad y no divulgación de información en los contratos de egreso.
- Implementar los controles de seguridad del proceso de Gestión Contractual, con el acompañamiento de la Oficina de Informática y Telecomunicaciones cuando sea solicitado.
- Implementar los controles necesarios para dar cumplimiento a la ley de protección de datos personales, relacionados con los contratistas y terceros.
- Debe informar a los supervisores e interventores, el inicio de la ejecución de los contratos de para su respectiva gestión y trámites internos en la entidad.
- Debe proteger la información de los contratistas y terceros, de acuerdo con la regulación vigente de datos personales.
- Debe revisar que los documentos exigidos para suscribir el contrato se encuentren en el expediente de cada proceso, de acuerdo con la regulación vigente.
- Debe solicitar a los contratistas y terceros la autorización para el uso y tratamiento de los datos personales de acuerdo con la normatividad legal vigente.

4.5 GIT GESTIÓN DEL TALENTO HUMANO O EL PROFESIONAL ESPECIALIZADO CON FUNCIONES DE ABOGADO EN LAS DIRECCIONES TERRITORIALES

- Controlar y salvaguardar la información de datos personales del personal de planta del IGAC, en concordancia con la normatividad vigente.
- Implementar los controles de seguridad del proceso Talento Humano, con el acompañamiento de la Oficina de Informática y Telecomunicaciones cuando sea solicitado.
- Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a la normatividad vigente.
- Debe realizar las verificaciones requeridas por la regulación vigente, para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo provisional o de libre nombramiento y remoción en el IGAC, antes de su vinculación definitiva.
- Debe asegurar que el personal candidato a ocupar un cargo provisional o de libre nombramiento y remoción en el IGAC cumpla con las competencias necesarias para proveer el cargo en los aspectos de educación, formación o experiencia solicitada.
- Debe proteger la información del personal candidato de acuerdo con la regulación vigente de datos personales.
- La vinculación de los servidores públicos se da con el cumplimiento de los requisitos y documentos exigidos por Ley.
- Debe solicitar al personal de libre nombramiento y remoción, la autorización debidamente firmada para el uso y tratamiento de los datos personales de acuerdo con la normatividad legal vigente.
- Debe informar los deberes y responsabilidades como servidor público.
- Debe construir con el apoyo de la oficina de Informática y Telecomunicaciones el plan de capacitación en temas de seguridad de la información según los requerimientos de la entidad.
- Debe verificar las novedades de vinculación, desvinculación, traslados del personal u otras, y notificarlas a la Oficina de Informática y Telecomunicaciones, para realizar las actividades respectivas sobre los usuarios en el sistema.

- Debe notificar en la inducción y reinducción a todos los servidores públicos y contratistas de la Entidad, sobre el cumplimiento de las políticas, lineamientos de seguridad de la información y demás relacionadas.
- Debe comunicar a los servidores públicos, el cumplimiento de las responsabilidades y los deberes de seguridad de la información que continúan vigentes después de la desvinculación de acuerdo con lo estipulado en la regulación vigente.
- Los servidores públicos en el momento de traslado o desvinculación con la Entidad deben entregar a los jefes inmediatos o supervisores todos los elementos tanto de información física, lógica y demás que le fueron entregados para la realización de sus funciones.
- Todos los servidores públicos deben presentar una paz y salvo al finalizar su vinculación con la Entidad, para que se deshabilite el acceso de usuario al Dominio.

4.6 OFICINA DE CONTROL INTERNO

- Elaborar y presentar el programa de auditoría del SGSI al Comité Institucional de Coordinación de Control Interno para aprobación.
- Realizar las auditorías internas del SGSI de acuerdo con el plan definido en la entidad.
- Informar a quien corresponda, los hallazgos, no conformidades, observaciones y oportunidades de mejora relacionadas con el SGSI.
- Presentar y socializar a quien corresponda, los resultados de las auditorías en materia del SGSI.
- Evaluar y realizar seguimiento al plan de mejoramiento del SGSI en cada uno de los procesos.
- Implementar los controles de seguridad del proceso de evaluación y control de la gestión interna, con el acompañamiento de la Oficina de Informática y Telecomunicaciones cuando sea solicitado.

4.7 GIT GESTIÓN DE SERVICIOS ADMINISTRATIVOS

- Coordinar y/o realizar el mantenimiento de la infraestructura de seguridad física.
- Realizar el apoyo y/o acompañamiento en la implementación, seguimiento y supervisión de los controles de seguridad física de sede central y territoriales.
- Gestionar ante la aseguradora cuando corresponda los diferentes eventos y/o incidentes relacionados con la seguridad física que pongan en riesgo la seguridad de la información.
- Gestionar la adquisición y supervisar la instalación de los controles de acceso de seguridad física (biométricos u otros) en sede central, con el acompañamiento de la Oficina de Informática y Telecomunicaciones cuando sea solicitado.
- Velar por el normal funcionamiento de los aires acondicionados. Se exceptúan los aires acondicionados del centro de datos.

4.8 OFICINA ASESORA DE PLANEACIÓN

- Apoyar y participar metodológicamente en la formulación, aprobación y publicación de metodologías, procedimientos, políticas, lineamientos, manuales, entre otros, del SGSI para la alineación y articulación con el Sistema Integrado de Gestión.
- Socializar la metodología para la construcción de los mapas de riesgos a los procesos de la entidad.

4.9 GIT GESTIÓN DOCUMENTAL

- Proponer e implementar los controles de seguridad de la información definidos para los activos de información que custodia, con el acompañamiento de la Oficina de Informática y Telecomunicaciones cuando sea solicitado.
- Reportar los incidentes de seguridad de la información asociados a los activos que custodia, en la herramienta de gestión provista para tal fin por la Oficina de Informática y Telecomunicaciones.
- Custodiar y preservar la información que se encuentra en el archivo central.

- Apoyar a los procesos en la actualización, creación y definición de las tablas de retención documental como insumo para el levantamiento y/o actualización del inventario de activos de información.

4.10 GIT CONTROL DISCIPLINARIO

- El GIT Control Disciplinario implementará las acciones disciplinarias correspondientes, por las posibles o presuntas violaciones de la política de seguridad de la información, de acuerdo con la falta en que incurran los servidores públicos de la entidad vinculados y/o desvinculados, según los resultados de la investigación.

4.11 PROCESO DE COMUNICACIONES

- Producir piezas de comunicación las cuales pueden ser digitales o impresas, con mensajes
- institucionales relacionados con seguridad de la información para comunicación interna.
- Publicar, divulgar información y mensajes institucionales a través de la página web, IGACNET, pantallas digitales, redes sociales y correo institucional relacionados con seguridad de la información.
- Facilitar la comunicación y divulgación de las Políticas de Seguridad de la información, establecidas en este manual a los servidores públicos y contratistas de la entidad.

4.12 DIRECTORES TERRITORIALES

- Reportar los incidentes de seguridad de la información asociados a los activos que custodia tanto en la territorial como en las unidades operativas de Catastro, en la herramienta de gestión provista para tal fin por la Oficina de Informática y Telecomunicaciones.
- Realizar seguimiento al cumplimiento de las políticas y lineamientos de seguridad de la información para proteger y preservar la confidencialidad, integridad y disponibilidad de la información, tanto en la territorial como en las unidades operativas de Catastro.

4.13 PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Realizar la identificación, clasificación y valoración de los activos de información en su proceso.
- Realizar la actualización del inventario de activos de información de su proceso cuando se requiera y socializarlo con la Oficina de Informática y Telecomunicaciones de la entidad y en el caso que competa reportar al GIT Gestión Documental.
- Velar por el cumplimiento de los lineamientos del tratamiento de la información para asegurar la integridad, confidencialidad y disponibilidad del activo de información asignado.
- Realizar la implementación y el seguimiento al cumplimiento de las actividades y controles de seguridad de la información en su proceso.
- Gestionar los recursos necesarios para la implementación de los controles de seguridad de la información para la gestión de riesgos sobre los activos de información en su proceso.
- Desarrollar los planes de mejoramiento de seguridad de la información asociados a los resultados de las auditorías internas del SGSI y demás mecanismos de análisis, seguimiento y evaluación.
- Apoyar la planificación, implementación, evaluación de desempeño y mejora continua del SGSI en su proceso.
- Participar en la sensibilización y/o capacitaciones del SGSI.
- Realizar la identificación, evaluación y tratamiento de riesgos sobre los activos de información relacionados con su proceso, con el acompañamiento de la Oficina de Informática y Telecomunicaciones.
- Reportar a la Oficina de Informática y Telecomunicaciones los incidentes de seguridad de la información.
- Participar de manera activa en la solución de los incidentes de seguridad de la información.

4.14 CUSTODIOS DE LA INFORMACIÓN

- Los custodios de la información son personas, procesos, proveedores u otros, designados por los propietarios de los activos de información para administrar la seguridad de los activos de información.
- Proponer y definir los controles de seguridad de la información para los activos de información que custodia.
- Implementar los controles de seguridad definidos en los activos de información que custodia para garantizar los criterios de Confidencialidad, Integridad y Disponibilidad de la información.
- Reportar los incidentes de seguridad de la información asociados a los activos que custodia, a la Oficina de Informática y Telecomunicaciones de la entidad.

4.15 SERVIDORES PÚBLICOS, CONTRATISTAS Y TERCEROS

- Dar cumplimiento a los manuales, procedimientos, lineamientos y políticas del Sistema de Gestión de Seguridad de la Información del IGAC.
- Reportar eventos o incidentes de seguridad de la información a la Oficina de Informática y Telecomunicaciones.
- Administrar y gestionar la información de tal forma que se garanticen los criterios de confidencialidad, integridad y disponibilidad de los activos de información de la entidad.
- Dar cumplimiento a la Ley de protección de datos personales.
- Firmar y cumplir los acuerdos de confidencialidad y no divulgación de la información.
- Los servidores públicos de la entidad deben cumplir con los acuerdos de confidencialidad y no divulgación de información establecidos en la Ley 734 de 2002.
- Participar en las sensibilizaciones y/o capacitaciones del SGSI.
- Todos los servidores públicos, contratistas y terceros deben tomar conciencia de su aporte a la eficacia de la seguridad de la información, y aplicarla en beneficio de una mejora del desempeño de sus funciones.
- Todos los servidores públicos, contratistas y terceros deben entregar de manera formal a los
- supervisores y/o jefes inmediatos, todos los elementos tanto de información física, lógica y demás que le fueron entregados para la realización de sus funciones.
- Solicitar la expedición del carné que lo acredita como servidor público y/o contratista del Instituto.
- Todos los servidores públicos, contratistas y terceros deben mantener la confidencialidad de la información por fuera de las instalaciones del IGAC.
- La responsabilidad de seguridad de la información es pieza fundamental de los términos y condiciones del empleo. La violación o no cumplimiento de las responsabilidades y lineamientos definidos en las políticas de seguridad de la información del IGAC, serán causa de la aplicación de acciones disciplinarias.

5. DESARROLLO

La política de seguridad de la información se soporta en la definición de políticas específicas de seguridad de la información que se describen a continuación:

5.1 POLÍTICA DISPOSITIVOS MÓVILES

Las medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles serán orientadas con el objeto de mitigar los riesgos asociados al acceso, pérdida y divulgación no autorizados de la información del IGAC, a través de la asignación de controles asociados con la asignación de privilegios de acceso, borrado seguro de la información y aplicación de técnicas de cifrado.

5.2 POLÍTICA TELETRABAJO

El IGAC debe implementar medidas para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo (todas las formas de trabajo

por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual").

5.3 POLÍTICA DE USO ACEPTABLE

Los servidores Públicos, contratistas y terceros que laboran en las instalaciones del IGAC (vinculados con un proveedor (empresa o entidad externo)), deben conocer y aplicar las reglas para el uso aceptable de los activos de información, incluyendo los recursos tecnológicos, donde se realiza el procesamiento de la información.

5.4 POLÍTICA DE CONTROL DE ACCESO

El acceso de los servidores Públicos, contratistas y terceros que laboran en las instalaciones del IGAC (vinculados con un proveedor (empresa o entidad externo)) a la información y a los recursos tecnológicos del IGAC, debe ser debidamente solicitado y autorizado por el responsable de dicho recurso, basado en la premisa "Todo está restringido, a menos que esté expresamente permitido".

5.5 POLÍTICA SOBRE EL USO DE CONTROLES CRIPTOGRÁFICOS

El intercambio de los datos clasificados como información pública reservada debe usar técnicas de cifrado de información para garantizar la protección y privacidad en el intercambio de la información; de igual manera se debe proteger y definir un tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
La adopción de controles de cifrado y firma digital de datos serán un mecanismo que minimice la materialización de riesgos de seguridad de la información.

5.6 POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

Los papeles, medios de almacenamiento removibles y archivos que se encuentran desplegados en las pantallas de las terminales/equipos de cómputo, deben mantenerse de forma protegidos.

5.7 POLÍTICAS DE TRANSFERENCIA DE INFORMACIÓN

La información que es transferida internamente o hacia terceros, debe ser protegida contra interceptación, copiado, modificación, enrutado y destrucción, de acuerdo con su clasificación de información.

5.8 POLÍTICA DE DESARROLLO SEGURO

Los desarrollos de software deben ser efectuados con base en la aplicación de reglas y técnicas de programación seguras, que refuercen la seguridad del nuevo sistema o la mejora de los ya existentes.

5.9 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES

Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores en la etapa precontractual y contratistas a los activos de información del IGAC, se deben acordar durante las etapas de planeación (que inicia con la identificación de la necesidad y finaliza con la elaboración de los estudios previos) y precontractual del proceso de contratación que recae en el establecimiento de la relación contractual con un proveedor a través de la inclusión de cláusulas en los estudios previos y técnicos que den cumplimiento a los requisitos de seguridad de la información conforme a la norma ISO27001:2013.

6. IMPLEMENTACIÓN

A continuación, se describe la estrategia de planificación y control operacional necesaria para implementar el SGSI, la cual estará soportada por el desarrollo de planes que garanticen la gestión de riesgos de seguridad digital de forma efectiva, y el cumplimiento de los objetivos de seguridad de la información.

6.1 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Para dar cumplimiento a los objetivos de seguridad de la información del IGAC que se encuentran relacionados en el Manual del sistema de gestión integrado - SGI, a continuación, se presentan los mecanismos que evidencian su establecimiento:

Para el objetivo de seguridad de la información 1: *Definir lineamientos, políticas y procedimientos de seguridad de la información*, se deben documentar y socializar a los usuarios internos y externos del IGAC donde dichos documentos estén protegidos, controlados y disponibles para su uso, dónde y cuándo se necesite.

Para esto, el IGAC establece bajo la resolución 1840 de 2018 la política del Sistema de Gestión Integrado del IGAC, donde incorpora los requisitos de cada uno de los sistemas de gestión y control que lo conforman y en el cual se incluye la del SGSI, resaltando la importancia de orientar este sistema "hacia la protección de la privacidad, confidencialidad, integridad y disponibilidad de la información y activos, de los clientes y los grupos de interés, para habilitar el desarrollo de la misión institucional, en un ambiente controlado de riesgos de la información. La información es un activo primordial en la prestación de los servicios a la ciudadanía y la toma eficiente de decisiones, razón por la cual existe un compromiso expreso hacia la protección de las propiedades más significativas como parte de la estrategia orientada a la continuidad del negocio, la administración de riesgos asociados a la seguridad y privacidad de la información y la consolidación de una cultura de seguridad de la información".

Así mismo, el IGAC a través del documento *Elaboración, Actualización Y Control De La Información Documentada Establecida En El Sistema De Gestión Integrado – SGI*, estableció las actividades para identificar, elaborar, actualizar, derogar, revisar, aprobar, oficializar, divulgar y controlar los documentos correspondientes a los procesos establecidos en el Sistema de Gestión Integrado – SGI.

Por otro lado, en la caracterización del proceso de Gestión Informática se encuentra establecida la actividad: "*Implementar controles, estándares y procedimientos para alcanzar los niveles requeridos de calidad en los sistemas de información y servicios tecnológicos de la entidad*", la cual genera como salida controles, estándares y procedimientos que soportan la implementación del SGSI.

Para el objetivo de seguridad de la información 2: *Establecer la gestión de riesgos de seguridad asociados a la información de la Entidad*, se debe establecer lineamientos con base en lo establecido en el Modelo Integrado de Planeación y Gestión – MIPG, de forma integrada, donde la identificación de los riesgos de seguridad digital sean compatibles con la libertad de expresión, el libre, flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales, en concordancia con lo establecido en el CONPES 3854 Política Nacional de Seguridad Digital.

Para esto, el IGAC ha establecido una Política de Administración del Riesgo la cual tiene como objetivo fomentar la cultura de la prevención del riesgo en todos los niveles de la Institución, gestionar de forma anticipada las vulnerabilidades o eventos que puedan afectar el logro de los objetivos institucionales. Dicha política integra los lineamientos para identificar, tratar y manejar los riesgos de seguridad digital, de corrupción y de gestión.

Para el objetivo de seguridad de la información 3: *Implementar controles de seguridad con el objetivo de optimizar la gestión de la seguridad de la información en la Entidad, teniendo en cuenta los recursos disponibles*, se debe determinar los límites y la aplicabilidad del SGSI considerando la autoevaluación de la implementación del SGSI definiendo las prioridades frente a su implementación.

Para esto, el IGAC ha decidido implementar controles de seguridad de la información, de acuerdo con

las necesidades y expectativas evidenciadas en el documento denominado *Declaración de aplicabilidad*.

Así mismo aplica de forma continua el instrumento de autoevaluación (herramienta de diagnóstico) que hace parte del Modelo de Seguridad y Privacidad de la Información – MPSI y el cual arroja como resultado el estado actual de la entidad con respecto a la implementación de los objetivos de control de seguridad de la información y el nivel de madurez de dichos controles.

En relación con la implementación de los controles planeados para la presente vigencia, el IGAC se ha apoyado en recurso humano adicional a través de la contratación de servicios profesionales.

Para el objetivo de seguridad de la información 4: *Realizar la identificación y clasificación de los activos de información de la Entidad teniendo en cuenta los principios de confidencialidad, integridad y disponibilidad*, se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

Para esto, el IGAC ha establecido el procedimiento de Gestión de Activos el cual tiene por objeto gestionar la identificación y/o revisión, clasificación, publicación y etiquetado de los activos de información teniendo en cuenta los respectivos niveles de confidencialidad, integridad y disponibilidad, los propietarios, custodios y usuarios.

Para el objetivo de seguridad de la información 5: *Promover la cultura de seguridad de la información en la Entidad*, se deben establecer actividades de sensibilización, capacitación y educación en seguridad de la información de acuerdo con la caracterización de usuarios y la tipificación de estos con base en el acceso a la información del IGAC que cada uno tiene.

Para esto, el IGAC anualmente establece un plan de comunicación, sensibilización y capacitación en seguridad de la información el cual se mide a través de indicadores establecidos en el Plan de Acción anual de la Oficina De Informática Y Telecomunicaciones.

Para el objetivo de seguridad de la información 6: *Mantener el SGSI actualizado, vigente, auditado y velar por la mejora continua de la seguridad de la información de la Entidad*, se debe definir una estructura organizacional con funciones y responsabilidades que permita asegurar la dirección y apoyo gerencial, para soportar la administración y desarrollo de estrategias sobre seguridad de la información.

Para esto, el IGAC define un *Manual Sistema De Gestión Integrado – SGI* en el cual se describe el Sistema de Gestión Integrado (SGI) implementado en el IGAC y los sistemas que lo conforman; el SGSI hace parte de éste.

Estratégicamente el IGAC ha conformado un Comité Institucional de Gestión y desempeño, a través de la resolución N° 320 de 2018 "Por la cual se crea y conforma el Comité Institucional de Gestión y Desempeño del IGAC" en la cual se definen funciones específicas relacionadas con la Gestión de la Seguridad de la Información – "Artículo 4. Funciones del Comité Institucional de Gestión y Desempeño, numeral 6".

Así mismo, se puede identificar como en el manual de funciones del IGAC se establecen responsabilidades frente a la ejecución de funciones específicas con relación a la seguridad de la información: "Dar cumplimiento al componente de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea y a los estándares internacionales aplicables."

6.2 DOCUMENTACIÓN DEL SGSI

En el marco de la implementación del SGSI, el IGAC debe mantener documentada la información que

es necesaria para su eficacia, asegurando que:

En la creación y actualización de los documentos, éstos sean identificados y se defina el tipo de soporte (análogo, digital y electrónico).

El IGAC ha establecido el procedimiento *Manejo de Archivos de Gestión y Central*, el cual tiene como objetivo proporcionar a los funcionarios y contratistas una herramienta que los guie para el desarrollo de actividades de Gestión Documental relacionadas con la aplicación de las Tablas de Retención Documental (TRD), atendiendo las directrices del Archivo General de la Nación y el Programa de Gestión Documental del IGAC.

6.3 PLANIFICACIÓN Y CONTROL DE CAMBIOS DEL SGSI

En el marco de la implementación del SGSI, el IGAC debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acciones para mitigar los efectos adversos cuando sea necesario.

Para esto, los cambios en los sistemas de procesamiento de información se realizan a través de la *Administración del Control de Cambios en Infraestructura Tecnológica,* donde se establece un procedimiento que permita administrar y controlar los cambios realizados en los sistemas de información, aplicativos, portales y plataforma tecnológica del IGAC, para atender las solicitudes que generan los usuarios, minimizar los errores que puedan presentarse en los sistemas de información, mejorar los servicios e implementar medidas de seguridad.

7. SEGUIMIENTO

El seguimiento inicial de la presente política debe implementarse como una función continua de recolectar y analizar sistemáticamente información que permita determinar el progreso, el cumplimiento de los logros y objetivos y el uso de los recursos asignados en cada proyecto y plan a ejecutar.

Este seguimiento constituye la base para la gestión de una iniciativa del conocimiento y la innovación, ya que provee información sobre el progreso en la ejecución de la política, al comparar los avances logrados frente a las metas propuestas, en términos de los compromisos y los resultados.

Los resultados del seguimiento se registrarán en las herramientas de Autoevaluación establecidas dentro del Modelo Integrado de Planeación y Gestión (MIPG).

8. EVALUACION

La evaluación está a cargo de la Oficina de Control Interno, quienes en el IGAC se encargan de la tercera línea de defensa tal como lo establece el Modelo Integrado de Planeación y Gestión -MIPG en la Dimensión 7 "Control Interno", el objetivo de esta evaluación es el de proporcionar Información sobre la efectividad de los controles establecidos para la implementación del SGSI.

La evaluación a la presente política se hará anualmente y los criterios para dicha evaluación son los establecidos en los diferentes mecanismos implementados dentro del Sistema de Gestión Integrado como son:

- Seguimiento a los Riesgos.
- Seguimiento los Indicadores.
- Cumplimiento de los planes.
- Acciones correctivas y de Mejora.
- Cumplimiento de la Normatividad legal vigente.
- Cumplimiento a los requisitos establecidos por el IGAC.
- Revisión por la alta dirección.

9. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
13/08/2020	° Se adopta como versión 1 por corresponder a la creación del documento. Emisión Inicial Oficial.	1

Elaboró y/o Actualizó:	Revisó Técnicamente:	Revisó Metodológicamente:	Aprobó:
Nombre: Carlos Rafael González Contreras **Cargo:** Contratista Oficina Asesora de Planeacion	**Nombre:** Adriana Rocío Tovar Cortés **Cargo:** Jefe Oficina Asesora de Planeacion **Nombre:** Isis Johanna Gómez Peralta **Cargo:** Oficina Informática y Telecomunicaciones	**Nombre:** Laura Gonzalez Barbosa **Cargo:** Contratista Oficina Asesora de Planeacion	**Nombre:** Comité de Gestión y Desempeño del 13 de agosto de 2020