IGAC
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI

Sistema de Gestión Integrado MIPG

SGC
Sistema de Gestión de Calidad

SGA
Sistema de Gestión Ambiental

SGSST
Sistema de Gestión de la Seguridad y Salud en el Trabajo

SGD
Sistema de Gestión Documental

SCI
Sistema de Control Interno

SLNS
Sistema Laboratorio Nacional de Suelos

SGSI
Sistema de Gestión de Seguridad de la Información

IGAC
INSTITUTO GEOGRÁFICO AGUSTÍN CODAZZI

Sistema de Gestión Integrado MIPG

Manual de
Seguridad de la Información

Código: MN-GET-02 **Versión:** 1 **Vigente desde:** 11/06/2024

CONTENIDO

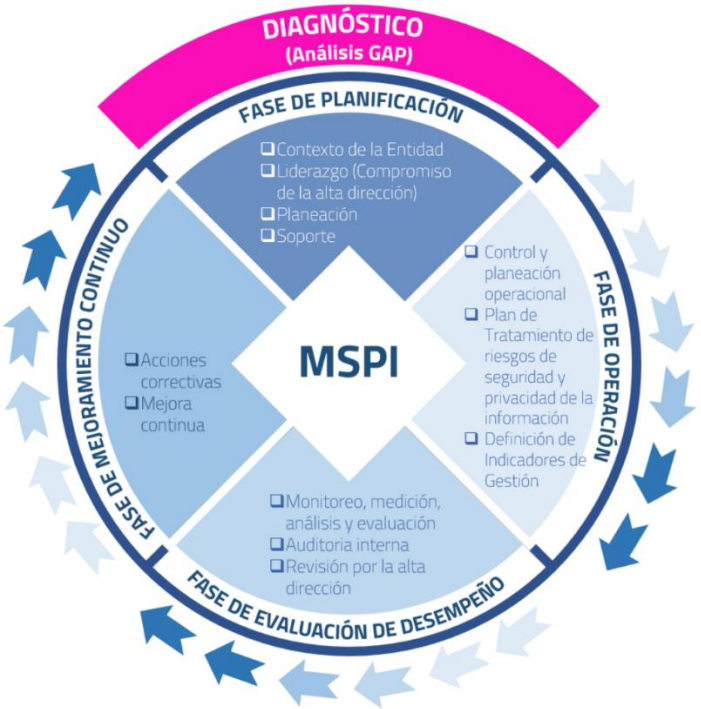
1. INTRODUCCIÓN

Con la evolución de las tecnologías de la información y las comunicaciones y el incremento exponencial de incidentes de seguridad de la información que generan afectaciones económicas y reputacionales a las entidades del estado; el Instituto Geográfico Agustín Codazzi-IGAC, en el marco de la implementación de la Política General de Seguridad de la Información y la mejora continua del Sistema de Gestión y Seguridad de la Información-SGSI, estableció el Manual de Seguridad de la información para definir lineamientos, documentar los controles existentes, prevenir, mitigar los riesgos asociados a la información (física y digital) y fortalecer la integridad y disponibilidad de la información.

El Sistema de Gestión de Seguridad de la Información del IGAC atiende los requerimientos normativos externos e internos, los componentes técnicos, tecnológicos y de funcionamiento, el SGSI está basado en el ciclo PHVA (Planear, Hacer, Verificar y Actuar) y se desarrollará en 5 fases:

1. **Diagnóstico**: Se realiza un diagnóstico para identificar el nivel de adopción de SGSI y el nivel de madurez de este, este se debe realizar por lo menos una vez al año.
2. **Planificación**: Se determina los requerimientos, el alcance y los objetivos del SGSI teniendo en cuenta sus procesos, el ser una entidad de orden nacional y el contexto interno y externo del IGAC. En esta fase se realiza el inventario y clasificación de los activos de información y la valoración y tratamiento de riesgos de la seguridad de la información.
3. **Operación**: En esta fase se implementan los controles administrativos, físicos y tecnológicos con el fin de disminuir el impacto o la probabilidad de ocurrencia de los riesgos de seguridad de la información identificados en la etapa de planificación.
4. **Evaluación de desempeño**: Se establecen las métricas y herramientas con las que se evaluará el SGSI.
5. **Mejoramiento Continuo**: Se implementan las acciones necesarias para mejorar el nivel de madurez del SGSI, la solución y no repetición ante la materialización de riesgos de seguridad de la información.

Ilustración 1. Ciclo del Modelo de Seguridad y Privacidad de la Información



Fuente: Tomado del documento maestro del MSPI

2. OBJETIVO

Establecer el marco para la adopción, implementación, apropiación, gestión y mejora continua del Sistema de Gestión de Seguridad de la Información-SGSI, políticas específicas y lineamientos relacionados con seguridad de la información como complemento a lo definido en la Política General de Seguridad de la Información, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información del Instituto Geográfico Agustín Codazzi.

3. ALCANCE

El Sistema de Gestión de Seguridad de la Información (todos sus componentes), la Política de Seguridad de la Información y el Manual de Seguridad de la Información aplicará a servidores públicos, contratistas y proveedores que accedan a la información, procesos y controles definidos para cumplirlo en Sede Central y Direcciones Territoriales.

4. DESARROLLO

4.1 DIAGNÓSTICO

El autodiagnóstico se realiza semestralmente mediante el "Instrumento de Evaluación SGSI", a través de este instrumento se identifica el nivel de madurez de la seguridad, privacidad, los controles adoptados, así como su nivel de implementación y posibles acciones tendientes a la mejora continua de la seguridad de la información.

Este instrumento mide las diferentes cláusulas y controles establecidos por la Norma ISO 27001, en la cual se basa el Modelo de Seguridad y Privacidad de la Información-MSPI del MINTIC y el Sistema de Gestión de Seguridad de la Información-SGSI del del Instituto Geográfico Agustín Codazzi-IGAC, a continuación, se describen los niveles de madurez del SGSI:

CRITERIOS VALORACIÓN			
NIVEL		**CALIFICACIÓN**	**CRITERIO**
Inexistente	Nivel 0	0	▪ Ausencia de procedimientos documentados y/o formalizados. ▪ Actividades relacionadas con la Seguridad de la Información parcial o totalmente inexistente. ▪ Ausencia de controles. ▪ No se tiene conciencia de los riesgos de Seguridad de la Información.
Definido	Nivel 1	25	▪ Existen algunas iniciativas sobre Seguridad de la Información. ▪ La implementación de los controles depende de cada servidor público o contratista. ▪ No se realiza identificación de activos de información y de riesgos. ▪ Los incidentes de Seguridad de la Información se gestionan de manera reactiva. ▪ La implementación de un control depende de cada servidor público o contratista y es principalmente reactiva. ▪ No existen procedimientos documentados.
Documentado	Nivel 2	50	▪ Se cuenta con documentos (procedimientos, guías, instructivos, entre otros) de Seguridad de la Información y de la Información definidos, aprobados, pero no se implementan siempre. ▪ Se conocen los riesgos de Seguridad de la Información, pero no se gestionan en todo el Instituto. ▪ Se cuenta con recursos para realizar actividades de Seguridad de la Información y de la Información. ▪ La información de Seguridad se comparte en el Instituto de manera informal. ▪ Existen controles que permiten identificar incidentes de seguridad de la información, pero no se gestionan formalmente.
Aplicado	Nivel 4	75	▪ La gestión de Seguridad de la Información y de la Información se actualiza continuamente de acuerdo con la gestión de riesgos, a los cambios en los requisitos del Instituto y los cambios en las amenazas y la tecnología.

CRITERIOS VALORACIÓN			
NIVEL		CALIFICACIÓN	CRITERIO
			▪ Los riesgos de Seguridad de la Información y de la Información se gestionan formalmente en todo el Instituto. ▪ Los documentos (procedimientos, guías, instructivos, entre otros), y controles se aplican casi siempre, en algunos casos no se aplican o implementan oportunamente o la forma de aplicarlo no es la indicada. ▪ Se cuenta con métricas e indicadores que permiten medir la gestión de Seguridad de la Información. ▪ Se realizan auditorías de Seguridad de la Información.
En optimización	Nivel 5	100	▪ Los procesos, procedimientos, demás documentos y controles se monitorean, miden y se aplican oportuna y correctamente de acuerdo a como están documentados. ▪ Las servidores públicos y contratistas poseen el conocimiento y las habilidades para realizar sus roles y responsabilidades asignados en Seguridad de la Información. ▪ Se responde efectivamente a los incidentes de Seguridad de la Información y de la Información.

4.2. PLANIFICACIÓN DEL SGSI

4.2.1. ROLES Y RESPONSABILIDADES

Oficial de Seguridad de la Información o profesional designado por DTIC: Servidor público o contratista que se encarga de liderar la implementación y mantenimiento de las políticas de seguridad de la información en el IGAC. Es responsable de garantizar que se establezcan medidas adecuadas de seguridad de la información y de supervisar la implementación de las políticas, manual y procedimientos de seguridad de la información en toda el Instituto, las responsabilidades asociadas a este rol son:

- Coordinar las actividades para el diseño, implementación, operación, revisión y mejora continua del Sistema de Gestión de Seguridad de la información a desarrollar con todos los procesos del IGAC.
- Apoyar a la Dirección de Tecnologías de la Información y Comunicaciones en la identificación, selección e implementación de los mecanismos, controles y herramientas tecnológicas necesarias para realizar el tratamiento de riesgos de seguridad de la información.
- Revisar las políticas, lineamientos, directivas, circulares, instrucciones, planes, protocolos y toda la documentación relacionada con seguridad de la información.
- Evaluar el desempeño del SGSI periódicamente e informar al Comité Institucional de Gestión y Desempeño o quien haga sus veces del avance en la implementación y estado de madurez del SGSI.
- Coordinar la gestión de cualquier evento o incidente de seguridad de la información y mantener informado al Comité Institucional de Gestión y Desempeño o quien haga sus veces del estado de este.
- Coordinar la ejecución de las actividades establecidas en el plan de uso y apropiación del SGSI.

Comité Institucional de Gestión y Desempeño o quien haga sus veces: Grupo de servidores públicos y/o contratistas responsables de supervisar y evaluar el SGSI del IGAC. Este comité operará con los siguientes miembros:

- Director General.
- Subdirector General.
- Director de Tecnologías de la Información y Comunicaciones.
- Jefe Oficina Asesora de Planeación.
- Jefe Oficina Asesora Jurídica.
- Oficial de Seguridad de la Información o profesional designado por DTIC.

Las responsabilidades asociadas son:

- Asegurar la implementación y desarrollo de planes, programas, políticas de gestión y directrices en materia de seguridad de la información, así como aprobar estas, supervisar su implementación, sus procedimientos, y aprobar cambios y mejoras en el SGSI del IGAC.
- Brindar acompañamiento e impulsar el desarrollo de proyectos asociados al plan de implementación del Sistema de Gestión de Seguridad de la Información, facilitando o gestionando los recursos humanos, técnicos y financieros necesarios a nivel institucional.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos relacionados con la seguridad de la información.
- Revisar, analizar y ejecutar las acciones que considere adecuadas frente a los incidentes de seguridad que se materialicen en el manejo de la información.

Este comité podrá operar como subcomité de uno existente, siempre y cuando mantenga los miembros descritos.

Usuarios: Todos los servidores públicos, contratistas y personal de proveedores del IGAC que manejan, procesan o tienen acceso a información del Instituto, las responsabilidades asociadas son:

- Cumplir con las políticas, lineamientos y procedimientos establecidos en la Política General de Seguridad de la Información, Manual de Seguridad de la Información del IGAC y en cualquier otro documento relacionado con seguridad de la información.
- Informar cualquier evento o incidente de seguridad que pueda afectar al Instituto.
- Usar los activos de información únicamente para el desarrollo de sus funciones u obligaciones, implementando las medidas de seguridad adecuadas.
- Conocer, apropiar y dar cumplimiento a las directrices, políticas, procedimientos y demás lineamientos de seguridad de la información del Instituto.
- Participar activamente en las campañas de sensibilización, entrenamientos y las capacitaciones en seguridad información, así como atender las recomendaciones, tips, comunicadas.

Responsable del SGI: Servidor público o contratista encargado de gestionar el Sistema de Gestión Integrado del Instituto, en el cual se incluye la gestión de seguridad de la información. Es responsable de garantizar que se establezcan medidas adecuadas de seguridad de la información en los procesos relacionados con el sistema de gestión integrado, y de supervisar la implementación de las políticas y procedimientos de seguridad de la información en su respectivo ámbito.

Auditor Interno del SGSI: Servidor público o contratista encargado de realizar auditorías internas en el SGSI del IGAC, con el fin de evaluar la efectividad de las políticas y procedimientos de seguridad de la información en el Instituto, las responsabilidades asociadas son:

- Planear, establecer e implementar el programa de auditorías para el SGSI.
- Informar al Comité Institucional de Gestión y Desempeño o quien haga sus veces los resultados de las auditorías.
- Conservar la información documentada como evidencia de la realización de las auditorias de acuerdo con el programa de auditorías.

Director(a) DTIC: encargado de gestionar los sistemas de información utilizados por el IGAC, así como de liderar y supervisar el Sistema de Gestión de Seguridad de la Información-SGSI en el Instituto. El Director(a) de Tecnologías de la Información y Comunicaciones tiene la responsabilidad de garantizar que se establezcan medidas adecuadas de seguridad de la información en los sistemas de información del IGAC, de supervisar la implementación de las políticas y procedimientos de seguridad de la información en los sistemas de información y servicios tecnológicos, y de asegurar el correcto funcionamiento y la mejora continua del SGSI. Como responsable del SGSI, este rol también implica la coordinación con otros responsables de procesos y subprocesos del Instituto, para garantizar la

alineación de las prácticas de seguridad y la adopción de las políticas y procedimientos establecidos en el marco del SGSI.

Subdirección de Información: el Subdirector y equipo de trabajo asociado se encargarán de:
- Aplicar los componentes de seguridad en la Interoperabilidad.
- Establecer el modelo de datos.
- Identificar y clasificar los activos de información del Instituto.
- Identificar y valorar los riesgos de seguridad de la información del Instituto.

Subdirección de Sistemas de Información: el Subdirector y equipo de trabajo asociado se encargarán de:
- Aplicar los estándares y buenas prácticas en el desarrollo de software.
- Validar los requerimientos de seguridad de la información para nuevos desarrollos.
- Atender las recomendaciones del Oficial de Seguridad de la Información o profesional designado de la DTIC relacionados con el ciclo de vida de desarrollo de software.
- Realizar las remediaciones de las vulnerabilidades y brechas encontradas en el ciclo de vida de desarrollo.

Subdirección de Infraestructura Tecnológica: el Subdirector y equipo de trabajo se encargarán de:
- Administrar y gestionar las herramientas de seguridad y realizar la generación de reportes que permitan identificar oportunidades de mejora.
- Desarrollar las etapas de análisis, pruebas, implementación y revisión de parches de seguridad de las distintas plataformas tecnológicas del IGAC.
- Implementación de los controles sobre la infraestructura tecnológica o servicios administrados por la DTIC de acuerdo con las políticas, lineamientos y directrices establecidos para fortalecer la seguridad de la información.

Mesa de Servicio de TI: equipo de trabajo que se encargará de:
- Informar posibles incidentes o eventos de seguridad de la información al Oficial de Seguridad de la Información.
- Divulgar y recordar a los usuarios las buenas prácticas y controles de seguridad que deben tener en cuenta para la debida protección de la información del Instituto.
- Conocer, apropiar y dar cumplimiento a las directrices, políticas, procedimientos y demás lineamientos de seguridad de la información del Instituto.

En cuanto a las responsabilidades para la implementación de las políticas específicas de Seguridad de la Información se describen (4) cuatro tipos de responsables:
1. **Implementación:** Se refiere a los procesos, subprocesos, dependencias y servidores públicos que se encargarán de poner en práctica cada lineamiento definido.
2. **Apoyo en la implementación**: Se refiere a los procesos, subprocesos, dependencias, servidores públicos o contratistas que apoyarán al responsable en la implementación de los lineamientos.
3. **Cumplimiento:** Se refiere a los servidores públicos contratistas o proveedores que deben cumplir los lineamientos, procedimientos o instructivos definidos por los implementadores o apoyos a la implementación.
4. **Acompañamiento y Orientación**: Se refiere a las dependencias u Oficina de Control Interno, Oficina de Control Interno Disciplinario, auditoría interna o quien haga sus veces las cuales brindan un nivel de asesoría proactivo y estratégico que vaya más allá de la ejecución eficiente y eficaz del Plan Anual de Auditorías.

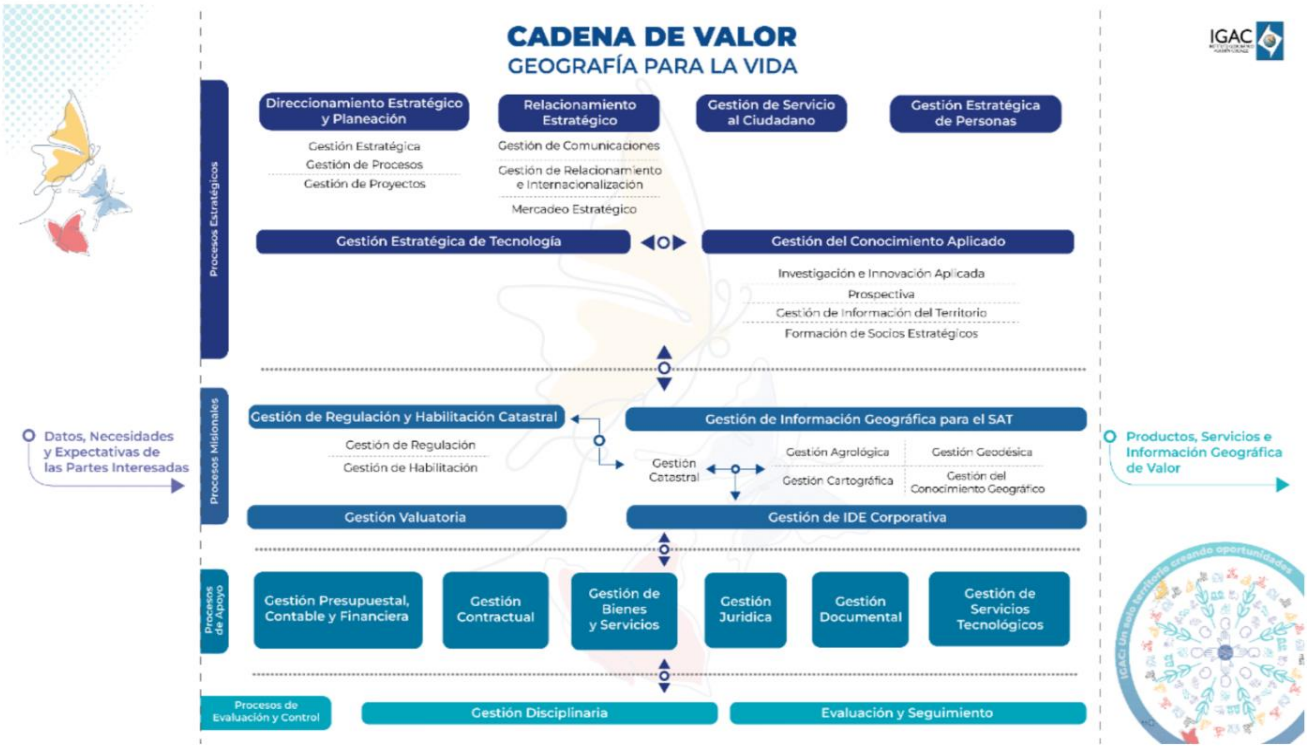
4.2.2. CONTEXTO

Conocer del Instituto, su contexto interno y externo, misión, objetivos estratégicos y elementos relevantes que podrían influir en la implementación del Sistema de Gestión de Seguridad de la Información.

El contexto del Instituto Geográfico Agustín Codazzi está determinado en el Plan Estratégico Institucional 2022-2026 "Geografía para la vida" especialmente en el desarrollo del *Anexo 1. Herramienta Administración Estratégica del Plan Estratégico Institucional* donde se analizan factores externos, políticos, económicos, sociales, tecnológicos, ecológicos (ambientales) y legales, en el entorno competitivo de cara a la competencia, ciudadanos, partes interesadas y proveedores, y las debilidades, oportunidades, fortalezas y amenazas para conocer las características internas y los riesgos externos a los que se puede estar enfrentado el Instituto.

Propósito Central: Es la autoridad geográfica y catastral del país, esto quiere decir que somos los encargados de regular y ejecutar acciones geográficas, cartográficas, agrológicas, geodésicas y catastrales para el desarrollo de nuestros territorios.

Mapa de Procesos: esquema que permite la identificación de los 18 procesos con sus respectivos subprocesos del instituto.



4.2.3. LIDERAZGO Y COMPROMISO

El Instituto Geográfico Agustín Codazzi-IGAC estableció el Comité Institucional de Gestión y Desempeño o quien haga sus veces formado por miembros de la Alta Dirección, para revisar, aprobar, hacer seguimiento y apoyar la implementación del SGSI, liderando desde cada función la apropiación del Sistema de Gestión de Seguridad de la Información y proveyendo los recursos necesarios para su funcionamiento.

4.2.4. SOPORTE

- **Recursos:** El IGAC deberá destinar dentro del presupuesto anual los recursos económicos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI. Dicho presupuesto deberá estar reflejado dentro del Plan Anual de Adquisiciones, así mismo se deberá contar con el recurso humano necesario y capacitado para liderar, implementar y gestionar las estrategias que propendan con la protección del Instituto.

  Por otra parte, se requiere contar de manera constante con los recursos necesarios para la implementación de controles lógicos y físicos que se necesiten para garantizar la confidencialidad, integridad y disponibilidad de la información del Instituto.

- **Competencia:** El Instituto debe contar con personal calificado para implementar el Sistema de Gestión de Seguridad de la Información-SGSI, considerando su formación y experiencia adecuada.

- **Toma de conciencia:** El IGAC, mediante la Dirección de Tecnologías de la Información y las Comunicaciones, formula periódicamente un plan de uso y apropiación, para fortalecer los conocimientos sobre seguridad de la información para servidores públicos, contratistas y proveedores, para mitigar riesgos asociados a la información del Instituto.

  La Política General de Seguridad de la información es el documento principal en materia de seguridad de la información y debe ser conocido y aplicado por los usuarios, socializado por los canales internos y externos de comunicación del Instituto.

- **Comunicación:** Los lineamientos definidos en el marco de la seguridad de la información serán comunicados de manera oportuna a los servidores públicos, contratistas y proveedores que tengan acceso a la información institucional, con el fin de mantener una comunicación permanente y que estos estén enterados de la implementación o mejora de los controles establecidos para la protección de la información.

- **Información documentada:** El SGSI del IGAC tiene políticas, manuales, procedimientos, guías, instructivos y formatos necesarios para la documentación que requiere el sistema basado en buenas prácticas, normas internacionales, para que esté disponible y pueda ser consultada por cada miembro del Instituto.

  La documentación asociada al SGSI cuenta con un proceso de mejora continua y es actualizada de acuerdo con las necesidades que tenga el Instituto, cambios en la normativa vigente y cambios en los requisitos técnicos en la NTC ISO 2700:2022. Adicionalmente, está se encuentra respaldada y controlada, siguiendo los lineamientos del Sistema de Gestión de Calidad del Instituto.

4.2.5 EVALUACIÓN DEL DESEMPEÑO DEL SGSI

El seguimiento, medición, análisis y evaluación se realiza para comprobar la efectividad, eficiencia y eficacia de los controles, el tratamiento de riesgos, el plan operacional, la gestión de incidentes y la medición del objetivo de seguridad de la Información; brindando un soporte para el sostenimiento y optimización del Sistema de Gestión de Seguridad de la Información.

El desarrollo del seguimiento y medición se realiza mediante:

- **Indicador del Sistema de Gestión de Seguridad de la Información**: Con el fin de realizar el seguimiento al SGSI se establece un único indicador que permite medir el grado de avance de implantación.

- **Revisiones:** Las revisiones internas y externas buscan identificar oportunidades de mejora en la gestión de la seguridad de la información, dichas revisiones se realizan mediante:
  - Auditorías internas.
  - Revisiones técnicas.
  - Auditorías Externas.
  - Evaluación FURAG.
  - Evaluación implementación PESI.
  - Autodiagnóstico.

4.2.6 INVENTARIO DE ACTIVOS DE INFORMACIÓN E INFRAESTRUCTURA CRÍTICA

El IGAC realiza el inventario de los activos de información e infraestructura crítica con el fin de determinar los activos que intervienen en el tratamiento de la información, establecer los propietarios y custodios de estos, así como realizar la valoración respecto a la confidencialidad, integridad y disponibilidad.

El inventario y clasificación de activos se elabora de acuerdo con el procedimiento Gestión de Activos de Información código PC-GET-01, este se debe actualizar por lo menos una vez al año.

El proceso de Gestión Documental y la Subdirección de Infraestructura Tecnológica, con el apoyo del Oficial de Seguridad de la Información o profesional designado de la DTIC deberán establecer un sistema de etiquetado y control de acceso para la información clasificada, a fin de garantizar que solo las personas autorizadas tengan acceso a la misma y que se cumplan los controles y procedimientos establecidos.

4.2.7 VALORACIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión de riesgos de seguridad de la información permite identificar, analizar y valorar los riesgos mitigando la materialización de estos y disminuyendo el impacto sobre los procesos, así como determinar el tratamiento y aceptación de los riesgos residuales. La gestión de riesgos es continua y debe realizarse el proceso de valoración por lo menos una vez al año.

La gestión de riesgos de seguridad es coordinada por la Dirección de Tecnologías de la Información y Comunicaciones de acuerdo con lo establecido en la Política Administración del Riesgo, vigente.

4.3 LINEAMIENTOS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD

El IGAC define las políticas específicas con el fin de documentar cada uno de los controles físicos y lógicos que se requieren para la protección de la información y son de obligatorio cumplimiento por parte de los servidores públicos, contratistas, visitantes, proveedores y terceros. Adicionalmente están clasificadas en diferentes temáticas, teniendo en cuenta el contexto interno y externo del Instituto:

4.3.1 PERSONAS

Objetivo: Definir lineamientos para el manejo de la seguridad de la información de los servidores públicos y contratistas en términos y condiciones de la vinculación, ejecución del contrato y retiro del Instituto (antes, durante y después), sensibilizándolos en temas de seguridad de la información.

1. Previo la vinculación de contratistas, la dependencia del Instituto que demande la contratación deberá implementar controles que permitan validar la idoneidad del aspirante y la verificación de antecedentes ajustados a la normativa vigente. Para el caso de vinculación de nuevos funcionarios la Subdirección de Talento Humano deberá realizar el proceso de validación de la idoneidad y verificación de antecedentes ajustados a la normativa y procedimientos vigentes.

2. El proceso de ingreso al Instituto, aplicable para servidores públicos y contratistas deberá incluir la autorización para el tratamiento de los datos personales de acuerdo con lo definido por la Política de Protección de Datos personales del IGAC y la Ley 1581 junto con sus decretos reglamentarios.
3. La Subdirección de Talento Humano, GIT de Gestión Contractual y las Direcciones Territoriales establecen los mecanismos y controles necesarios para la protección de la información aportada por parte del aspirante al cargo o a suscribir un contrato de prestación de servicios con el IGAC.
4. El Oficial de Seguridad de la Información o profesional designado de la DTIC, realizará jornadas o actividades de inducción, socialización y sensibilización en temas relacionados con seguridad de la información, por medio de los canales de comunicación institucionales establecidos en coordinación con la Subdirección de Talento Humano.
5. En los estudios previos, pliego de condiciones o contratos, el GIT de Gestión Contractual y las Direcciones Territoriales deben incluir entre las obligaciones generales del contratista el cumplimiento de los lineamientos de seguridad de la información del IGAC.
6. La Subdirección de Talento Humano deberán hacer suscribir a los servidores públicos que se vinculen con el Instituto, un acuerdo de confidencialidad de la información, como control preventivo con el fin de mitigar riesgos asociados a la fuga de la información Institucional calificada como pública clasificada o pública reservada.
7. Formalizado el procedimiento de ingreso al Instituto, el jefe inmediato o supervisor de contrato debe solicitar el requerimiento en la herramienta de gestión de la Mesa de Servicio de TI solicitando la creación de cuenta de dominio, y demás servicios que requiera el usuario para la ejecución de sus funciones u obligaciones contractuales.
8. Es responsabilidad de los servidores públicos y contratistas participar de forma activa en los espacios de socialización y actividades de temas asociados a la seguridad de la información.
9. El incumplimiento a los lineamientos de seguridad de la información que ponga en riesgo la información del IGAC será atendido como un incidente de seguridad de la información y puede provocar el inicio de acciones legales, las cuales se enmarcaran de conformidad con lo definido en la Ley. La Oficina de Control Interno Disciplinario regirá para los casos que se presenten con servidores públicos, y la Oficina Asesora Jurídica para los casos que se presenten de contratistas.
10. Cuando un funcionario o contratista cese en sus funciones o culmine su contrato el jefe inmediato o supervisor de contrato o quien haga sus veces será el encargado de velar por que la información que tenía a su cargo se encuentre almacenada en los repositorios oficiales del área.
11. Al finalizar su vinculación el servidor de público y contratista deberá realizar la entrega del carnet a la Subdirección de Talento de Humano y realizar la entrega del inventario asignado al proceso de Gestión de Bienes y Servicios.
12. Al momento de la solicitud de paz y salvo por parte de los servidores públicos y contratistas a la Dirección de Tecnologías de la Información y las Comunicaciones, los accesos a sistemas de información, herramientas de colaboración entre otros serán desactivados de manera inmediata por parte de la Subdirección de Infraestructura Tecnológica. Es responsabilidad del jefe inmediato o supervisor del contrato la desactivación de las credenciales de acceso de Sistemas de Información o aplicativos no administrados por la DTIC o externos.
13. Las novedades administrativas de los servidores públicos incluyendo traslados entre dependencias o suspensiones que superen los 10 días, deben ser reportadas por el superior jerárquico de manera inmediata a la Subdirección de Infraestructura Tecnológica a través de la herramienta de Mesa de Servicios, con el fin que se suspendan o reasignen los accesos a los sistemas de información o plataformas tecnológicas que administra la DITC. En caso de suspensión de un contrato de prestación de servicios personales que supere 10 días deberá ser reportada por el supervisor en la misma forma indicada para los fines pertinentes.

Responsables:

- Subdirección de Talento Humano (Implementación)
- GIT de Gestión Contractual (Implementación)
- Direcciones Territoriales (Implementación)

- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Oficina de Control Interno Disciplinario (Apoyo en la implementación)
- Oficina Asesora Jurídica (Apoyo en la implementación)
- Subdirección de Infraestructura Tecnológica (Apoyo en la implementación)
- Servidores públicos y contratistas (Cumplimiento)

4.3.2 USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN

Objetivo: Establecer lineamientos claros para el uso adecuado de los recursos de información del IGAC, asegurando que los servidores públicos, contratistas y proveedores que tengan acceso a la información institucional los utilicen de manera responsable, cumpliendo con las normas de seguridad, ética y legalidad.

1. Los recursos de información del IGAC solo pueden ser utilizados para fines autorizados relacionados con el desarrollo de actividades laborales y los objetivos del Instituto. Queda estrictamente prohibido el uso de los recursos para actividades personales o cualquier actividad que viole la ley, las políticas del Instituto, los derechos de terceros.
2. Los servidores públicos, contratistas y proveedores que tengan acceso a la información institucional, deben cumplir con todas las leyes, regulaciones y normas éticas aplicables en el uso de los recursos. Esto incluye el respeto a los derechos de autor, la privacidad de los datos, la confidencialidad de la información sensible y la prohibición de difamación, acoso, discriminación u otras conductas inapropiadas.
3. Los servidores públicos, contratistas y proveedores que tengan acceso a la información institucional deben respetar la privacidad de la información del IGAC y no divulgar información confidencial o sensible a terceros no autorizados. Se deben seguir los lineamientos y procedimientos establecidos para el manejo y protección de la información confidencial. Todos los servidores públicos deben firmar el acuerdo de confidencialidad del IGAC.
4. El IGAC se reserva el derecho de monitorear y auditar el uso de los recursos de información para asegurar el cumplimiento de esta política y para garantizar la seguridad de la información. Los usuarios deben estar conscientes de que el uso de los recursos puede ser monitoreado y registrado.
5. No se deben reutilizar documentos para impresión con datos personales, semiprivados, privados o sensibles o documentos catalogados como pública reservada o publica clasificada.
6. No se debe dejar desatendidos y sin ningún control de acceso documentos físicos, medios de almacenamiento externo (USB, discos duros, SD Card, CD, DVD, entre otros), Tokens y otros activos de información en los puestos de trabajo, oficinas, salas de reuniones o lugares de acceso público.

Responsables:

- Subdirección de Infraestructura Tecnológica (Implementación)
- Subdirección de Sistemas de Información (Implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores públicos y contratistas (Cumplimiento)

4.3.3 GESTIÓN DE SEGURIDAD FÍSICA

Objetivo: Garantizar el aseguramiento físico de los activos de información del IGAC, aplicando controles de seguridad en el espacio físico, para mitigar riesgos asociados por accesos no autorizados.

1. Todas las áreas determinadas como "Áreas Seguras" son de acceso restringido y deben cumplir con el instructivo de trabajo en áreas seguras, teniendo controles de acceso, y registrando todas las actividades realizadas en estas.

2. Las áreas que se hayan definido como seguras y los activos de información que la componen, estarán protegidas del acceso no autorizado mediante controles físicos de acceso y tecnologías de autenticación fuerte (por ejemplo: token, tarjetas de proximidad, o, controles biométricos).
3. En las áreas seguras donde se encuentren activos informáticos y de archivo documental, se debe cumplir como mínimo con los siguientes lineamientos:
    a. No consumir alimentos ni bebidas.
    b. No ingresar sustancias inflamables.
    c. No permitir el acceso de personal ajeno al Instituto.
    d. No se deben almacenar elementos ajenos a los requeridos de acuerdo con la actividad que se realice en el área segura.
    e. No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del responsable de dichas áreas.
    f. No se permite el ingreso de equipos electrónicos (computadores portátiles, cámaras, tabletas, celulares, USB, etc.), así como maletas o contenedores; excepto cuando exista debida justificación y autorización para portarlos. En este último caso, deberán ser registradas al ingreso y salida para mitigar el riesgo de ingreso de elementos no autorizados o la extracción de elementos.
4. Debe contar con un sistema de video vigilancia que permita el monitoreo y registro de ingreso y actividades realizadas en estas.
5. Para la selección e implementación de controles de seguridad para las áreas físicas de las sedes del IGAC se tendrá en cuenta la posibilidad de daños producidos por incendio, inundación, explosión, agitación civil; otras formas de fenómenos naturales como terremotos, ciclones y erupciones volcánicas, inundaciones; y situaciones producidas intencionalmente o resultantes de fallas humanas como incendios, explosiones, actos terroristas, robo, espionaje, infiltración o ataques contra el Instituto.
6. Para las áreas de almacenamiento de documentación física se tendrá en cuenta lo dispuesto en el Acuerdo 50 de 2000 sobre "Prevención de deterioro de los documentos de archivo y situaciones de riesgo" y el Acuerdo 06 de 2014 sobre "Conservación de Documentos" del Archivo General de la Nación; con base a lo anterior el Instituto propenderá por la implementación de los siguientes controles:
    a. Detectores automáticos de humo o de calor conectados con servicios exteriores de urgencia.
    b. Personal de vigilancia.
    c. Sistemas de extinción escogidos con la asesoría de los bomberos: extinguidores manuales, sistemas de extinción fijos.
    d. Puertas cortafuego y dámper motorizado.
    e. Realizar programas regulares de mantenimiento de las instalaciones eléctricas y asegurarse que las salidas de emergencia sean de fácil acceso y de apertura desde el interior.
    f. Es necesario hacer respetar las medidas restrictivas hacia los fumadores, aislar los productos sensibles como películas de nitrato o productos químicos inflamables y evitar las fotocopias en salas de almacenamiento o en espacios que tengan material inflamable.
    g. La protección contra los efectos del agua incluirá la verificación constante de los sistemas hidráulicos como canales, goteras, terrazas, ventanas, etc. Hay que asegurar el mantenimiento de las canalizaciones y evitar las redes de evacuación o suministro de agua en las placas de las salas de almacenamiento. Prever un pozo o un sistema de evacuación de aguas para las salas subterráneas.
7. Las puertas que utilicen el sistema de control de acceso donde se procese o almacene activos de información deben permanecer cerradas, y es responsabilidad de todos los servidores públicos, contratistas y terceros autorizados, evitar que las puertas permanezcan abiertas.
8. Las personas que ingresen o salgan de las instalaciones del IGAC, independientemente de su tipo de vinculación con el IGAC servidor público, contratista, visitantes, deben registrar en la bitácora de vigilancia, el ingreso y salida de los dispositivos tecnológicos personales (portátiles, tablets,

cámaras de video o fotografía, entre otros), para los institucionales debe realizarlo bajo lineamientos establecidos y formato de Salida de bienes del instituto código FO-INV-PC03-03 V1 de la Gestión de Bienes y Servicios.
9. Los visitantes deberán permanecer acompañados de un funcionario o contratista del IGAC, cuando se encuentren dentro de alguna de las áreas seguras o restringidas del Instituto.
10. Los servidores públicos y contratistas deben portar el carné del Instituto en un lugar visible mientras se encuentren en la instalación del IGAC.
11. Los visitantes que se encuentren en las instalaciones del IGAC deberán estar debidamente identificados.

Responsables:
- Subdirección Administrativa y Financiera (Implementación)
- Grupo Interno de Trabajo de Gestión Documental (Implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Subdirección de Infraestructura Tecnológica (Implementación)
- Servidores públicos y contratistas (Cumplimiento)

4.3.4 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Mitigar afectaciones en la integridad, disponibilidad y confidencialidad de la información a través de la identificación, tratamiento y gestión oportuna de los riesgos de seguridad de la información.

1. Los servidores públicos y contratistas del Instituto deberán reportar de manera oportuna y con carácter obligatorio, los riesgos de seguridad de la información identificados por medio de la herramienta de gestión de la Mesa de Servicio de TI como un evento de seguridad.
2. Los líderes de los procesos deberán documentar los resultados de la evaluación de riesgos y los planes de tratamiento de los riesgos de seguridad de la información existentes en el Instituto
3. El IGAC propende por la implementación de controles tanto físicos como lógicos, orientados a minimizar la probabilidad de que un riesgo de seguridad de la información se materialice.
4. Se realizarán campañas de socialización y comunicación de la Metodología de Gestión de Riesgos de Seguridad de la Información, para su debida implementación.
5. Se hará seguimiento a la gestión de riesgos y ejecución de los planes de acción definidos dentro de la misma, revisando periódicamente la variación de la calificación de los riesgos.
6. La frecuencia y condiciones para la realización de las Gestiones de Riesgo son las especificadas en la Metodología Gestión de Riesgos de seguridad de la información.
7. La Dirección de Tecnologías de la Información y las Comunicaciones, junto con sus Subdirecciones, realiza análisis de vulnerabilidades y pruebas de seguridad orientadas a los Sistemas de Información, Infraestructura y servicios tecnológicos, así como pruebas de ingeniería social a servidores públicos, contratistas y proveedores con acceso a información institucional, con el fin de establecer brechas que puedan llegar a materializar riesgos de seguridad de la información.
8. La DTIC, por medio de la Subdirección de Infraestructura Tecnológica, administra y monitorea proactiva y preventivamente los entornos digitales, con el fin de proteger y asegurar los sistemas de información críticos, herramientas, accesos lógicos, hardware y software dispuestos para la operación segura del Instituto, mitigando las vulnerabilidades o debilidades identificadas.

Responsables
- Dirección de Tecnologías de la Información y Comunicaciones (Implementación)
- Subdirección de Infraestructura Tecnológica (Implementación)
- Subdirección de Sistemas de Información (Implementación)
- Subdirección de Información (Implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)

- Líderes de proceso (Implementación)
- Oficina Asesora de Planeación (Implementación)
- Direcciones Territoriales (Implementación)
- Servidores Públicos y contratistas (Cumplimiento)

4.3.5 GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Establecer los procedimientos y lineamientos necesarios para la gestión efectiva de los incidentes de seguridad de la información en el IGAC. Esta política tiene como objetivo garantizar una respuesta adecuada y oportuna frente a cualquier incidente que pueda comprometer la confidencialidad, integridad o disponibilidad de la información.

1. Todos los servidores públicos, contratistas y proveedores que tengan acceso a la información Institucional, deben reportar los eventos o incidentes por medio de los mecanismos y lineamientos establecidos en el procedimiento vigente de Gestión de Incidentes de Seguridad de la Información que detecten. La notificación deberá ser rápida y precisa, brindando información relevante sobre la naturaleza del incidente y su impacto potencial.
2. Para todos los incidentes de seguridad de la información se debe realizar un análisis exhaustivo para evaluar su gravedad, alcance y posibles causas, de acuerdo con lo definido en el procedimiento vigente de Gestión de Incidentes de Seguridad de la Información. Esto incluirá la recopilación y preservación de evidencia, así como la participación de expertos en seguridad de la información en caso de ser necesario. El análisis permitirá comprender la naturaleza del incidente y determinar las acciones adecuadas a tomar.
3. Se debe ejecutar una atención apropiada y proporcionada al incidente de acuerdo con los tiempos establecidos en el procedimiento de gestión de incidentes. Esto puede incluir la mitigación de la amenaza, la restauración de los sistemas afectados, la implementación de medidas correctivas y la comunicación con las partes interesadas pertinentes. Se asignarán responsabilidades claras a los equipos involucrados en la respuesta al incidente, asegurando una coordinación efectiva y un enfoque colaborativo.
4. Se debe hacer una revisión de las matrices de riesgo de seguridad de la información de los procesos impactados para verificar si el riesgo materializado en el incidente debe ajustarse en cuanto a su evaluación o no identificado.
5. Se debe realizar seguimiento y monitoreo de los incidentes, para evaluar la efectividad de las medidas tomadas, identificar lecciones aprendidas y realizar mejoras continuas en los controles y procedimientos de seguridad de la información.
6. La DTIC realiza actividades para la generación de cultura, toma de conciencia y capacitación en seguridad de la información, con el fin de establecer una cultura de seguridad y respuesta efectiva frente a los incidentes.
7. Se mantendrá el registro de lecciones aprendidas de los incidentes de seguridad de la información, que sirva de insumo para el tratamiento adecuado y oportuno de nuevos incidentes de seguridad de la información.
8. La Subdirección de Infraestructura Tecnológica implementará las herramientas tecnológicas necesarias para monitorear y prevenir la ocurrencia de incidentes de seguridad de la información.
9. La DTIC y el Oficial de Seguridad de la Información, deben mantener contacto con grupos de interés especiales como MINTIC, COLCERT, CSIRT entre otros, los cuales le permitan tener conocimiento sobre las mejores prácticas y mantenerse actualizado con la información de seguridad relevante, que ayude a prevenir incidentes de seguridad.
10. La DTIC, podrá solicitar apoyo de entidades externas y/o proveedores para la aplicación de medidas de contención y recuperación de los activos de información afectados, previa evaluación y/o análisis del incidente.

Responsables

- Dirección de Tecnologías de la Información y Comunicaciones (Implementación)

- Subdirección de Infraestructura Tecnológica (Implementación)
- Subdirección Administrativa y Financiera (Implementación)
- GIT de Gestión Documental (Implementación)
- Subdirección de Información (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores públicos y contratistas (Cumplimiento)

4.3.6 CULTURA INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN

Objetivo: Generar conocimiento, apropiación e implementación de prácticas de Seguridad de la Información por parte de los servidores públicos, contratistas y proveedores que tengan acceso a la información institucional, con el fin de establecer una cultura de seguridad y respuesta efectiva frente a la prevención de incidentes de seguridad de la información.

1. El IGAC desarrollará estrategias para sensibilizar de manera permanente a los servidores públicos, contratistas y proveedores que tengan acceso a la información institucional en temas de seguridad de la información.
2. La Dirección de Tecnologías de la Información y Comunicaciones y el Oficial de Seguridad de la Información, diseñarán y desarrollarán anualmente el Plan de Uso y Apropiación donde se establezcan los temas que se deben comunicar, los temas de sensibilización, los responsables, herramientas, público objetivo y el cronograma para la ejecución de estas actividades, con el fin de realizar la divulgación de los lineamientos, procesos, políticas, procedimientos y controles que se establezcan y el fomento del comportamiento responsable y seguro en los entornos digitales.
3. Los servidores públicos y contratistas deberán participar activamente en las jornadas de sensibilización y capacitación orientadas al fortalecimiento de la seguridad de la información, con el fin de mantenerse informado y fortalecer los conocimientos y habilidades para responder ante posibles riesgos y amenazas digitales.
4. La DTIC monitoreará el conocimiento y conciencia sobre las prácticas de seguridad de la información de servidores públicos, contratistas o terceros; para identificar los aspectos a reforzar con el objetivo de evitar vulnerabilidades derivadas de la gestión del personal.
5. El Oficial de Seguridad de la Información o profesional designado comunicará de forma oportuna y eficiente la emisión de políticas, protocolos, metodologías, manuales y procedimientos definidos para garantizar la seguridad de la información del Instituto de la Entidad.
6. La DTIC mediante el Oficial de Seguridad de la Información o profesional designado de la DTIC y apoyado por la Subdirección de Talento Humano y el GIT de Gestión Contractual realizará campañas para socializar, sensibilizar e implementar políticas, protocolos, metodologías, manuales y procedimientos definidos para garantizar la seguridad de la información; dirigidas a servidores públicos, contratistas o proveedores que acceden a la información del Instituto.
7. Los eventos o incidentes de seguridad de la información que tengan como causa el descuido, las malas prácticas, el no acatamiento de las políticas, o recomendaciones socializadas en las actividades establecidas en el Plan de uso y apropiación de Seguridad de la Información por parte de servidores públicos, contratistas o proveedores que tengan acceso a la información institucional, los harán responsables de los posibles incidentes de seguridad de la información que se puedan presentar.
8. Los servidores públicos, contratistas y personal de proveedores deben participar en las actividades establecidas en el Plan de Sensibilización y Concientización de Seguridad de la Información, para mantenerse informado y fortalecer los conocimientos y habilidades para responder ante posibles amenazas digitales.

Responsables

- Dirección de Tecnologías de la Información y Comunicaciones (Implementación)
- Oficial de seguridad de la información o profesional designado de la DTIC (Implementación)

- Subdirección de Talento Humano (Apoyo en la implementación)
- Oficina Asesora de Planeación (Apoyo en la implementación)
- Oficina Asesora de Comunicaciones (Apoyo en la implementación)
- Servidores Públicos y contratistas (Cumplimiento)

4.3.7 GESTIÓN DE PROVEEDORES

Objetivo: Establecer los lineamientos y las responsabilidades para la selección, contratación, supervisión de contratos, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información del IGAC en todo momento. Se busca asegurar que los proveedores cumplan con los requisitos de seguridad de la información y mantengan un alto nivel de protección en el manejo de los activos de información del IGAC.

1. Dentro de los acuerdos, contratos o convenios firmados entre el IGAC y los proveedores se deben definir claramente los requerimientos de seguridad de la información, protección digital y establecer un compromiso de confidencialidad respecto a la información producida dentro de la ejecución de los contratos que haya sido determinada o calificada como información reservada o clasificada de conformidad con la Constitución o la Ley.
2. La Dirección de Tecnologías de la Información y Comunicaciones es responsable de incluir en los contratos que tiene bajo su responsabilidad, condiciones en las cuales se establezcan y acuerden los requisitos de seguridad de protección y seguridad de la información relacionadas con el bien o servicio a contratar y de igual forma garantizar el cumplimiento de los acuerdos de nivel de servicio-ANS, requeridos.
3. Para dar acceso a los activos de información del Instituto a un proveedor, se debe considerar la clasificación a la que se concederá el permiso, administración, uso o tratamiento para establecer los controles de seguridad apropiados; esto, previo a la verificación de la suscripción del contrato suscrito con el Instituto que contenga el Compromiso de Confidencialidad y demás requisitos de la Política General de Seguridad de la Información.
4. Los proveedores deben conocer y cumplir las políticas, procedimientos, lineamientos y demás directrices relacionadas a la protección y seguridad de la información del IGAC que sea inherente a la actividad que va a realizar.
5. El proveedor se obliga a exigir a sus empleados, proveedores y/o subcontratistas relacionados con el proceso de contratación, el cumplimiento irrestricto del compromiso de confidencialidad adquirido con el Instituto en virtud de este Contrato (Cuando aplique).
6. La Subdirección de Infraestructura Tecnológica podrá realizar pruebas de análisis de vulnerabilidades o Ethical Hacking, en los casos que aplique, a los activos de información administrados y/o suministrados al Instituto por terceros.
7. El o los proveedores deben suministrar la información solicitada por el Instituto en los términos y condiciones que la entidad requiera sin que se pueda oponer reserva o confidencialidad alguna tratándose de información del Instituto o asociado a la ejecución de sus actividades contractuales.
8. En el marco del desarrollo contractual, el proveedor debe apoyar o desarrollar las actividades de remediación de vulnerabilidades o de tratamientos de riesgos asociados a los activos de información que administra o provee al Instituto, de acuerdo con las alertas o resultados de ejercicio de Ethical Hacking desarrollados por el Instituto.
9. Cuando haya cambio de proveedor o de tecnología suministrada por el proveedor se debe garantizar la devolución de la información y se debe aplicar el borrado seguro de la información, para garantizar que no haya fuga de esta.

Responsables:

- Subdirección de Infraestructura Tecnológica (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)

° Proveedores y terceros (Cumplimiento)

4.3.8 PROTECCIÓN PARA EL INTERCAMBIO Y ACCESO A LA INFORMACIÓN

Objetivo: Establecer las acciones, procedimientos y controles necesarios para garantizar una transferencia segura de la información en el IGAC, minimizando los riesgos asociados a la pérdida, divulgación o alteración no autorizada de la misma. Además, busca asegurar que la información transferida llegue a su destino de manera íntegra y confidencial.

1. La Subdirección de Información, con el Oficial de Seguridad de la Información o profesional designado de la DTIC establece los estándares, lineamientos, controles y mecanismos para llevar a cabo el intercambio o acceso seguro de información a nivel interno y externo, y/o las condiciones de traslado y de reserva de la información de acuerdo con lo que la legislación vigente permita. El intercambio deberá garantizar que la información no tendrá un uso diferente al gestionado.
2. La Subdirección de Infraestructura Tecnológica, diseña e implementa los controles necesarios para proteger el intercambio o acceso de información a través de los servicios digitales contra interceptación, copiado, modificación, enrutado y destrucción.
3. La Subdirección de Infraestructura Tecnológica, establece las herramientas para el uso de técnicas criptográficas, canales de comunicación, servidores físicos y virtuales, sistemas de información, dispositivos de almacenamiento externos, entre otros.
4. Los acuerdos de intercambio o acceso de información que sean gestionados por los diferentes procesos o subprocesos del IGAC, deberán incorporar un anexo técnico que establezca la información a intercambiar, mecanismo tecnológico, periodicidad, formatos, que cumpla con lo establecido en el intercambio o acceso seguro de información.
5. Los colaboradores del IGAC solo podrán suministrar información a través de los canales o acceso seguros identificados en los anexos técnicos en los contratos o en los lineamientos de intercambio de información.
6. La información compartida con externos que no se encuentren en acuerdos o actos administrativos debe ser autorizado y aprobado por el líder de proceso y/o propietario del activo de información.
7. Los intercambios de datos deben ser transparentes, de calidad, con lenguaje claro y accesible a los usuarios o grupos de interés.
8. Si existe la necesidad de realizar intercambio de información por mecanismos diferentes a los establecidos en los lineamientos de intercambio o acceso seguro de información, se debe solicitar acompañamiento de la Subdirección de Información y del Oficial de Seguridad de la Información, para identificar los riesgos asociados y establecer los controles de seguridad apropiados.

Responsables

° Subdirección de información (Implementación)
° Subdirección de Infraestructura Tecnológica (Implementación)
° Subdirección General (Implementación)
° Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
° Entidades Públicas y externos (Cumplimiento)

4.3.9 CONTROLES PARA LA GESTIÓN DE REDES

Objetivo: Garantizar la integridad, confidencialidad y disponibilidad de la información transmitida a través de la red del Instituto. Esto se logra mediante la implementación de medidas de seguridad adecuadas, la protección de la infraestructura de red, la gestión de dispositivos de red y la prevención de accesos no autorizados o actividades maliciosas. El objetivo es asegurar que la red del IGAC esté protegida contra vulnerabilidades y amenazas, y que los activos de información estén seguros en todo momento.

1. Establecer procedimientos para la gestión y configuración de los dispositivos de red, asegurando que se implementen las actualizaciones de firmware y parches de seguridad, y se mantengan las configuraciones adecuadas para prevenir vulnerabilidades.
2. Implementar mecanismos de seguridad, como firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS), para filtrar y controlar el tráfico de red, garantizando que solo se permita el acceso autorizado y se bloquee cualquier actividad maliciosa.
3. Establecer herramientas y procedimientos para el monitoreo constante de la red, protocolos y puertos para identificar actividades sospechosas, anomalías de tráfico e intrusiones. Además, se debe realizar registros de eventos y llevar a cabo un análisis de seguridad periódico.
4. Definir e implementar pruebas de penetración interna y externa para detectar vulnerabilidades en la red del IGAC.
5. Se debe realizar gestión y monitoreo constante sobre los equipos tecnológicos de seguridad garantizando:
    a. Las reglas configuradas en equipos de seguridad deben ser revisadas continuamente.
    b. Las firmas y actualizaciones de todos los dispositivos deben encontrarse al día.
    c. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs debe ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis.
    d. Se debe revisar periódicamente el estado de cableado y puntos de red verificando que no existan interferencias o conexiones no autorizadas.
6. Los equipos de seguridad y de comunicación deben contar con mecanismos de autenticación sólidos, como el uso de contraseñas robustas, autenticación de dos factores y gestión adecuada de cuentas de usuario. Asimismo, se deben establecer políticas de control de acceso para restringir el acceso a la red y a los recursos según los privilegios asignados.
7. Con el fin de fortalecer los conocimientos de seguridad en las redes, se establecen estrategias que permitan concientizar a los servidores públicos, contratistas o proveedores que tengan acceso a la información del Instituto, que accedan a la red haciendo uso de las mejores prácticas de seguridad, la importancia de proteger la información y las responsabilidades individuales en la protección de la red.
8. La Subdirección de Infraestructura Tecnológica es responsable de garantizar que los puertos físicos y lógicos de diagnósticos y configuración de plataformas que soporten sistemas de información estén siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.
9. La Subdirección de Infraestructura Tecnológica debe asegurar que la red de ciudadanos no tenga conexión directa a los servidores a fin de evitar afectaciones a la seguridad de la información.
10. La Subdirección de Infraestructura Tecnológica debe definir un esquema de separación de las redes y de los dominios lógicos, teniendo en cuenta los servicios de información, usuarios, aplicaciones y las especificaciones dadas por los líderes de la información, siempre en cumplimiento de la Políticas de Control de Acceso, Uso Aceptable de los Activos de información y los principios de construcción de Sistemas Seguros.
11. La Subdirección de Infraestructura Tecnológica debe sincronizar los relojes de todos los sistemas con una única fuente de referencia de tiempo como la hora legal colombiana (https://horalegal.inm.gov.co/), para asegurar la exactitud de todos los registros de auditoría, que puedan ser necesarios.
12. La Subdirección de Infraestructura Tecnológica será responsable de verificar que se utilicen arquitecturas de enrutamiento que limiten el acceso remoto a los puntos críticos de la red. A través de herramientas que permitan verificar el tráfico de red de origen y destino.
13. La Subdirección de Infraestructura Tecnológica debe establecer el seguimiento continuo de los permisos de acceso validando la rotación que se pueda presentar de servidores y contratistas, además, el monitoreo a los canales dispuestos el Instituto y el aseguramiento de los procesos de autenticación.
14. La red WIFI corporativa y la red LAN son para uso exclusivo de los equipos institucionales tales como equipos de cómputo, dispositivos móviles, entre otros.

15. Para los equipos personales que necesiten realizar conexión a la red WIFI, se le asignará el acceso a la red de acuerdo con el rol o perfil.
16. Los contratistas o personal de proveedores que hagan uso de los equipos personales para el desarrollo de su objeto contractual y que necesiten realizar conexión a la red WIFI, se les asignará la red de contratistas y deberán cumplir como mínimo con los siguientes requisitos de seguridad:
17. Garantizar control de acceso mediante contraseña o reconocimiento de huella.
    a. Tener instalada y actualizada una herramienta de antivirus.
    b. Tener actualizado el sistema operativo del dispositivo móvil en la versión más reciente y estable.
    c. Cumplir con la reglamentación vigente sobre uso de software legal, el usuario es responsable de contar con todo el software de su dispositivo licenciado.
18. La DTIC puede implementar y monitorear controles que permitan conocer el estado de seguridad de los equipos personales que sean autorizados a conectarse a la red contratistas, por medio de VPN u otro tipo de conexión remota.
19. La Subdirección de Infraestructura Tecnológica debe establecer herramientas de monitoreo permanente que permitan generar alertas tempranas ante posibles eventos de seguridad de la información que se puedan presentar.
20. La Subdirección de Infraestructura Tecnológica debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios como a otros equipos. Se deben revisar configuraciones de fábrica (usuarios, contraseñas y archivos compartidos). Los servidores deben tener habilitados sus sistemas de auditoría para permitir el registro de los eventos, se debe realizar configuraciones de seguridad de fábrica.
21. La Subdirección de Infraestructura Tecnológica debe realizar la documentación necesaria para el uso, utilización y manejo de los servicios de red en aras de fortalecer la base de conocimiento de la herramienta de gestión de la Mesa de Servicio de TI.

Responsables

- Dirección de Tecnologías de la Información y Comunicaciones (Implementación)
- Subdirección de Infraestructura Tecnológica (Implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores públicos y contratistas (Cumplimiento)

4.3.10 CONTROLES EN EL USO DEL SERVICIO DE INTERNET

Objetivo: Gestionar el acceso y uso del servicio de internet por parte de los servidores públicos, contratistas o proveedores que tengan acceso a la información institucional, prestando un servicio adecuado del internet y servicios relacionados de acuerdo con las necesidades del Instituto estableciendo controles que permitan mitigar la materialización de los riesgos asociados a su uso.

1. El servicio de acceso a Internet debe utilizarse para las tareas propias de la función desarrollada en cada dependencia del IGAC. Es responsabilidad de cada miembro del Instituto utilizar los servicios de conexión a Internet de forma productiva y eficiente para el Instituto.
2. La Subdirección de Infraestructura Tecnológica en conjunto con el Oficial de Seguridad de la Información, define las políticas, restricciones de acceso, ancho de banda máximo a utilizar, horarios, derechos de descarga de archivos, permisos de navegación y demás relacionados, para garantizar el uso eficiente y racional del Internet.
3. La Subdirección de Infraestructura Tecnológica implementa los controles necesarios de acuerdo con el cumplimiento de las funciones, obligaciones y/o cargo de los servidores públicos o contratistas del Instituto. Lo anterior, con el fin de mitigar los riesgos inherentes al uso de internet, que incrementan los riesgos y vulnerabilidades de la información.
4. Los usos diferentes a los necesarios para el cumplimiento de las funciones del Instituto son de entera responsabilidad de los servidores públicos, contratistas, y proveedores del IGAC al que se le asigna

la cuenta de acceso al servicio, y el uso no adecuado se considera una violación a la política de seguridad de la información. La Subdirección de Infraestructura Tecnológica implementa los mecanismos necesarios que soporten el uso seguro de internet haciendo uso de herramientas especializadas, que permitan analizar y registrar de manera detallada el tráfico desde y hacia el Instituto, si así se requiere, esto sin vulnerar el derecho a la intimidad y privacidad de los servidores públicos.

5. El acceso a sitios Web o la instalación de aplicaciones para intentar evadir los controles y políticas de seguridad de navegación están totalmente prohibidos y su detección será tratada como un incidente de seguridad.
6. Descargar archivos provenientes de Internet implica un riesgo para la seguridad de la información por lo cual únicamente se debe realizar cuando sea necesario, previa justificación de la necesidad; está prohibida la descarga de archivos con extensiones de tipo (*.exe, *.bat, *.prg, *.bak, *pig, entre otros).
7. La Subdirección de Infraestructura Tecnológica se reserva el derecho a monitorear, hacer seguimiento, auditoría y de guardar registro de todos los sitios que se ingresan a través de la red del Instituto (no a las actividades desarrolladas), lo que permite a la Subdirección hacer un seguimiento completo de todos los sitios de Internet a los cuales se acceden y definir las restricciones pertinentes.
8. Los servidores públicos, contratistas o proveedores que tengan acceso a la información institucional del IGAC, no podrán utilizar el servicio de internet para el envío, descarga o visualización de información con contenidos restringidos o que atenten contra la integridad moral de las personas o instituciones, o que esté protegida por derechos de autor o que pongan en riesgo la seguridad y reputación del Instituto, el uso del servicio para actividades comerciales particulares, el acceso a sitios de entretenimiento online, el acceso a sitios Web considerados como ilegales por la normatividad colombiana, incluidos en la Ley de delitos informáticos y aquellos prohibidos por la Ley de Infancia y Adolescencia.
9. La Subdirección de Infraestructura Tecnológica definirá el navegador que será utilizado por los servidores públicos y contratistas en los computadores del Instituto, así como, los controles que permitan garantizar una utilización segura del servicio.
10. No se deben almacenar usuarios y contraseñas en los navegadores que permitan el acceso sin ningún tipo de control (contraseña, sistemas biométricos entre otros) a sistemas de información, herramientas de colaboración, correo, entre otros.
11. La Subdirección de Infraestructura Tecnológica verifica y emite concepto sobre la viabilidad o no de habilitar las páginas, servicios o aplicativos Web que se encuentren bloqueados atendiendo el resultado del análisis de seguridad, dichas solicitudes deben ser realizadas a través de la herramienta de gestión de la Mesa de Servicio de TI y contar con la justificación para su uso de acuerdo con los ANS internos y/o procedimientos definidos por la DTIC. El Instituto se reserva el derecho de suspender dichos servicios de acuerdo con situaciones de riesgo identificadas o reportadas a la Dirección de Tecnologías de la Información y las Comunicaciones.
12. La Subdirección de Infraestructura Tecnológica realiza el monitoreo del origen de las conexiones al servicio de correo electrónico y VPN bloqueando las conexiones que considere sospechosas realizadas desde otros países.
13. Los usuarios del servicio de internet son responsables de evitar prácticas o usos que comprometan la seguridad de la información del Instituto, tales como descargas de software no autorizado.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores públicos y contratistas (Cumplimiento)

4.3.11 CONTROLES PARA SERVICIOS EN NUBE

Objetivo: Establecer los requisitos y procedimientos necesarios para garantizar la seguridad de la información al utilizar servicios de nube pública en el IGAC, incluyendo la selección y evaluación de proveedores, la protección de datos, la gestión de accesos y la continuidad del servicio.

1. La administración de los servicios en nube es responsabilidad de la Subdirección de Infraestructura Tecnológica, teniendo en cuenta:
    a. Contar con acuerdo de confidencialidad con el proveedor.
    b. Contar con acuerdos de niveles de servicio con un 99.5% como mínimo.
    c. Contar con lineamientos de gestión de usuarios de la nube. Estos usuarios deben ser autorizados por la Subdirección de Infraestructura Tecnológica y/o el líder de la información.
    d. Los canales de conexión a la nube deben ser seguros, usar protocolos que permitan la encriptación de las comunicaciones entre el navegador y el servidor web
    e. Se debe realizar una autenticación segura.
    f. Se debe contar con contraseñas robustas e implementación de doble factor de autenticación de acceso a la nube.
    g. Establecer una gestión de capacidad y de disponibilidad de la nube.
    h. La información sensible debe ser cifrada
    i. Debe contar con medidas preventivas que eviten la denegación del servicio.
2. Todos los servicios de nube privada y pública deben ser contratados únicamente por la Subdirección de Infraestructura Tecnológica y estos deberán cumplir con la Política General de Seguridad de la Información junto con sus procedimientos y lineamientos.
3. Para seleccionar el uso de servicios en la nube, se deben identificar y valorar los riesgos asociados a dicho servicio, según la información a gestionarse y clasificación de los activos de información.
4. Se deben establecer mecanismos de autenticación, autorización y registro para cada una de las actividades realizadas sobre el almacenamiento en la nube.
5. La Subdirección de Infraestructura Tecnológica es responsable de establecer los medios de acceso, los dispositivos que tienen acceso, las ubicaciones desde las cuales se puede acceder a los servicios en la nube.
6. La Subdirección de Infraestructura Tecnológica, implementa estrategias para el respaldo de la información alojada en la nube.
7. Los servidores públicos, contratistas o proveedores que tengan acceso a la información institucional del IGAC, son responsables del otorgamiento de accesos y permisos a las carpetas que compartan desde la nube de almacenamiento institucional a otras personas del Institutoy/o externos.
8. La descarga de información de la nube en equipos personales no autorizados por parte de servidores y/o contratistas será tratado como un incidente de seguridad de la información.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores Públicos y contratistas (Cumplimiento)

4.3.12 MANEJO DE EQUIPOS DE CÓMPUTO

Objetivo: Definir lineamientos necesarios para usar los equipos de cómputo del IGAC (computadores de escritorio, portátiles, tabletas, impresoras y otros dispositivos), y manejar adecuadamente la información procesada.

1. Los equipos de cómputo asignados a servidores públicos y contratistas son exclusivos del cumplimiento de las funciones u obligaciones asignadas, y la responsabilidad de su buen uso recaerá sobre la persona asignada.

2. Se deben tomar medidas preventivas al momento de consumir bebidas y alimentos en el puesto de trabajo, considerando que el verter líquidos puede causar daños en los componentes electrónicos, cualquier daño por mal uso o manejo será responsabilidad del servidor público o contratista.
3. La Subdirección de Infraestructura Tecnológica, se reserva el derecho de monitorear el contenido y software instalado en los equipos del Instituto para verificar el tipo de información, su uso y licenciamiento del software instalado. De esta manera contenidos de música, vídeo, fotos o demás que no correspondan al desempeño de las funciones u obligaciones contractuales respectivas del servidor público o contratista podrían ser borrados sin previa consulta. Así mismo, el software no autorizado o sin licenciamiento, será desinstalado.
4. Los únicos autorizados para realizar cambio de partes, actualizaciones, destapar, desconectar, retirar, y/o reparar equipos, y realizar instalación de software son los técnicos de soporte designados por la Subdirección de Infraestructura Tecnológica e ingenieros de las Direcciones Territoriales previa solicitud a través de la herramienta de gestión de la Mesa de Servicio de TI en Sede Central y en las Direcciones Territoriales
5. La Subdirección de Infraestructura Tecnológica a través de la Mesa de Servicio de TI de Sede Central y los Ingenieros Territoriales a nivel Nacional deberá aprovisionar los computadores antes de ser entregados al usuario, garantizando que:
    a. Sean formateados a bajo nivel o borrados de manera segura para que la información de los anteriores usuarios no sea recuperable o accesible.
    b. El software instalado sea el software base (Software Estándar Corporativo) definido por la Subdirección de Infraestructura Tecnológica y este cuente con el respectivo licenciamiento.
    c. Los sistemas operativos y demás aplicativos deberán tener instaladas las últimas actualizaciones estables a la fecha de entrega del equipo.
    d. El antivirus deberá permanecer actualizado, funcionando y administrado desde consola.
    e. Contar con las herramientas de seguridad establecidas por la Subdirección de Infraestructura Tecnológica.
    f. Se encuentren en condiciones en buen estado, limpios y en óptimas condiciones para su uso.
6. La Subdirección de Infraestructura Tecnológica a través de la Mesa de Servicio de TI deberá asegurar que los usuarios y perfiles de usuario que traen por defecto los sistemas operativos y software instalado en los computadores de escritorio, equipos portátiles, impresoras y demás dispositivos adquiridos por el IGAC sean modificados antes de entrar en uso. Dichos elementos deben entregarse sin permisos de acceso con rol de administrador, al usuario final.
7. El bloqueo automático de la pantalla y la ejecución del protector de pantalla en los computadores de escritorio y/o portátiles del IGAC después de un tiempo determinado de inactividad (5 min) será implementado como control preventivo de intrusión no autorizada a los equipos. La implementación de estos mecanismos preventivos estará a cargo de la Subdirección de Infraestructura Tecnológica. Sin embargo, cada usuario deberá garantizar que nadie pueda ingresar al equipo de cómputo durante su ausencia, bloqueando su equipo de cómputo antes de alejarse del mismo.
8. Los servidores públicos y contratistas que tengan asignados equipos de cómputo deben mantener la cultura de bloquear el equipo cuando se ausente de su puesto de trabajo
9. El escritorio de Windows de los computadores y/o portátiles no se debe utilizar para guardar ningún tipo de archivo, excepto los accesos directos que se configuren desde la Mesa de Servicio de TI.
10. Se debe registrar y/o autorizar los equipos tecnológicos del Institutoque ingresen y/o se retiren en todas las sedes de la entidad, según los procedimientos definidos por la Subdirección Administrativa y Financiera.
11. Los dispositivos personales que requieran conectarse a las redes institucionales deberán aplicar las mismas medidas y configuraciones de seguridad a los dispositivos del Instituto.

12. Los equipos de cómputo asignados por el Instituto deben permanecer en las instalaciones de la entidad, excepto cuando sea necesario retirarlos de esta para ser utilizados en actividades inherentes al desarrollo de las funciones, como en comisiones, reuniones externas, eventos, trabajo en casa, teletrabajo o cualquier otra actividad de este tipo que esté autorizada, y deben retornar a las instalaciones en el menor tiempo posible una vez culminada dicha actividad, en caso de retiro el equipo debe realizarlo bajo lineamientos establecidos y formato de Salida de bienes del instituto código FO-INV-PC03-03 V1 de la Gestión de Bienes y Servicios y debe ser devuelto al Instituto informando a la Subdirección de Infraestructura Tecnológica.
13. Los equipos de cómputo al finalizar la jornada laboral deben quedar apagados en caso de no necesitar ser usados con conexión remota.
14. Toda la información debe ser alojada en el repositorio oficiales o herramientas colaborativas asignadas, no se debe almacenar información de manera local en los equipos de cómputo.
15. No está permitido compartir carpetas entre equipos de usuario final.
16. La Subdirección de Infraestructura Tecnológica es la encargada de programar y autorizar el personal para la realización de mantenimientos preventivos.
17. La Mesa de Servicio de TI no es responsable de la información que se almacené en los discos duros de los equipos del instituto, en caso de daño o pérdida la Subdirección de Infraestructura Tecnológica no es responsable de la restauración o recuperación de la información.
18. La Mesa de Servicio de TI realizara el borrado seguro o formateo a bajo nivel de los equipos de cómputo que por su obsolescencia sean dados de baja, que sean enviados a garantía o se deban reasignar.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Apoyo en la implementación)
- Subdirección Administrativa y Financiera (Implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores Públicos y contratistas (Cumplimiento)

4.3.13 DISPOSITIVOS MÓVILES

Objetivo: Establecer un marco de seguridad sólido que proteja la información y los recursos del IGAC al utilizar dispositivos móviles institucionales. El cual busca garantizar que los dispositivos móviles sean utilizados de manera segura y responsable, y que se implementen las medidas de seguridad adecuadas para proteger la información confidencial y prevenir riesgos de seguridad.

1. La Subdirección de Infraestructura Tecnológica instala, actualiza y configura el software y los controles necesarios para proteger los dispositivos móviles institucionales, implementa controles en los servicios o infraestructura a la que se accede desde dispositivos móviles personales autorizados; deben aceptarlos y adoptarlos Servidores Públicos y contratistas, mitigando las pérdidas, fugas de información o la afectación de estos ante ciberataques.
2. El uso de los dispositivos móviles institucionales será para uso exclusivo del desarrollo de las funciones u obligaciones institucionales de los Servidores Públicos y contratistas del IGAC.
3. Es responsabilidad del funcionario o contratista al que se le asigne y use dispositivos móviles institucionales, sincronizar o cargar la información almacenada cada vez que finalice la actividad desarrollada, alojándola en los servicios de nube autorizados por el Instituto, para respaldo de la información.
4. Los dispositivos móviles que no sean propiedad del IGAC y que estén autorizados para acceder a la información, sistemas de información o servicios tecnológicos institucionales, deben contar como mínimo con las siguientes condiciones de seguridad:
5. Garantizar control de acceso mediante contraseña o reconocimiento de huella.
6. Tener instalada y actualizada una herramienta de antivirus.

7. Tener actualizado el Sistema Operativo del dispositivo móvil en la versión más reciente y estable.
8. Cumplir con la reglamentación vigente sobre uso de software legal, el usuario es responsable de contar con todo el software de su dispositivo licenciado.
9. Cualquier incidencia que pueda afectar a la confidencialidad, integridad o disponibilidad de los dispositivos móviles mencionados en el punto anterior, debe ser reportada como un incidente de seguridad de la información.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores públicos y contratistas (Cumplimiento)

4.3.14 CONTROLES DE ACCESO LÓGICOS

Objetivo: Establecer lineamientos para el manejo de los accesos a los sistemas de información y recursos del IGAC, con el objetivo de minimizar el riesgo de accesos no autorizados o uso indebido de la información.

1. Los controles y permisos para el acceso a la información, sistemas de información, plataforma tecnológica y servicios de red serán establecidos de acuerdo con la clasificación de la información, las funciones u obligaciones de los Servidores Públicos y contratistas según corresponda, las necesidades y requerimientos de cada una de los procesos o subprocesos del IGAC orientadas a garantizar la protección y seguridad de la Información.
2. La Subdirección de Infraestructura Tecnológica, establece una Política de contraseñas adecuada y alineada con las buenas prácticas en seguridad. La política de contraseñas establecida en los sistemas de información, plataforma tecnológica o sistema de autenticación definirá los requisitos de las contraseñas y los plazos de mantenimiento de una misma contraseña. La Política de contraseñas deberá ser conocida por los servidores públicos y contratistas.
3. Es responsabilidad de cada funcionario, contratista o tercero que tenga acceso o uso de cualquier activo de información, el resguardo de sus contraseñas, por lo tanto, no podrán estar escritas o expuestas en su puesto de trabajo, no deben prestarse o compartirse con el fin de evitar que sean conocidas por otras personas.
4. Los accesos a la información en formato digital, sistemas de información, plataforma tecnológica y servicios de red del IGAC, serán gestionados mediante la asignación de un usuario único para cada funcionario o contratista de acuerdo con su perfil y los accesos necesarios para el cumplimiento de sus funciones u obligaciones, asignados mediante el principio de mínimo privilegio, este usuario es intransferible y cada funcionario o contratista es responsable de las acciones que se ejecuten con éste.
5. Los accesos lógicos, asignados a los servidores públicos, contratistas y proveedores deben ser desactivados una vez se terminen los vínculos contractuales con el IGAC, por solicitud del supervisor del contrato, por trámite de paz y salvo o por la Subdirección de Talento Humano. La desactivación de los permisos de acceso de servidores públicos acorde con la resolución de desvinculación y la de los contratistas de acuerdo con la fecha de terminación del contrato.
6. Las conexiones a los sistemas de información que se realicen desde fuera de las instalaciones del IGAC se deberán realizar mediante las herramientas definidas por la Subdirección de Infraestructura Tecnológica, las cuales permiten el registro de las actividades de conexión realizadas durante el tiempo que permanezca conectado.
7. La conexión de dispositivos de infraestructura a la red de datos institucional debe coordinarse con la Subdirección de Infraestructura Tecnológica mediante la herramienta de gestión de la Mesa de Servicio de TI, según los procedimientos definidos.

8. La creación, modificación, des habilitación o retiro de usuarios en los sistemas de información y/o servicios de red y/o infraestructura tecnológica se realiza de acuerdo con el procedimiento definido en la Subdirección de Infraestructura Tecnológica. Es responsabilidad de las dependencias la administración de las credenciales de acceso de los servicios o sistemas de información que no estén bajo la gobernanza de la Subdirección de Infraestructura Tecnológica.
9. Ante cualquier sospecha de que el usuario asignado para el ingreso a cualquiera de las herramientas tecnológicas o sistemas de información del Instituto ha sido utilizado de manera inadecuada, debe informarse inmediatamente a la Mesa de Servicio de TI.
10. La Subdirección de Infraestructura Tecnológica definirá las condiciones y/o requerimientos para la implementación de mecanismos de doble factor de autenticación para los servicios y/o sistemas de información y/o Infraestructura Tecnológica donde sea requerido un mayor nivel de protección en el acceso.
11. Los accesos a los sistemas de información deberán contar como mínimo con un usuario y contraseña, con el fin de proteger el acceso no controlado a la información institucional.
12. La Subdirección de Infraestructura Tecnológica debe realizar el mantenimiento, actualización y/o depuración de las cuentas de usuario de los sistemas de información y/o aplicativos, de acuerdo con las novedades administrativas. Además, deberán realizar la validación de las cuentas en períodos de inactividad mayores a 3 meses. Es responsabilidad de las dependencias realizar las actividades mencionadas anteriormente para los servicios o sistemas de información que no estén bajo la gobernanza de la Subdirección de Infraestructura Tecnológica.
13. La Subdirección de Infraestructura Tecnológica realiza la gestión permanente de los accesos lógicos de los usuarios asignados a los servidores, contratistas y terceros, realizando la habilitación, modificación o desactivación de estos, de acuerdo con el tiempo que tenga de vínculo con el IGAC, el cargo o funciones que desempeñen, o si sufren alguna modificación en su rol o cambio de dependencia; esto con el fin de prevenir que los accesos a los sistemas queden activos para usuarios que ya no deberían acceder o que ya no tienen vínculo con el Instituto.
14. La DTIC solo otorgará a los usuarios accesos a los sistemas, aplicaciones o bases de datos que estén bajo su alcance bajo la autorización dada por correo electrónico por los líderes de los procesos o líderes funcionales, previa justificación del tipo de permiso que requiere, tiempo y la razón del mismo.
15. La contraseña de acceso a los equipos de cómputo debe ser cambiada cada 30 días para lo cual se establece una política en el Directorio Activo.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- Subdirección de Sistemas de Información (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores públicos y contratistas (Cumplimiento)

4.3.15 GESTIÓN DE CUENTAS PRIVILEGIADAS

Objetivo: Definir lineamientos para la adecuada gestión de las cuentas de usuario con privilegios de administración sobre los componentes tecnológicos.

1. Las cuentas de usuario privilegiado de las plataformas tecnológicas que soporta la operación de los sistemas de información o aplicaciones deben ser autorizadas formalmente por el Subdirector de Infraestructura Tecnológica, las cuentas de administración funcional a cargo de dependencias diferentes a la Subdirección de Infraestructura Tecnológica deben ser informadas a dicha Subdirección.

2. La Subdirección de Infraestructura Tecnológica mantendrá un registro actualizado de las cuentas de usuario privilegiadas, el cual debe contener el responsable y la justificación de la necesidad de uso.
3. Las cuentas de usuario privilegiado sólo deben ser otorgadas a los servidores públicos y contratistas que las requieran, los cuales deben hacer un uso apropiado de estas y usarlas únicamente para el cumplimiento de sus funciones.
4. Las cuentas de usuario privilegiado sólo podrán ser utilizadas en la actividad de administración o configuración del sistema o plataforma para la cual se requieren dichos privilegios. No podrá ser utilizada en actividades de operación rutinarias para lo cual debe existir un perfil de menores privilegios que lo permita.
5. Las cuentas de usuario privilegiado o similares, definidas por defecto, en sistemas e infraestructura tecnológica, deben ser usadas únicamente en caso de que no sea posible asignar cuentas de administración sobre usuarios nombrados y/o en caso de pérdida de acceso de los usuarios de administración nombrados. Siempre que sea posible las mismas deben ser eliminadas o deshabilitadas, además de modificadas sus contraseñas por defecto. Se debe contar con un mecanismo de recuperación de acceso privilegiado, dicho mecanismo debe mantener las garantías de confidencialidad
6. Para las cuentas de usuario privilegiado o similares, en sistemas e infraestructura tecnológica, deberán definirse los requisitos para la caducidad de los derechos de acceso privilegiado.
7. Las competencias de los usuarios con derechos de acceso privilegiado deberán revisarse regularmente con el objetivo de verificar que se encuentran alineadas con sus obligaciones.
8. Las credenciales de acceso de los usuarios privilegiados o similares deben ser almacenadas y/o custodiadas estableciendo mecanismos que aseguren la confidencialidad de la información secreta de autenticación, tales como, cifrado, acceso restringido mediante asignación de contraseña.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- Subdirección de Sistemas de Información (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores Públicos y contratistas (Cumplimiento)

4.3.16 USO DE CORREO ELECTRÓNICO

Objetivo: Establecer lineamientos y controles para el uso seguro y adecuado del correo electrónico institucional.

1. El servicio de correo electrónico debe utilizarse exclusivamente para las actividades propias de las funciones del IGAC. Cualquier uso diferente al cumplimiento de las funciones u obligaciones con el Instituto se consideran una violación a la Política General de Seguridad de la Información por parte de los servidores públicos y contratistas al que se les asigna la cuenta de correo electrónico.
2. Los correos electrónicos serán considerados parte de los registros del Institutoy conforme a esto están sujetos a ser almacenados, monitoreados y auditados en los casos permitidos por la ley.
3. El envío de correos masivos está restringido, únicamente será permitida esta actividad por las cuentas autorizadas por la Secretaria General para esta labor.
4. Está permitido enviar correos a máximo 50 destinatarios, y se debe utilizar el campo CCO (con copia oculta) para mantener la confidencialidad de las cuentas a las que se dirige la comunicación.
5. La única cuenta de correo electrónico autorizada para el manejo de información institucional es el asignado con el dominio @igac.gov.co, esta cumple con los parámetros de seguridad y requerimientos de ley para tal fin.

6. Las cuentas de correo electrónico oficiales del Instituto son las establecidas por la Subdirección de Infraestructura Tecnológica. Los Servidores Públicos, contratistas y proveedores que tengan acceso a la información institucional, que utilicen otras cuentas de correo para la gestión de sus labores en el Instituto, reconocen y aceptan que los incidentes de seguridad de la información generados por el uso de servicios de cuentas de correo electrónico no autorizadas serán de su entera responsabilidad y serán considerados una violación a la Política de Seguridad de la Información.
7. La Subdirección de Infraestructura Tecnológica podrá restringir el acceso a plataformas de correo distintas a la plataforma oficial de correo del Instituto, con el fin de mitigar los riesgos de fuga o pérdida de información y descarga de software malicioso.
8. La Subdirección de Infraestructura Tecnológica se reserva el derecho de filtrar, de manera automática, los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán analizados por las herramientas de protección definidas para tal fin.
9. La configuración de acceso a la cuenta de correo desde medios distintos a los asignados por el IGAC debe ser validado y monitoreado periódicamente por la Subdirección de Infraestructura Tecnológica.
10. Es prohibido el uso del correo electrónico del IGAC para el envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, que promuevan la discriminación sobre la base de raza, color, pertenencia étnica, origen nacional o social, género, edad, estado marital, orientación sexual, religión o discapacidad, opiniones políticas o de otra índole, posición económica, nacimiento o cualquier otra condición social, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales o cualquier contenido que represente riesgos para la seguridad de la información.
11. Es responsabilidad de los servidores públicos y contratistas informar a la Mesa de Servicio de TI cuando lleguen a su buzón correos sospechosos, cadenas y phishing, entre otros.
12. Ningún servidor público o contratista podrá utilizar el Chat Corporativo para enviar información que no sea propia del ejercicio de sus funciones y que esté enmarcada dentro de la ejecución de estas, como tampoco para divulgar información de carácter privado o confidencial a cargo del Instituto, ni para dar a conocer decisiones administrativas que no se encuentren en firme y debidamente ejecutoriadas.
13. Los servidores públicos y contratistas no deben suministrar los datos de acceso o clave de la cuenta de correo asignada por el Instituto. Si se sospecha que esta clave es conocida debe ser cambiada inmediatamente y reportada como un incidente de seguridad de la información.
14. Al momento de la firma de paz y salvo, el servidor público o contratista de la DTIC procederá a deshabilitar la cuenta de usuario de red y por lo tanto la cuenta de correo electrónico institucional, como medida preventiva. Si se requiere una extensión de tiempo, el jefe inmediato o supervisor del contrato enviará la solicitud a la Mesa de Servicio de TI, donde deberá justificar la causa y asumirá los riesgos asociados a tener habilitada una cuenta de usuario para un servidor público o contratista sin vínculo contractual o laboral con el Instituto.
15. El servicio de correo electrónico debe implementar mecanismos de doble factor de autenticación, si el usuario no está de acuerdo con la implementación de esta medida de seguridad solo podrá usar el correo en las instalaciones del Instituto.
16. No se entregan copias de correo, OneDrive o información almacenada en cualquier herramienta colaborativa suministrada por el IGAC, en caso de que un(a) Ex funcionario(a), Ex contratista requiera aportar o soportar como evidencias en el marco de una investigación fiscal, disciplinaria o penal que esté en curso, en su contra, información incluida en el correo institucional o alguna de las herramientas asignadas durante su vinculación con el IGAC, previa presentación de la solicitud formal motivada indicando esta condición, el Institutoverificará dentro de sus archivos y proporcionará directamente al ente de control el acceso en forma de consulta a la información que se referencie en el proceso.

17. Si los proceso o subprocesos requieren para el ejercicio de las funciones de la utilización de una cuenta de correo genérica, está debe ser solicitada por el líder o jefe previa justificación del uso y responsable de la misma.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Líderes de procesos (Cumplimiento)
- Servidores Públicos y contratistas (Cumplimiento)

4.3.17 CONTROL DE COPIAS DE SEGURIDAD

Objetivo: Establecer los lineamientos y procedimientos para la creación, gestión y almacenamiento de copias de seguridad de la información en el IGAC. Se busca garantizar la ejecución periódica de copias de seguridad, así como la adecuada protección y custodia de los respaldos, con el fin de asegurar la rápida recuperación de la información en caso de pérdida o daño.

1. La dirección de la DTIC, o quien esta delegue recibirán, a través de la herramienta de gestión de la Mesa de Servicios de TI, por parte de los líderes de los procesos y dependencias, los requerimientos para respaldar la información en función de su criticidad y la frecuencia con que se debe realizar.
2. La Subdirección de Infraestructura Tecnológica debe generar pruebas periódicas de restauración de las copias de respaldo, dándole prioridad a las aplicaciones que soporten los procesos misionales.
3. Los medios de almacenamiento con información respaldada deben ser manipulados única y exclusivamente por el personal designado por la Subdirección de Infraestructura Tecnológica, para tal fin.
4. El GIT de Gestión Documental, o quien esta delegue, debe establecer los niveles de protección física y ambiental adecuados para proteger la información bajo su custodia.
5. La Subdirección de Infraestructura Tecnológica, debe generar copias de respaldo de información de acuerdo con lo establecido en el plan de respaldo.
6. En caso de existir un custodio externo de los medios de respaldo, éste debe contar con los controles de seguridad necesarios para su almacenamiento y gestión relacionada con la entrega o retiro de estos al responsable designado por la Subdirección de Infraestructura Tecnológica.
7. Es responsabilidad de todos los Servidores Públicos y contratistas almacenar la información asociada con su labor, en los repositorios oficiales establecidos por el Instituto, para garantizar que la información está siendo respaldada.
8. La solicitud para la restauración de los respaldos de información por parte de los colaboradores retirados del IGAC, deben realizarse mediante requerimiento formal ante el Instituto, la cual será revisada y analizada por parte del líder del proceso propietario de la información y el oficial de seguridad de la información, de acuerdo con el tiempo y retención definido en el plan de copias de respaldo a cargo de la Subdirección de Infraestructura Tecnológica.
9. No se entregan copias de correo, repositorios de almacenamiento, o información almacenada en cualquier herramienta colaborativa suministrada por el IGAC, en caso de que un(a) Ex funcionario(a), Ex contratista requiera aportar o soportar como evidencias en el marco de una investigación fiscal, disciplinaria o penal que esté en curso en su contra, información incluida en el correo institucional o alguna de las herramientas asignadas durante su vinculación con el IGAC, previa presentación la solicitud formal motivada indicando esta condición, el Institutoverificará dentro de sus archivos y proporcionará directamente al ente de control acceso en forma de consulta a la información que se referencie en el proceso.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- El GIT de Gestión Documental (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores Públicos y contratistas (Cumplimiento)

4.3.18 DESARROLLO SEGURO

Objetivo: Establecer las directrices y requisitos para desarrollar software y aplicaciones de manera segura, minimizando los riesgos de seguridad y protegiendo la información de la organización. Se busca fomentar la adopción de buenas prácticas de desarrollo seguro y promover la conciencia sobre la importancia de la seguridad desde las etapas iniciales del ciclo de vida del desarrollo.

1. Los servidores públicos y contratistas que realicen actividades del ciclo de vida de desarrollo de software deben tener entrenamiento básico en seguridad de la información y privacidad, y deben conocer la Política General de Seguridad de la Información.
2. La Subdirección de Sistemas de Información, debe asegurar que se diseñen e implementen los requerimientos de seguridad en el software, ya sea desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.
3. La especificación de los requisitos de seguridad de la información para nuevos desarrollos y sistemas de información se deben implementar buenas prácticas de desarrollo en la que se garantice los niveles de seguridad mínimos que se tienen establecidos y, estos serán identificados de acuerdo con los protocolos, guías y lineamientos establecidos en la Política de Seguridad de la Información.
4. Los requerimientos de seguridad de la información identificados deben considerar los posibles riesgos, a fin de establecer los mecanismos de seguridad de la Información, que apliquen para el caso de: software de terceros o desarrollos propios.
5. Durante el desarrollo del código para software específico o sistemas de información, se deben establecer revisiones de código estático, permitiendo tener un mejor nivel de seguridad, evidenciando tempranamente problemas del software o sistema de información, esta actividad debe ejecutarse previo a la puesta en producción.
6. El software desarrollado por parte de los servidores públicos o contratistas debe contar con una herramienta para el control de versiones que permita a los desarrolladores llevar el control de versiones del software desarrollado.
7. Los contratos establecidos para el desarrollo de software por parte de contratistas del IGAC o contratados con terceros deben especificar los acuerdos sobre propiedad, entrega y custodia del código fuente y sus respectivas versiones, documentación técnica y de uso del software o sistema de información, derechos de propiedad intelectual, soportes del desarrollo de las actividades establecidas en la presente política.
8. El software desarrollado por los servidores públicos o contratistas del IGAC, en el ejercicio de sus funciones u obligaciones, se entiende propiedad del Instituto quien tendrá los derechos de autor patrimoniales, propiedad intelectual y éste deberá ser documentado, almacenado y controlado de acuerdo con los procedimientos establecidos por la Subdirección de Sistemas de Información.
9. La información que se encuentra en los sistemas de producción no puede ser disminuida en los niveles de protección, por tanto, para procesos de desarrollo y pruebas, se debe evitar el uso de datos de producción y en caso de ser necesario su utilización, anonimizar los datos o de lo contrario garantizar la eliminación segura al momento de finalización de las pruebas.
10. Una vez concluido el desarrollo del software o sistema de información, se deben ejecutar pruebas de seguridad que permitan establecer el cumplimiento de los requisitos de establecidos, la verificación de los controles de seguridad para minimizar los posibles riesgos y vulnerabilidades.

11. Las actividades realizadas por los servidores públicos y/o contratistas que efectúen labores de desarrollo de software pueden ser monitoreadas y/o auditadas por la Subdirección de Infraestructura Tecnológica y/o Subdirección de Sistemas de Información, para preservar la seguridad de los ambientes de prueba, desarrollo y producción. En caso de detectarse comportamientos sospechosos o anómalos, estos serán tratados como un incidente de seguridad de la información.
12. El software utilizado o necesario durante el ciclo de vida de desarrollo debe ser validado desde el componente de seguridad de la información, adicionalmente, las herramientas de desarrollo y los componentes de cada sistema de información deben estar actualizados con todos los parches generados para las versiones en uso y se debe verificar que se estén ejecutando la última versión aprobada del sistema.
13. Las actividades ejecutadas por los servidores públicos y/o contratistas que efectúen labores de desarrollo de software a los cuales se le asigne usuarios con permisos de administrador son de su total responsabilidad. En caso de detectarse comportamientos sospechosos o anómalos, estos serán tratados como un incidente de seguridad de la información.
14. Los cambios de software se realizarán siempre en el ambiente de pruebas dispuesto por el Instituto. Una vez superada la etapa de pruebas y de seguridad la Subdirección de Sistemas de Información documenta y coordina el paso a producción con la dependencia funcional (si aplica), previa presentación y aprobación por parte del Equipo de Gestión de Cambios y lineamientos establecidos en el procedimiento vigente de Gestión de Cambios de TI.
15. Si los nuevos desarrollos son adquiridos a través de terceros, se deberá seguir un proceso formal de adquisición. Los contratos con los proveedores tendrán incluidos los requisitos de seguridad de la información y la puesta en producción se realizará previa aprobación del Equipo de Gestión de Cambios de TI.
16. Todo desarrollo de software realizado en el Instituto debe ser autorizado por la Subdirección de Sistemas de Información y debe cumplir todos los lineamientos establecidos para el desarrollo seguro.
17. La Subdirección de Sistemas de Información debe realizar la documentación necesaria para el uso, utilización y manejo cuando aplique de los sistemas de información en aras de fortalecer la base de conocimiento de la herramienta de gestión de la Mesa de Servicio de TI.

Responsables

- Subdirección de Sistemas de Información (Implementación)
- Subdirección de Infraestructura Tecnológica (Apoyo en la implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Procesos o subprocesos del IGAC (Cumplimiento)

4.3.19 CONTROL PARA EL TRABAJO SEGURO A DISTANCIA O EN CASA

Objetivo: Establecer los requisitos y procedimientos para garantizar la seguridad en la conexión remota en el contexto del teletrabajo en el IGAC, protegiendo la información confidencial y asegurando la integridad de los datos.

1. Los servidores públicos y contratistas deben cumplir con todos los lineamientos establecidos en esta política cuando se esté realizando trabajo seguro a distancia o en casa.
2. Los servidores públicos deberán seguir los lineamientos establecidos por la Subdirección de Talento Humano en el procedimiento Modalidad de Teletrabajo vigente.
3. Los equipos personales que se autoricen para el trabajo seguro a distancia o en casa deben ser autorizados por la Subdirección de Infraestructura Tecnológica cumpliendo como mínimo con los siguientes requisitos:
    a. Control de acceso al usuario mediante contraseña o reconocimiento de huella.

b. Tener instalada y actualizada una herramienta de antivirus.
c. Software instalado licenciado en el equipo (Si aplica)
d. Sistema Operativo actualizado

4. La Subdirección de Infraestructura Tecnológica implementa controles que permitan la verificación de cumplimiento de condiciones mínimas de seguridad establecidas en el numeral 2.
5. Cuando sea posible la conexión remota a los Sistemas de Información del IGAC debe realizarse mediante VPN, el cual es el recurso implementado por la Subdirección de Infraestructura Tecnológica para la conexión externa.
6. En los computadores o dispositivos móviles usados para realizar trabajo remoto no se debe guardar usuarios y contraseñas para conexión a los sistemas de información, correo electrónico, almacenamiento en nube entre otros.
7. Las conexiones remotas solicitadas por los servidores públicos, contratistas y proveedores deben ser aprobadas por el jefe inmediato o el supervisor del contrato según aplique especificando los servicios, aplicaciones, servidores tecnológicos, entre otros y el tiempo de conexión requerido, por medio de la herramienta de mesa de servicio de la Subdirección de Infraestructura Tecnológica.
8. La Subdirección de Infraestructura Tecnológica, monitorea las conexiones remotas a fin de verificar el buen uso y detectar posibles eventos de seguridad, pudiendo bloquear la conexión ante comportamientos anómalos o sospechosos.
9. Toda la información debe ser almacenada en las carpetas compartidas o repositorios establecidos por la Subdirección de Infraestructura Tecnológica, no se debe almacenar información pública clasificada publica o publica reservada en equipos personales.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- Subdirección de Talento Humano (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores Públicos y contratistas (Cumplimiento)

4.3.20 USO DE DISPOSITIVOS DE ALMACENAMIENTO EXTERNO

Objetivo: Establecer los requisitos y procedimientos para el uso de dispositivos de almacenamiento externo (USB, Discos Externos, DVD, CD, Blue Ray, ZIP Drive, SD Card, o cualquier otro dispositivo que pueda ser usado para el almacenamiento de información, mitigando los riesgos de fuga de información, contaminación por virus, acceso no autorizado, entre otros.

1. La instalación, configuración y activación para el uso de dispositivos de almacenamiento externo (asignados por el IGAC o personales), estará a cargo de la Dirección de Tecnología de la Información y Comunicaciones, previa autorización del (la) jefe de la dependencia y el (la) Oficial de Seguridad de la Información, las solicitudes se atenderán a través de la Mesa de Servicios de TI.
2. La Dirección de Tecnología de la Información y Comunicaciones implementará las restricciones para llevar trazabilidad y control del uso de los medios de almacenamiento externos conectados a los computadores portátiles o de escritorio propiedad del IGAC, según los permisos establecidos.
3. La conexión de dispositivos usados como tokens de acceso a plataformas de entidades del gobierno, bancos, entre otros, estará habilitada permanentemente
4. La Dirección de Tecnologías de la Información y Comunicaciones debe monitorear el uso de medios de almacenamiento externo en la plataforma tecnológica y las estaciones de trabajo del IGAC.
5. La Dirección de Tecnología de la Información y Comunicaciones debe mantener el inventario de servidores públicos contratistas y/o personal provisto por terceros que estén autorizados y habilitados para dar uso de dispositivos de almacenamiento externo con sus respectivos soportes.

6. Todos los dispositivos de almacenamiento externos o personales autorizados para equipos de cómputo del IGAC se deberán analizar con herramientas de antivirus dispuestas por la Dirección de Tecnología de la Información y Comunicaciones para identificar posibles amenazas y reducir daños, pérdidas o fugas de información o a la infraestructura tecnológica, si el análisis da positivo para virus, se debe avisar inmediatamente a la Mesa de Servicio de TI.
7. Se debe cifrar el dispositivo o la información contenida en este si está clasificada cómo publica clasificada o publica reservada.
8. Los dispositivos de almacenamiento externo deben usarse como almacenamiento temporal de información, por lo que, tras cumplirse el objetivo, debe borrarse seguramente la información del IGAC.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)
- Servidores Públicos, contratistas y proveedores (Cumplimiento)

4.3.21 FORTALECIMIENTO EN CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

1. La Subdirección de Infraestructura Tecnológica evaluará la necesidad de adquirir, implementar o actualizar las herramientas que permitan gestionar de manera adecuada los controles de seguridad de la información.
2. La Dirección de Tecnologías de la Información y Comunicaciones diseñará e implementará el Plan de Recuperación de Desastres tecnológicos (DRP) orientado al restablecimiento de los sistemas, servicios, comunicaciones e infraestructura tecnológica del IGAC, que le permitan continuar con su funcionamiento en caso de presentarse un incidente que amerite su ejecución.
3. Cada vez que se realicen cambios en las aplicaciones y/o sistemas de información y/o Infraestructura Tecnológica críticos se debe tener en cuenta su modificación o inclusión en el DRP con el fin de evitar afectaciones en la disponibilidad de los servicios.
4. Cada vez que se construya, actualice, pruebe o se ponga en activación el Plan de Recuperación de Desastres tecnológicos, se deberá contemplar la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos, y deberá ser probado con el escenario que simule la materialización de un ataque cibernético.
5. La Dirección de Tecnologías de la Información y Comunicaciones establece las estrategias de seguridad de la Información para la implementación, gestión y seguimiento de los lineamientos establecidos en la Política General de Seguridad de la Información y demás lineamientos para proteger la infraestructura tecnológica, Sistemas de información, servicios e información del IGAC.
6. La Subdirección de Infraestructura Tecnológica establece las estrategias de ciber resiliencia para poder resistir o responder a ataques o interrupciones imprevistas mediante la gestión, protección, detección e identificación, respuesta y recuperación de amenazas cibernéticas.
7. Todas las adquisiciones de bienes y/o servicios tecnológicos deben ser revisadas técnicamente y/o avaladas por la Dirección de Tecnologías de la Información y Comunicaciones para garantizar la inclusión de características asociadas a la preservación de la confidencialidad, integridad y disponibilidad de la información y los entornos digitales.

Responsables

- Subdirección de Infraestructura Tecnológica (Implementación)
- Dirección de Tecnologías de la Información y Comunicaciones (Implementación)
- Subdirección de Sistemas de Información (Apoyo en la implementación)
- Subdirección de Información (Apoyo en la implementación)
- Oficial de Seguridad de la Información o profesional designado de la DTIC (Apoyo en la implementación)

- Servidores Públicos y contratistas (Cumplimiento)

4.4 DESVIACIONES Y EXCEPCIONES AL MANUAL DE SEGURIDAD DE LA INFORMACIÓN

Las excepciones a las políticas, procedimientos y controles en la Gestión de la Seguridad de la Información deben ser evaluadas por la Dirección de Tecnologías de la Información y Comunicaciones y el Oficial de Seguridad de la Información, teniendo en cuenta:

- El evento que genera la excepción.
- Los posibles riesgos que puedan presentarse con la excepción.
- El posible impacto que pueda generar la excepción.
- Las acciones para el manejo de la excepción.
- Si es necesario, por el impacto que pueda generar en la operación del Instituto, continuidad de los servicios y, en general, en cumplimiento de la misionalidad, la situación de excepcionalidad deberá informarse y escalarse a la Dirección General.

5. DEFINICIONES

- **Acción Correctiva**: Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable.
- **Acción de Mejora:** Actividad para mejorar el desempeño.[1]
- **Activo de Información:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.[2]
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.[3]
- **Auditoría:** Es un proceso de verificación y/o validación del cumplimiento de una actividad según lo planeado y las directrices estipuladas[4]
- **Confidencialidad:** Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.[5]
- **Control**: Medida que modifica el riesgo. Sinónimo de salvaguarda[6]
- **CSIRT:** Entidad del gobierno que se encarga de ofrecer servicios proactivos de reactivos, reactivos y de gestión de la seguridad básicos a todas las entidades del Estado, generando alertas y advertencias sobre amenazas y vulnerabilidades.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a pedido por una entidad autorizada.[7]
- **Gestión de riesgos**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos. [8]
- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.[9]
- **Información pública**: Es toda información que un sujeto obligado genere, obtenga, adquiera,
- controle en su calidad de tal.[10]
- **Información pública clasificada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre

[1] Ibidem
[2] Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información (s.f.). Tomado de https://www.iso27000.es/glosario.html
[3] Ibidem
[4] GRUPO VIDAWA SAS. (s/f). Auditoría, conceptos y definiciones clave. Kawak.net. Recuperado el 24 de mayo de 2023, de https://landing.kawak.net/conceptos-y-definiciones-clave-de-auditoria
[5] NTC ISO/IEC 27002:2013
[6] Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información (s.f.). Tomado de https://www.iso27000.es/glosario.html
[7] Norma ISO 27000:2018
[8] Lista de Glosarios de términos especializados (2017.febrero 17). Recuperado de https://glosarios.servidor-alicante.com/
[9] Ley 1712 del 6 de marzo de 2014, Artículo 6
[10] Ley No.1712 del 2014, Ley de Transparencia y del derecho de acceso a la información Pública Nacional

que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.[11]

- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.[12]
- **Integridad**: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.[13]
- **No Conformidad:** El no cumplimiento de un requisito especificado a la cual se debe dar tratamiento. Debe tratarse con una acción correctiva[14]
- **Observancia**: Cumplimiento exacto y puntual de lo que se manda ejecutar, como una ley, un estatuto o una regla.[15]
- **Protección de la información:** Conjunto de medidas preventivas y reactivas que deben tomarse para mantener la confidencialidad, la disponibilidad e integridad de la información obtenida para la búsqueda, así como el contacto y protección de personas y organizaciones que aporten información para la búsqueda.[16]
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.[17]
- **Seguridad de la información**: Es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la información.[18]
- **Sistema de Seguridad de la Información (SSI):** Diseño, implementación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.[19]
- **Soporte documental**: Medio que contiene la información, sin importar el material empleado. Además de los archivos en papel, también se entenderá como soporte documental el electrónico
- en que se pueden incluir los archivos audiovisuales, fotográficos, fílmicos, informáticos (textos, listados, bases de datos, cartografías, etc.), orales y sonoros, independientemente de su medio de almacenamiento (CDs, DVDs, USB y demás medios magnéticos, entre otros).[20]
- **Tercero**: Hace referencia a proveedores, empresas, organizaciones o entidades del estado con las que se realice algún convenio de acceso o transferencia de información.[21]

[11] Ibidem
[12] Ibidem
[13] Ibidem
[14] Norma Técnica Colombiana, NTC -ISO 9000:2015 Sistema de Gestión de la Calidad
[15] NTC ISO/IEC 27000:2013
[16] NTC ISO/IEC 27000:2013
[17] ISO/IEC 27000, (ISO Guía 73:2002)
[18] Seguridad de la Información [En Wikipedia]. Recuperado (2022, mayo 23) de https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
[19] ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información? (2013, febrero 19). Tomado de https://www.firma-e.com/blog/quees-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/
[20] ALCALDÍA MAYOR DE BOGOTÁ. Décimo Primer lineamiento distrital: Inventario de activos de información [en línea]. 11. Bogotá, D.C.: [s.n.], 2015 [consultado el 28, julio, 2022]. 28 p. Disponible en Internet: . 35 Manual de Políticas de Seguridad de la Información de la Cámara de Representante
[21] Manual de Políticas de Seguridad de la Información de la Cámara de Representantes. (2020, Julio). https://www.camara.gov.co/sites/default/files/2021-01/MANUAL%20POLITICAS%20DE%20SEGURIDAD%20-%20V2%2020200702%20%282%29%20%282%29_1.docx

6. CONTROL DE CAMBIOS

FECHA	CAMBIO	VERSIÓN
11/06/2024	◦ Se adopta como versión 1 por corresponder a la creación del documento. Emisión Inicial Oficial. ◦ Hace parte del proceso de **Gestión Estratégica de Tecnología.** ◦ Se crea el Manual de Seguridad de la Información, código **MN-GET-02**, versión 1.	**1**

ELABORÓ Y/O ACTUALIZÓ	REVISÓ TÉCNICAMENTE	REVISÓ METODOLÓGICAMENTE	APROBÓ
Nombre: Diego Ramirez Pulido **Cargo:** Contratista. Dirección de Tecnologías de la Información y Comunicaciones. **Nombre:** Juan de Jesús Aponte Buitrago. **Cargo:** Contratista. Dirección de Tecnologías de la Información y Comunicaciones	**Nombre:** Diego Fernando Carrero Barón **Cargo:** Subdirector General **Nombre:** Martha Lucia Parra García **Cargo:** Secretaria General **Nombre:** Gloria Marlen Bravo Guaqueta **Cargo:** Subdirectora. Subdirección de Talento Humano **Nombre:** Camila Gutiérrez Barragán **Cargo:** Subdirectora. Subdirección Administrativa y Financiera **Nombre:** Javier Enrique Gutiérrez Rocha **Cargo:** Coordinador. GIT Contratación. Subdirección Administrativa y Financiera. **Nombre:** Fabian Eduardo Camelo Sánchez **Cargo:** Jefe de Oficina Oficina Asesora de Planeación. **Nombre:** Cristian José Petro Petro **Cargo:** Subdirector. Subdirección de Infraestructura Tecnológica. **Nombre:** Diana Alexandra Ruiz Bedoya	**Nombre:** Orlando José Maya Martínez **Cargo:** Contratista. Oficina Asesora de Planeación.	**Nombre:** Perla Yadira Rojas Martínez **Cargo:** Directora. Dirección de Tecnologías de la Información y Comunicaciones.

ELABORÓ Y/O ACTUALIZÓ	REVISÓ TÉCNICAMENTE	REVISÓ METODOLÓGICAMENTE	APROBÓ
	Cargo: Subdirectora. Subdirección de Información. **Nombre:** Fernando Pérez Moreno **Cargo:** Subdirector. Subdirección de Sistemas de Información.		