Manual del Sistema de Gestión de Seguridad de la Información - SGSI

Instituto Colombiano Agropecuario - ICA

Abril 2020

El presente Manual es parte integral del Manual del Sistema de Gestión DIR-MEJ-MSG-001.

TABLA DE CONTENIDO

OBJETIVO 4
1 GENERALIDADES 4
1.1 APLICACIÓN 4
1.2 DEFINICIONES 4
1.3 NORMAS APLICABLES 4
2 INTRODUCCIÓN 5
2.1 MISIÓN 6
2.2 VISIÓN 7
2.3 ESTRUCTURA ORGANIZACIONAL 7
3 MODELO SISTEMA DE GESTION EN SEGURIDAD DE LA INFORMACIÓN SGSI 8
3.1 HISTORIA Y SGSI 8
3.2 DESCRIPCIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN 9
3.3 PRINCIPIOS 10
3.4 POLITICAS 10
3.5 PROCEDIMIENTOS 11
3.6 ESTÁNDARES 11
3.7 GUIAS 12
4 SISTEMA DE GESTIÓN EN SEGURIDAD DE LA INFORMACION SGSI 12
4.1 CONTEXTO DE LA ENTIDAD 12
4.1.1 CONTEXTO INTERNO 14
4.1.2 CONTEXTO EXTERNO 17
4.1.3 ANÁLISIS DOFA 20
4.2 PARTES INTERESADAS 21
4.3 POLITICA DE ALTO NIVEL DEL SGSI 22
4.4 OBJETIVOS DE SEGURIDAD DE LA INFORMACION 22
4.5 ALCANCE DEL SGSI 23
4.5.1 INTERFACES Y DEPENDENCIAS DEL SGSI 24
4.6 GESTIÓN DE RIESGOS 25

4.7 DECLARACION DE APLICABILIDAD 25
4.8 ORGANIZACIÓN DEL SGSI 26
4.9 AUTORIDADES, ROLES Y RESPONSABILIDADES 27
4.9.1 AUTORIDADES DE SEGURIDAD DE LA INFORMACIÓN 27
4.9.2 ROLES DE SEGURIDAD DE LA INFORMACIÓN 32
4.9.3 RESPONSABILIDADES DE OTRAS DEPENDENCIAS U OFICINAS 33
4.9.3.1 OFICINA TECNOLOGÍAS DE LA INFORMACIÓN 33
4.9.3.2 SUBGERENCIA ADMINISTRATIVA Y FINANCIERA 34
4.9.3.3 OFICINA ASESORA JURIDICA 38
4.9.3.4 OFICINA ASESORA DE PLANEACIÒN 39
4.9.3.5 OFICINA DE CONTROL INTERNO 39
4.9.3.6 OFICINA ASESORA DE COMUNICACIONES 39
5 FORMACIÓN y CAPACITACIÓN 40
5.1 INFORMACIÓN DOCUMENTADA 40
5.2 MANTENIMIENTO Y MEJORA DEL SGSI 41
5.2.1 MEDICIÓN DE LA EFICACIA DEL SGSI 41
5.2.2 AUDITORIA INTERNA 41
5.2.3 REVISIÓN POR LA DIRECCIÓN 41
5.2.4 MEJORA DEL SGSI 42
6 FORMAS 42
7 ANEXOS 42
7.1 INDICE DE ILUSTRACIONES 42
7.2 INDICE DE TABLAS 42

OBJETIVO

Presentar el Manual del SGSI, el cual es el documento que inspira y dirige el modelo del Sistema de Gestión de Seguridad de la Información, en adelante SGSI, adoptado por el INSTITUTO COLOMBIANO AGROPECUARIO, en adelante ICA; este documento expone y determina las intenciones, el alcance, los objetivos, las responsabilidades, las políticas y las directrices principales en relación a seguridad de la información, mantenimiento y mejora del SGSI enmarcado en el ciclo de mejoramiento continuo PHVA (planear, hacer, verificar y actuar).

1 GENERALIDADES

En pro de aportar al cumplimiento de los objetivos estratégicos del ICA, en el propósito específico de la entidad de "Lograr el Sistema Integrado de Gestión"[1], el presente Manual del SGSI es parte integral del Manual del Sistema de Gestión DIR-MEJ-MSG-001.

El Manual del SGSI inicia con el conocimiento de la entidad y la descripción de su contexto en términos de seguridad de la información, seguido de la definición de la política y objetivos de seguridad de la información y el establecimiento de los límites del SGSI; y concluye con la descripción de procedimientos, metodologías, estructura organizacional, roles y responsabilidades para el establecimiento, implementación, operación, supervisión y mantenimiento del SGSI de conformidad con el enfoque del ciclo de mejoramiento continuo PHVA, la NTC/ISO 27001:2013 y los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI y Política de Gobierno Digital.

1.1 APLICACIÓN

El alcance del presente Manual del SGSI aplica a todos los procesos de la entidad.

1.2 DEFINICIONES

Consultar Glosario de términos del sistema de Gestión de Seguridad de la Información.

1.3 NORMAS APLICABLES

- NTC/ISO 27001:2013
- NTC/ISO 27005:2009
- GTC/ISO 27002:2015
- NTC-ISO 31000:2011
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI y Política de Gobierno Digital.

[1] **Fuente**: Plan Estratégico Institucional 2016-2022

2 INTRODUCCIÓN

La Política de Gobierno Digital en Colombia, ha venido siendo implementado de manera sistemática y coordinada en todas las entidades públicas. En los últimos años, se han evidenciado cambios y avances en el uso y apropiación de la tecnología como herramienta que permite mejorar la gestión pública, la provisión de servicios y la transparencia, encaminados a cumplir las funciones del Estado (Salas, 2011).

El ICA, como entidad pública de orden nacional, adscrita al Ministerio de Agricultura y Desarrollo Rural hace parte de las entidades públicas que ha apropiado las iniciativas del Gobierno Nacional y las ha desplegado a todos sus niveles organizacionales, incluyéndolas en los objetivos estratégicos de la entidad y haciéndolas parte fundamental del Plan Estratégico Institucional.

En el desarrollo de sus funciones, el ICA diseña, desarrolla y ejecuta estrategias para prevenir, controlar y reducir riesgos sanitarios, biológicos y químicos para las especies animales y vegetales, que pueden afectar la producción agropecuaria, forestal, pesquera y acuícola de Colombia.

Sus acciones se orientan no solo a lograr una producción agropecuaria competitiva, con el fin de aportar al logro de los objetivos de la Apuesta Exportadora de Colombia sino a realizar inspección y control de productos agropecuarios, animales y vegetales, en los pasos fronterizos, aeropuertos y puertos.

El ICA es responsable de las negociaciones de acuerdos sanitarios y fitosanitarios bilaterales o multilaterales que permite la comercialización de los productos agropecuarios. No obstante, el ICA tiene la responsabilidad de garantizar la calidad de los insumos agrícolas y las semillas que se usan en Colombia, al tiempo que reglamenta y controla el uso de organismos vivos modificados por ingeniería genética para el sector agropecuario[2].

Dicho lo anterior, el ICA reconoce su importancia para el sector agrícola y ha identificado la *información* como uno de los activos más importantes y críticos para el desarrollo de sus funciones. En la gestión de los procesos estratégicos, misionales, apoyo y de evaluación, continuamente se está procesando, gestionando, almacenando, custodiando, transfiriendo e intercambiando información valiosa que puede ir desde un dato personal hasta secretos empresariales que no deben ser divulgados a personal no autorizado, porque pueden poner en riesgo hasta las importaciones y exportaciones del país.

En atención a lo anterior, la entidad asumió el reto de implementar el SGSI, siguiendo los lineamientos del MSPI de la Política de Gobierno Digital, a su vez reglamentado a través de lo contenido en el título 9 del Decreto 1078 de 2015 para el sector de tecnologías de la información y comunicaciones.

[2] **Fuente**: Portafolio de Servicios ICA

La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, así como para mantener el cumplimiento normativo y regulatorio aplicable a la entidad, además traslada confianza a las partes interesadas.

Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada. Por lo anterior, el SGSI del ICA adopta una metodología para la identificación y valoración de los activos de información, y una metodología para la evaluación y tratamiento de los riesgos; siendo éste el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto para la entidad y las partes interesadas.

Así mismo, el SGSI del ICA define políticas y procedimientos eficaces y coherentes con la estrategia de la entidad, como desarrollo de los controles adoptados para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, a través del establecimiento de indicadores que aseguran la eficacia de los controles; apoyado en los programas de auditoria y la revisión por la dirección, que concluyen en la identificación de oportunidades de mejora las cuales son gestionadas para mantener la mejora continua del SGSI.

Lo anterior se complementa con los programas de formación y transferencia de conocimiento en seguridad de la información y las campañas de sensibilización que se lideran al interior de la entidad.

Así pues, la entidad expone a través de este manual el modelo del SGSI adoptado por el ICA de acuerdo al ciclo PHVA (planear, hacer, verificar y actuar), con el propósito de cumplir con el marco normativo, la misión fijada y la visión trazada. Dicho manual describe las disposiciones acogidas por la entidad para establecer el contexto, las políticas, los objetivos, el alcance, los procedimientos, las metodologías, los roles, las responsabilidades y las autoridades del SGSI; de acuerdo con los requisitos legales, los contractuales y los normativos, que le aplican a la entidad, en el marco de seguridad de la información.

Para tal fin, la entidad ha adoptado los lineamientos normativos de: la NTC/ISO 27001:2013, la cual establece los requisitos para la implementación del SGSI, la NTC/ISO 31000:2011 que proporciona el esquema para la gestión de riesgos y las mejores prácticas, tales como ISO 27002:2015, ISO 27005:2009, entre otras; buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas de las partes interesadas.

2.1 MISIÓN[3]

"Trabajamos por la sanidad agropecuaria y la inocuidad agroalimentaria del campo colombiano."

[3] **Fuente**: Plan Estratégico Institucional 2016-2022

2.2 VISIÓN[4]

"Para el año 2022 el ICA incrementará su reconocimiento como autoridad sanitaria y de inocuidad agroalimentaria, en el ámbito nacional e internacional."

2.3 ESTRUCTURA ORGANIZACIONAL

A continuación, se presenta la estructura organizacional definida por el ICA de acuerdo al Decreto 4765 de 2008 y Decreto 3761 de 2009.

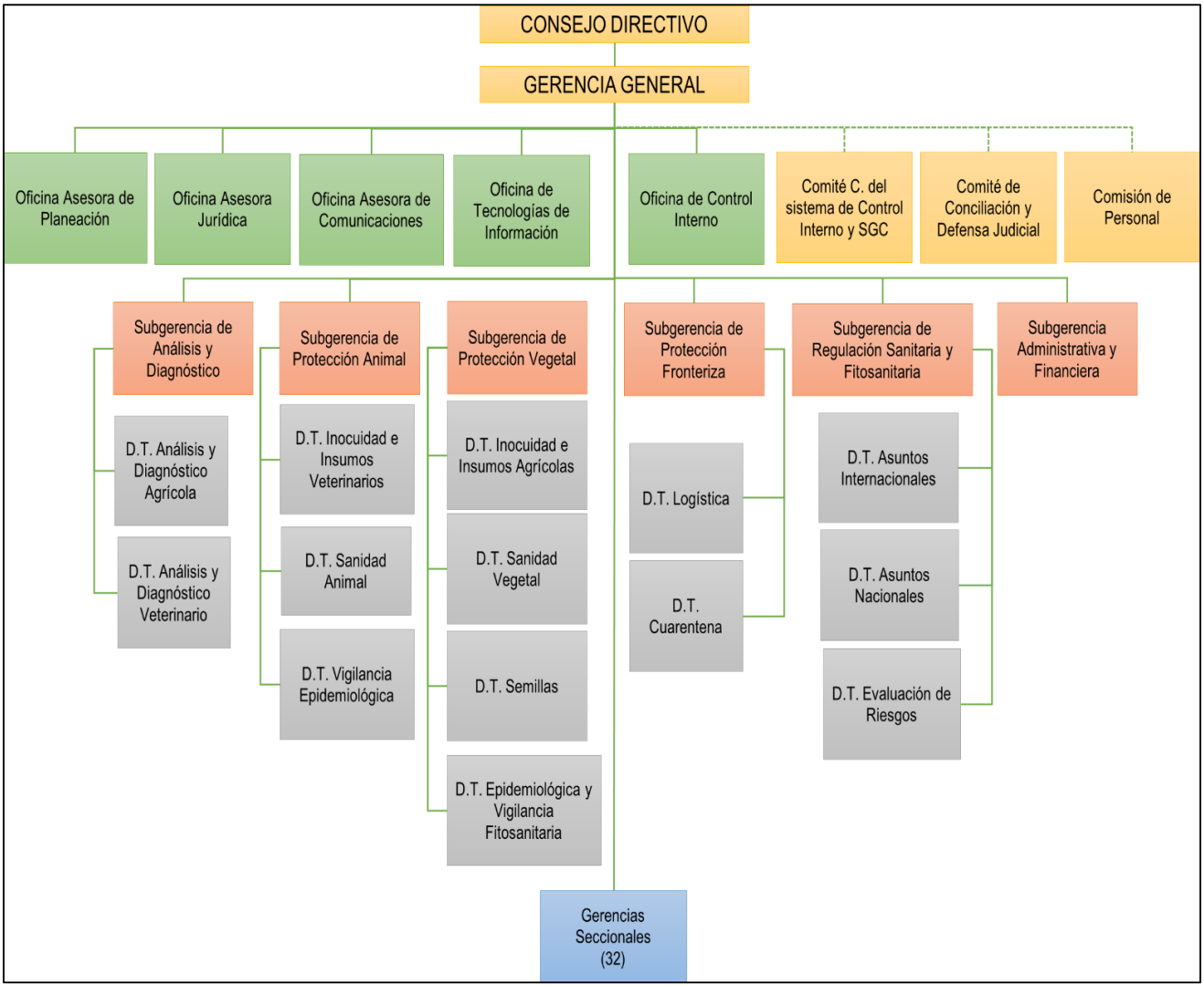


Ilustración 1. Organigrama ICA

[4] **Fuente**: Plan Estratégico Institucional 2016-2022

3 MODELO SISTEMA DE GESTION EN SEGURIDAD DE LA INFORMACIÓN SGSI

A continuación, se ilustra el modelo del SGSI adoptado por la entidad.

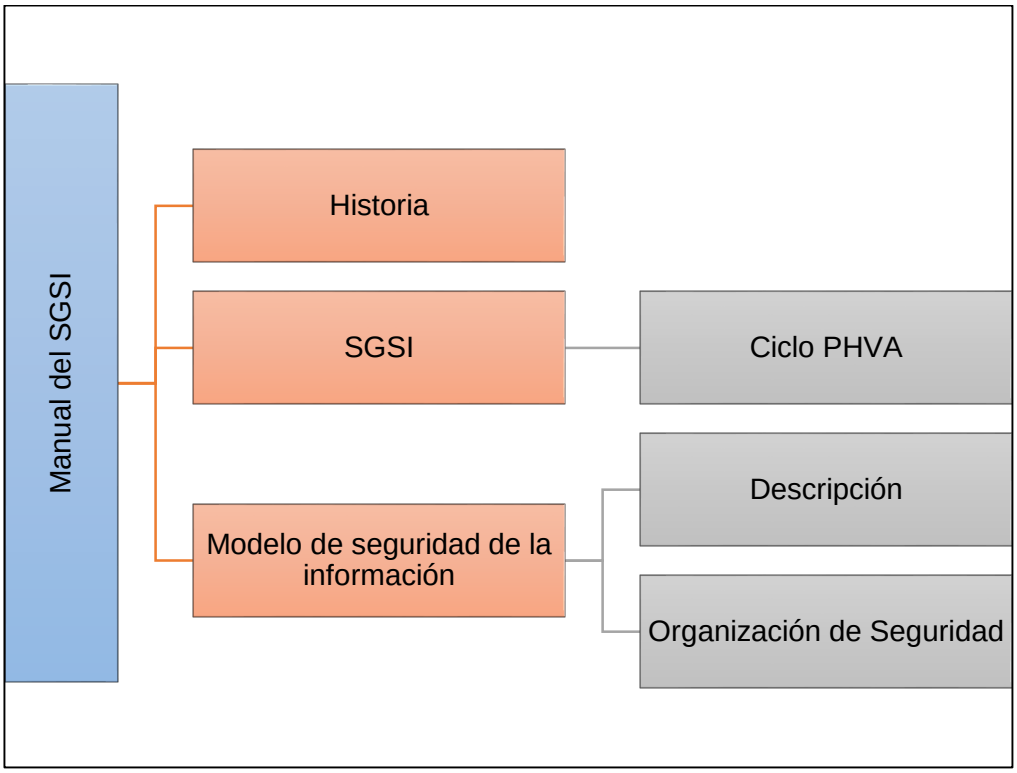


Ilustración 2. Modelo de seguridad de la información

3.1 HISTORIA Y SGSI

En la actualidad y de acuerdo con la expedición lo establecido en el título 9 del Decreto Único Reglamentario 1078 de 2015 del sector de Tecnologías de la información y las Comunicaciones; el ICA trabaja permanentemente en pos de implementar el SGSI siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI y la Política de Gobierno Digital, con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante la adecuada gestión del riesgo, la aplicación de la normatividad vigente y la implementación de mejores prácticas relacionadas con seguridad de la información.

En efecto, el modelo del SGSI del ICA se encuentra basado en el ciclo de mejoramiento continuo PHVA (Planear, hacer, actuar y verificar), el cual asegura que el SGSI esté expuesto a revisiones continuas cuando existe un cambio importante en la infraestructura o se requiera mejorar su efectividad dependiendo de las mediciones de parámetros claves de su operación. Se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.

A continuación, se enlistan los componentes de cada una de estas fases del ciclo:

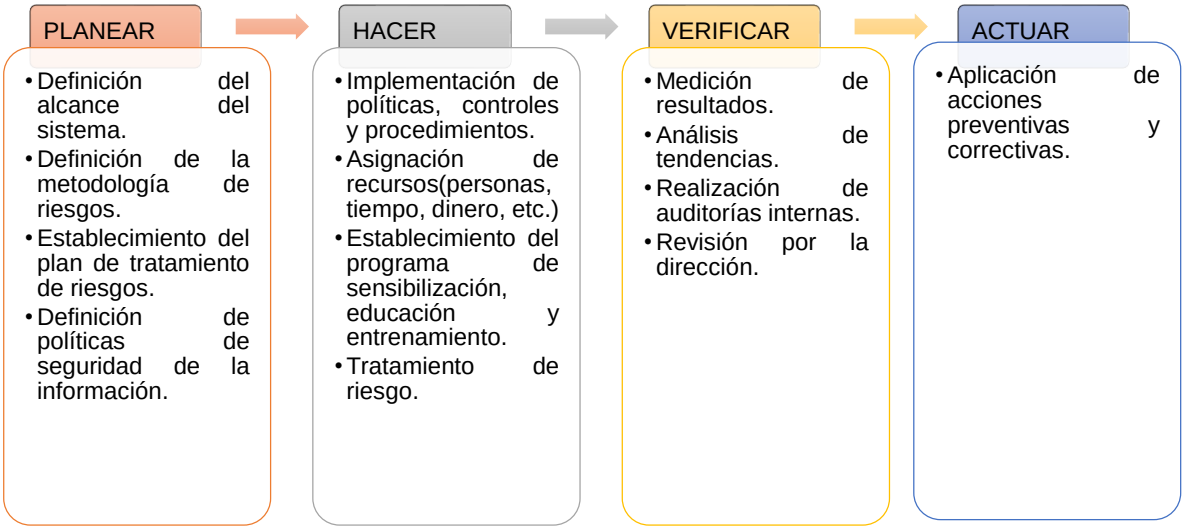


Ilustración 3. Fases del ciclo PHVA

3.2 DESCRIPCIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN

En el ámbito de Seguridad de la información, los componentes del sistema se ubican en diferentes niveles de acuerdo a su importancia, a continuación, se ilustran dichos componentes:

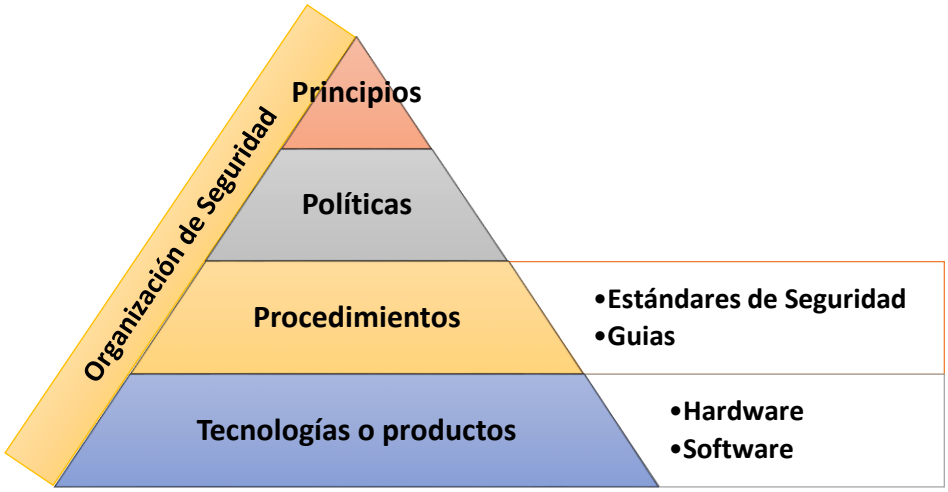


Ilustración 4. SGSI desde la perspectiva de sus componentes

3.3 PRINCIPIOS

Los principios son el soporte de la visión, la misión, la estrategia y los objetivos estratégicos de la entidad. En el marco de la seguridad de la información se exponen a continuación:

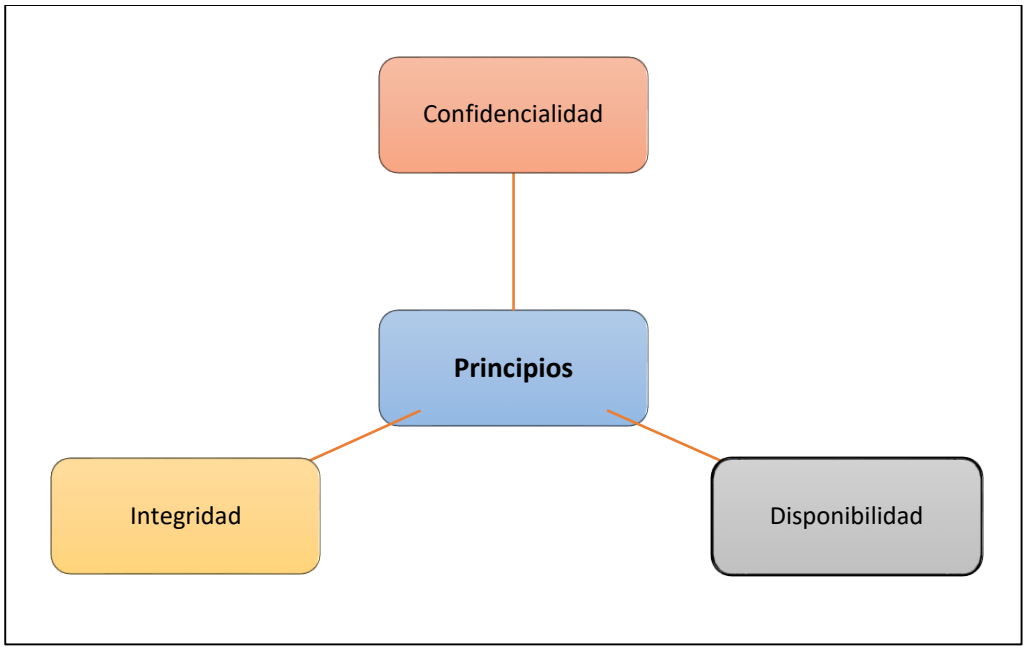


Ilustración 5. Principios de seguridad de la información

- La información es uno de los activos más importantes del ICA y, por lo tanto, se espera que sea utilizada acorde con los requerimientos de la entidad.
- La confidencialidad de la información de la entidad y de terceras partes debe ser mantenida, independientemente del medio o formato donde se encuentre.
- La información de la entidad debe preservar su integridad independientemente de su residencia temporal o permanente, o la forma en que sea transmitida.
- La información de la entidad debe estar disponible cuando sea requerida.

3.4 POLITICAS

Las políticas de seguridad de la información del ICA tienen por objetivo general asegurar que la información sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones (Confidencialidad); que esté protegida contra modificaciones no planeadas, realizadas con o sin intención (Integridad), que esté disponible cuando sea requerida (Disponibilidad) y que sea utilizada para los propósitos que fue obtenida (Privacidad).

Los objetivos específicos que persiguen las Políticas de Seguridad de la Información son:

- Establecer los fundamentos para el desarrollo y la implantación del SGSI.
- Definir la conducta a seguir en lo relacionado con el acceso, uso, manejo y administración de los recursos de información.
- Establecer y comunicar la responsabilidad en el uso de los activos de información, que soportan los procesos y sistemas del negocio.
- Administrar los riesgos en seguridad de la información.
- Establecer los canales de comunicación que le permitan a la Alta dirección mantenerse informada de los riesgos y uso inadecuado de los activos de información, y las acciones tomadas para su mitigación y corrección.
- Proteger la imagen, los intereses y el buen nombre del ICA.

Así pues, las políticas del SGSI se constituyen como directrices establecidas por el Líder u Oficial de Seguridad de la información y aprobadas por el Comité de Coordinación del Sistema de Control Interno y del Sistema integrado de Gestión, cuyo objetivo es orientar a los Funcionarios, Contratistas, Proveedores y/o Terceros, en el uso adecuado de la información y los recursos tecnológicos para mantener la confidencialidad, integridad y disponibilidad de estos. En efecto, las políticas para el ICA están documentas y establecidas en la Política de seguridad de seguridad y privacidad de la información[5].

3.5 PROCEDIMIENTOS

Los procedimientos de Seguridad de la Información se apoyan en la Política de seguridad y privacidad de la información. Estos documentos describen en forma específica una actividad o un proceso, Para crear o modificar documentos se sigue lo descrito en el Procedimiento Control de Documentos GIT-GCD-P-001.

3.6 ESTÁNDARES

Los estándares de seguridad se utilizan para mantener los diferentes componentes del SGSI con unas directrices normalizadas de seguridad. Esto permite establecer una línea base la cual da los parámetros básicos de seguridad y de ahí en adelante, dependiendo de los requisitos de los servicios, se habilitan estos servicios o protocolos.

[5] Ver Manual de Políticas de seguridad de la información del ICA

3.7 GUIAS

Documentos que tienen por objetivo y fin el conducir, encaminar y dirigir las acciones de seguridad de la información para dar cumplimiento a los principios y políticas definidas por el ICA.

No.	Guías
1.	Guía de Uso aceptable de activos.

4 SISTEMA DE GESTIÓN EN SEGURIDAD DE LA INFORMACION SGSI

4.1 CONTEXTO DE LA ENTIDAD

El ICA, es una entidad pública de orden nacional, adscrita al Ministerio de Agricultura y Desarrollo Rural, con personería jurídica, autónoma, administrativa y patrimonio independiente, creada en 1962 mediante el Decreto 1562 y reestructurada mediante los Decretos 4765 de 2008 y Decreto 3761 de 2009, los cuales establecen su naturaleza, objetivos, funciones y planta de personal, entre otras disposiciones.

La ley 101 de 1993, Ley general de Desarrollo Agropecuario y Pesquero, en su Artículo 65, define su ámbito de acción estableciendo su especialización en la protección sanitaria agropecuaria.

El Decreto 1840 de 1994 reglamenta el mencionado artículo y constituye el marco general de la sanidad agropecuaria en el país, establece la responsabilidad del ICA, sus atributos y funciones en materia de sanidad agropecuaria, control de insumos agropecuarios, de recursos genéticos y semillas, así como crea el Sistema Nacional de Protección Agropecuaria (SINPAGRO).

El ICA cuenta con treinta y dos (32) Gerencias Seccionales, así como con un número importante de oficinas locales ubicadas en distintos municipios del país, que le permiten cubrir un amplio espectro del territorio nacional y acercar a los clientes y/o usuarios, sus productos y servicios.

El ICA no solo diseña y ejecuta estrategias para prevenir, controlar y reducir riesgos que puedan afectar la producción agropecuaria en Colombia, también es responsable de las negociaciones de acuerdos zoosanitarios y fitosanitarios bilaterales o multilaterales, que permiten la comercialización de los productos agropecuarios en el exterior y sus acciones se orientan a lograr una producción agropecuaria competitiva, con el fin de aportar al logro de los objetivos de la apuesta exportadora de Colombia.[6]

[6] **Fuente**: Manual del Sistema de Gestión DIR-MEJ-MSG-001

En efecto, el ICA reconoce que la información es uno de los activos más importantes para cumplir las funciones y objetivos que le han sido delegados por el Gobierno Nacional, de ahí la importancia de realizar un análisis del contexto interno y externo de la entidad, con relación a seguridad de la información, para identificar cuáles son los riesgos que pueden o afectan su capacidad para lograr los resultados esperados frente al SGSI; así como identificar cuáles son las necesidades y expectativas de las parte interesadas.

A continuación, se detallan los diferentes actores que hacen parte del contexto interno y externo de la entidad.

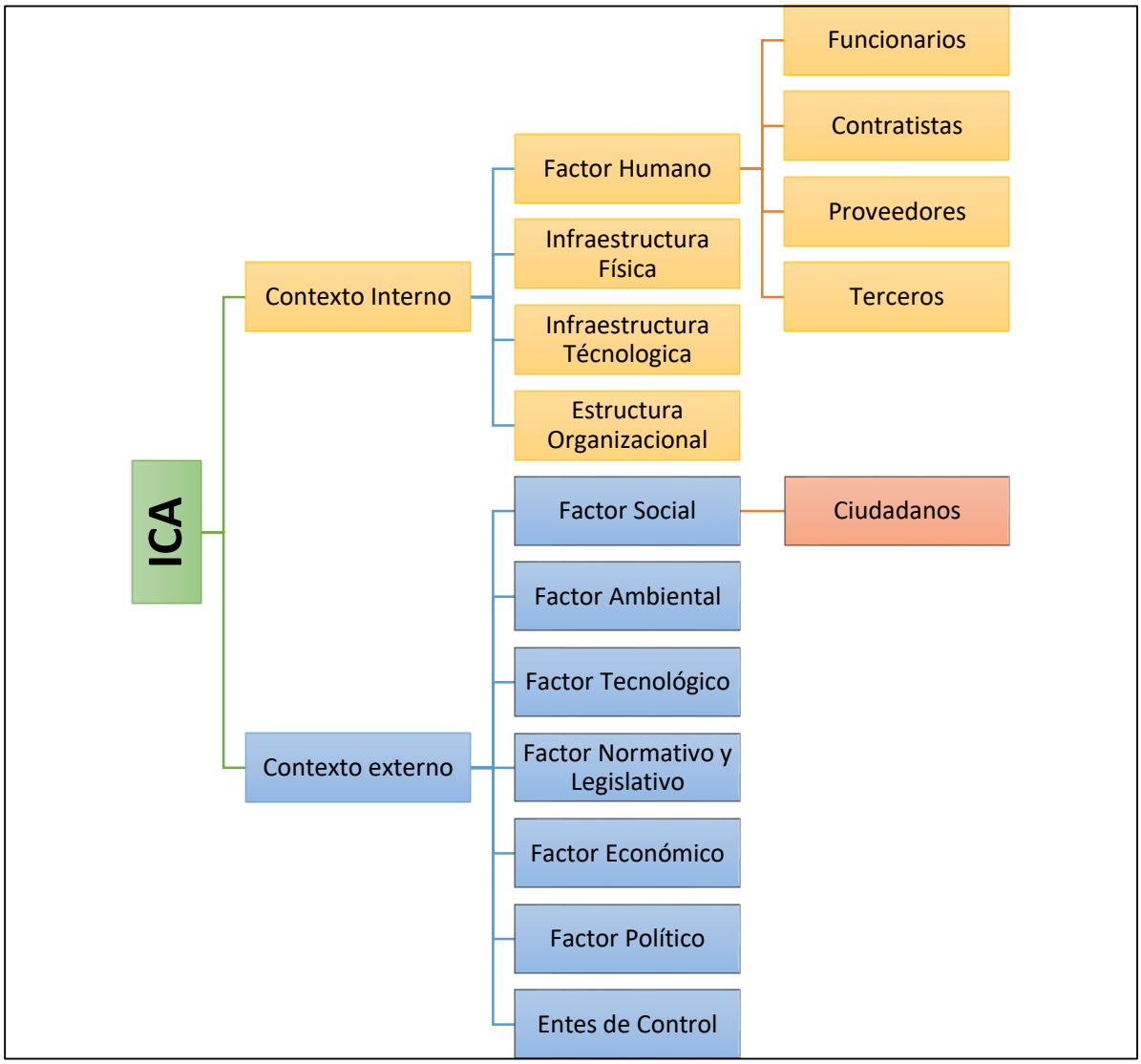


Ilustración 6. Contexto interno y externo de ICA

4.1.1 CONTEXTO INTERNO

- **Factor Humano**

  Las personas también hacen parte de los activos de información más importantes dentro de la entidad. En el ICA se encuentran representados en Funcionarios, Contratistas, Proveedores y/o Terceros, que continuamente se encuentran en interacción con los procesos de la entidad, y, por ende, gestionan, procesan, almacenan, distribuyen, intercambian y/o consultan información que puede ser reservada, sensible o interna. Por lo anterior, el factor humano representa una gran influencia para el cumplimiento de los lineamientos y las políticas de seguridad y privacidad de la información que ha establecido la entidad para minimizar el riesgo que de alguna manera las personas representan para el SGSI; situación que continuamente el ICA prevé a través de comunicados, programas de sensibilización y transferencia de conocimiento con relación a la seguridad de la información.

  a) Funcionarios: Es una persona que desempeña un empleo público. Se trata de un trabajador que cumple con funciones en el organismo del estado.

  b) Contratista: Persona natural o jurídica que se vincula a la entidad con el objeto de prestar al instituto un servicio determinado.

  c) Proveedores: Persona natural o jurídica con la que tiene un vínculo de contratación con la entidad, para la ejecución de un objeto el cual es prestar un bien o servicio determinado.

  d) Tercero: Persona natural o jurídica que a través de un convenio ejecuta un servicio determinado (p.e. pasantes).

- **Infraestructura Física**

  La oficina nacional del ICA, ubicada en Bogotá cuenta con unas instalaciones en arriendo, operando en los pisos 2, 6, 7, 8, 9, 10 y sótano 1, dichas oficinas cumplen con controles de seguridad para acceder a la misma, se exige porte del carnet institucional para los Funcionarios, Contratistas, Proveedores y/o Terceros.

  Para el registro de ingreso para visitantes se debe hacer en la recepción del segundo piso, donde deben presentar documento de identificación e indicar a que piso van y con quien es su reunión, con el fin de validar su ingreso y proceder a entrega de tarjeta de acceso al piso a visitar en la entidad.

  Cuando se ingresen dispositivos tecnológicos se debe:

  a. Los Funcionarios, Contratistas, Proveedores y/o Terceros; deben ser registrado en la bitácora de cada recepción del piso donde van a desarrollan sus actividades.

b. Los visitantes deberán registrarlos en la recepción del piso 2 y en la recepción del piso al cual se van a dirigir.

c. En cada uno de los pisos donde opera el ICA se cuenta con:
   - ✓ Áreas seguras.
   - ✓ Sistemas de detección y extinción de incendios.
   - ✓ Áreas de evacuación.
   - ✓ Señalización de áreas.
   - ✓ El edificio cuenta con cuatro (4) ascensores.

d. Para ingresar a los centros de cableado de cada piso, lo realiza únicamente el personal autorizado con el uso de llaves y tarjeta de proximidad; o si se requiere que un proveedor debe ingresar este debe ser estrictamente a acompañado por el personal autorizado del ICA durante su visita.

e. Para el ingreso al Datacenter, lo realiza personal autorizado con el uso de sistemas biométricos y de proximidad; o si se requiere que un proveedor debe ingresar este debe ser estrictamente a acompañado por el personal autorizado del ICA durante su visita.

- **Infraestructura Tecnológica**

  El ICA cuenta con dos (2) DATACENTER, el primero se encuentra ubicado en las instalaciones de las Oficinas Nacionales Bogotá piso 6 y soporta toda la gestión tecnológica a Nivel Nacional.

  Desde el Datacenter de Oficinas nacionales, se prestan los servicios de la operación de la entidad soportadas en TI, solamente ingresa personal autorizado a través de un sistema biométrico, adicionalmente cuenta con:

  a. Sistemas de detección y extinción de incendios.

  b. Se encuentran independientes los racks de servidores, cableado y UPS.

  c. Cada rack de servidores cuenta con la seguridad por medio de llaves y el acceso se realiza si es estrictamente necesario.

  d. La gestión de los servidores se hace remota a través de los esquemas de protección definida en las políticas de seguridad y privacidad de la información.

  El Datacenter alterno está ubicado en otra zona de Bogotá, fuera de los límites de las oficinas nacionales. Este Datacenter soporta los servicios de misión crítica y opera bajo un acuerdo marco de precios de Centro de Datos Nube Privada.

- **Estructura Organizacional**

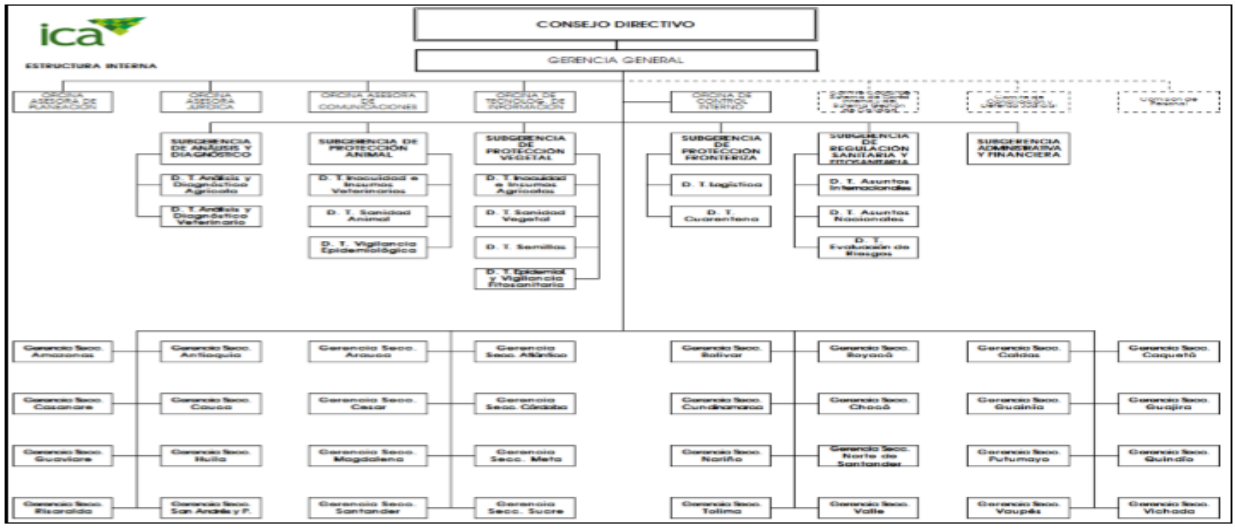
El Instituto está compuesto por:

a) Una Gerencia General que le rinde cuentas a un Consejo Directivo conformado por 7 consejeros, un representante del Presidente de la República, el Director Nacional de Planeación, el Ministro de Agricultura, el Director de Colciencias, el Director de Fedegan, el Presidente de la Sociedad de Agricultores de Colombia - SAC, Presidente de la Asociación Nacional de Usuarios Campesinos de Colombia - ANUC e invitados que tienen voz pero no voto que son el Presidente de Fenavi, PorkColombia, Asocolflores.

b) Cuenta con 3 Oficinas Asesoras, de Planeación, de Comunicaciones y Jurídica, 1 Oficina de Tecnologías de la Información y 1 Oficina de Control Interno. Dependiendo directamente del Gerente General se encuentran 6 Subgerencias 5 de naturaleza técnica: Subgerencia de Protección Animal, Subgerencia de Protección Vegetal, Subgerencia de Protección Fronteriza, Subgerencia de Análisis y Diagnóstico y Subgerencia de Regulación y 1 de carácter administrativo: Subgerencia Administrativa y Financiera. De estas Subgerencias Técnicas se desprenden 14 Direcciones Técnicas tal y como se observa en la imagen.

c) La Subgerencia Administrativa y Financiera cuenta con 11 Grupos de trabajo, que, aunque no aparecen en la estructura dado que no fueron formalizados por el Decreto 4765 de 2008, su creación obedece a la necesidad de la Alta Dirección de definir Roles y Responsabilidades en el marco de la gestión administrativa y financiera e implementar controles relacionados con los temas específicos de índole administrativo.

ESTRUCTURA INTERNA ACTUAL DEL INSTITUTO COLOMBIANO AGROPECUARIO –ICA-



Fuente: ICA, Página Web.

4.1.2 CONTEXTO EXTERNO

- **Factor Social**

  De acuerdo con las normas internacionales, el ICA coordina campañas para el control y la erradicación de enfermedades de control oficial. Cuenta con un sistema de información y vigilancia epidemiológica que realiza las investigaciones de focos y brotes de enfermedad y monitorea permanentemente la condición sanitaria del sector pecuario, la cual es reportada internacionalmente.

  Este esquema ha sido fundamental, para que en el 2009 Colombia fuera reconocida por la Organización Mundial de Sanidad Animal como país libre de fiebre aftosa con vacunación y en el 2017 se recertifico.

  Como resultado de esta labor, se ha mejorado el status sanitario del país en materia de enfermedades de control oficial lo que permite facilitar la admisibilidad de los animales y sus productos a mercados priorizados de manera conjunta con el sector privado.[7]

  Éste es tan solo un ejemplo del impacto social positivo que genera la gestión del ICA para el país, de ahí el interés de la entidad por proteger la información, que, utilizada de una manera adecuada, mejora la calidad de vida de los ciudadanos.

  a. Ciudadanos: Son las personas a las cuales se le ofrecen los servicios de la entidad.

- **Factor Ambiental**

  Las instalaciones de Oficinas Nacionales del ICA, están ubicadas en Avenida Calle 26 # 85b – 09 de la localidad de Fontibón.

  Las características ambientales de esta localidad de son las siguientes:

  Datos tomados de CCB Cámara de Comercio de Bogotá (2006).
  La localidad de Fontibón congrega diferentes actividades de tipo industrial, comercial, residencial e institucional que pueden desencadenan problemáticas ambientales y conflictos sociales, lo que redunda en el detrimento de la calidad del ambiente y por ende de la calidad de vida.

  La localidad es una de las dos zonas industriales de la ciudad, en la cual se establecen circuitos productivos que encadenan actividades industriales consideradas de alto impacto ambiental.

  Fontibón tiene una estructura empresarial especializada en el sector de los servicios (76%), la industria (18%) y la construcción (4%). La mayor participación de los servicios se explicó por el número de empresas dedicadas al comercio (38%) que representan el centro de la economía local, y en menor medida por el transporte, almacenamiento

[7] **Fuente**: Portafolio de Servicios ICA

y comunicaciones (11%), los servicios inmobiliarios y de alquiler (10%), la actividad de hoteles y restaurantes (8%) y otros servicios comunitarios (4%).

Según el tamaño de las empresas, se puede afirmar que Fontibón es una localidad de microempresarios. Del total de empresas matriculadas ante la Cámara de Comercio del 2006, 8.846 son microempresas, que representaron el 83% de las empresas establecidas en la localidad y el 4,4% de las de Bogotá. Las pymes (16%) y la gran empresa (1%).

En la localidad se encuentran empresas tan importantes como: Frigorífico Suizo S.A., Multidimensionales S.A., Manufacturas Eliot S.A., Sociedades anónimas en el sector de la industria; ALFA Trading Ltda., Pfizer S.A., Fresenius Medical Care Colombia S.A., y Carulla Vivero S.A., en la actividad de comercio, y Robayo Ferro & Cía. S.C.A., y Riesgos Profesionales Colmena S.A., en la actividad de intermediación financiera. La gestión de estas empresas representa un valioso aporte al desarrollo de la actividad económica y consolido a la localidad como un buen lugar para la ubicación de medianas y grandes empresas de servicios comerciales, financieros e industriales.

La mayor proporción de las empresas de Fontibón se localiza en la zona centro de la localidad, cerca del aeropuerto internacional El Dorado. Por su concentración empresarial se destacaron los barrios Fontibón Centro, Santa Cecilia, Predio Caldas, Modelia Occidental, La Esperanza Norte, Ciudad Salitre Occidental, Villemar Fontibón, Montevideo, San José Fontibón, La Esperanza, El Tintal y Los Alamos.

En consecuencia, las oficinas nacionales del ICA en Bogotá se encuentran rodeadas de diferentes industrias cuyos residuos pueden afectar las condiciones ambientales del sector y por ende la disponibilidad de Oficinas Nacionales ICA.

- **Factor Tecnológico**

  El ICA como entidad pública del orden nacional, debe implementar, de manera sistemática y coordinada, la Política de Gobierno Digital, la cual es una estrategia del Gobierno Nacional liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones que contribuye con la construcción de un Estado más eficiente, más transparente y participativo y que presta mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las TIC.

  En el campo tecnológico, los avances son vertiginosos, no sólo en cuanto a aplicaciones o servicios sino también en lo relacionado con la gestión de la tecnología al interior de las entidades, hecho que ha transformado los procesos y negocios al interior del mismo Estado.

  Por lo anterior, el ICA enfrenta grandes retos encaminados a mantener la seguridad de la información en el desarrollo de las siguientes actividades:

a. Planear y conceptualizar soluciones tecnológicas encaminadas a la prestación de servicios de la Política de Gobierno Digital.

b. Culminar la implementación de las cadenas de trámites y sistemas transversales diseñados.

c. Realizar desarrollo / mantenimiento a las soluciones tecnológicas operadas por el Programa.

d. Diseñar, desarrollar e implementar soluciones tecnológicas encaminadas a la prestación de servicios de Gobierno Digital.

e. Proveer dentro de un modelo estándar, los servicios de las soluciones tecnológicas operadas por el Programa (Salas, 2011).

- **Factor Normativo y Legislativo**
  El ICA, como Entidad Pública dispone de un marco normativo y regulatorio basado en las recomendaciones de las normas internacionales y normativas legales vigentes. Las normas, leyes, decretos y resoluciones, etc. que se han tenido en cuenta para la implementación del SGSI se encuentran identificadas y documentadas en el Normograma[8].

- **Factor Económico**
  Para el ICA, un aspecto que le genera un gran impacto es la asignación del presupuesto para la inversión (Aspecto Misional) y el funcionamiento de la entidad, debido a la problemática interna que enfrenta el país, puede disminuir esta asignación presupuestal emitida por el Ministerio de Hacienda la cual tiene en consideración algunos aspectos como: la globalización, materia de proceso de paz, tratado de libre comercio, deuda externa, el alza de las diferentes monedas como (Euro y Dólar), entre otros.

- **Factor Político[9]**
  A nivel político, el ICA identifica como oportunidades el posconflicto y los TLC`S y acuerdos comerciales que beneficien al sector. Por el contrario, encuentra como amenazas las siguientes:

  a. Prioridad del gobierno nacional hacia otros sectores empresariales; Ejemplo: Minero – Energético.
  b. Cierre de mercados internacionales por razones sanitarias y fitosanitarias.
  c. Traslado de funciones/misiones a otras entidades del estado o privadas.

[8] Ver Normograma de Seguridad de la Información de la entidad.
[9] **Fuente**: Plan Estratégico Institucional 2016-2022

d. Negociación de una reforma agropecuaria en el marco de los acuerdos de paz.
e. Falta de incentivos tributarios al sector.
f. Incentivos al Agro de países competidores en los mercados mundiales.

Para contrarrestar lo anterior, el ICA considera que uno de sus mayores diferenciadores, es sin duda alguna la implementación de la Política de Gobierno Digital y del Sistema Gestión de Seguridad de la Información "SGSI" que promueve la confidencialidad, Integridad y Disponibilidad de la Información para los Clientes Internos (Funcionarios, Contratistas, Proveedores y/o Terceros) y Externos (Entidades, agremiaciones, etc.).

- **Entes de Control**

El ICA y sus activos de información están continuamente expuestos a revisiones por parte de los entes de control y seguimiento; la entidad encuentra en el SGSI un mecanismo de control que le permite mantener la confidencialidad, integridad y sobre todo la disponibilidad de dichos activos para responder oportuna y eficazmente las solicitudes de los entes de control.

Entre las entidades de control y seguimiento se encuentran:
a) Contraloría General de la Nación.
b) Ministerio de Agricultura y Desarrollo Rural.
c) Ministerio de Hacienda y Crédito Público.
d) Procuraduría General de la Nación.
e) Contaduría General de la Nación.

4.1.3 ANÁLISIS DOFA

Luego de identificar los actores internos y externos, a continuación, se presenta el análisis DOFA (debilidades, oportunidades, fortalezas y amenazas) identificado por la entidad con relación a la seguridad de la información.

	Componentes Internos		Componentes Externos	
	Fortalezas		**Oportunidades**	
Factor Positivo	F1.	Personal altamente calificado, rigurosidad técnica y con habilidades de liderazgo.	O1.	Aprender de los incidentes conocidos ocurridos en otras Entidades y Organizaciones.
	F2.	Programas de sensibilización y transferencia de conocimiento actualizados e implementados.	O2.	Mantener comunicación activa con Organismos o Entidades Externas frente a temas de Seguridad que permite ampliar el panorama y la visión para la Entidad.
	F3.	Se cuenta con Sistemas de Gestión Integrados, que permite comunicar varios procesos y hacerlos parte integral del mismo.	O3.	Lograr que los objetivos de la Entidad se cumplan con un alto nivel de Seguridad en el manejo de la Información.

	Componentes Internos		Componentes Externos	
	Fortalezas		**Oportunidades**	
	F4. F5.	Implementación del SGSI que promueve la confidencialidad, Integridad y Disponibilidad de la información para los clientes internos (Funcionarios, Contratistas, Proveedores y/o Terceros) y Externos (Entidades, agremiaciones, etc.). Se cuenta con dos (2) Datacenter, en ubicaciones diferente; uno en las instalaciones de las Oficinas Nacionales y otro alterno.	O4 O5.	Participar con Entidades Públicas en pro de fortalecer la apropiación de la Cultura del SGSI. Realizar renovación de la Plataforma Tecnológica para mantener la Confidencialidad, Integridad y disponibilidad de la Información de la Entidad.
	Debilidades		**Amenazas**	
Factor Negativo	D1.	La entidad debe fortalecer los programas de divulgación y sensibilización a los Funcionarios, Contratistas, Proveedores y/o Terceros, frente al SGSI.	A1.	Apropiarse de los cambios normativos y legislativos vigentes que afecten el SGSI.
	D2.	La entidad carece de seguimiento y monitoreo de los controles implementados para verificar la efectividad y eficacia de los mismos.	A2.	Mantenerse actualizado con las evoluciones tecnológicas.
	D3.	La entidad debe fortalecer el plan de tratamiento de los riesgos que afecten el SGSI.	A3.	Dar cumplimiento a los requisitos de los entes de control.
	D4. D5.	Constante rotación del personal operativo responsable de los procesos. La entidad carece de uso y apropiación del SGSI.	A4. A5.	Dar cumplimiento al Manual del SGSI y a las políticas de seguridad y privacidad de la información. Ataques cibernéticos a las entidades públicas.

Tabla 1. Análisis DOFA

4.2 PARTES INTERESADAS

El ICA reconoce como sus grupos de interés a[10]:

PARTE INTERESADA	DESCRIPCIÓN	NECESIDADES Y EXPECTATIVAS FRENTE A SEGURIDAD DE LA INFORMACION
Usuarios Directos	Funcionarios, productores (ganaderos, agricultores, laboratorios, etc.) exportadores e importadores, comercializadores, transportadores, agentes de	Las partes interesadas esperan del ICA, un manejo responsable de la *información*, que, en el desarrollo de su objeto, ha sido suministrada, gestionada,

[10] **Fuente**: Manual del Sistema de Gestión GMC-GC-MC-001

PARTE INTERESADA	DESCRIPCIÓN	NECESIDADES Y EXPECTATIVAS FRENTE A SEGURIDAD DE LA INFORMACION
	intermediación aduanera y los terceros autorizados.	procesada, almacenada o transferida por la entidad. Adicionalmente las partes interesadas creen en que a través del establecimiento, implementación y mejora continua del SGSI, la entidad asegurará la integridad, disponibilidad y confidencialidad de la información, y el cumplimiento estricto de los requisitos legales, contractuales, regulatorios y normativos.
Usuarios Indirectos	Consumidores, las ONG´s y la ciudadanía.	
Entidades Públicas	Autoridades del sector y entes del Estado.	
Terceros Relacionados	Gremios de la producción, la academia, centros de investigación, Proveedores, Terceros y medios de comunicación.	
Entidades externas	Entidades homologas de otros países y los organismos internacionales de referencia.	

Tabla 2. Partes Interesadas

4.3 POLITICA DE ALTO NIVEL DEL SGSI[11]

Armonizados con el Plan Estratégico Institucional de la Entidad establece como Política de Alto Nivel del Sistema de Gestión de Seguridad de la Información - SGSI, la siguiente:

"La **información** es reconocida por el Instituto Colombiano Agropecuario (ICA) como uno de los activos más importantes para lograr los objetivos de la Entidad, es por eso que se **compromete** a disponer sus recursos tanto físicos, tecnológicos, financieros, informativos, de conocimiento y humanos para liderar y fortalecer la seguridad de la información a través del establecimiento, implementación y **mejora continua** de un Sistema de Gestión de Seguridad de la Información (SGSI); cuyo fin es el aseguramiento de la **integridad**, **disponibilidad** y **confidencialidad** de la información mediante la gestión y tratamiento adecuado de los **riesgos**, en el marco de los **requisitos normativos y legales** de la entidad y por lo tanto; participar activamente en el desarrollo del **Plan de Cultura y Sensibilización** de Seguridad de la Información".

4.4 OBJETIVOS DE SEGURIDAD DE LA INFORMACION

Articulados con la Política de Alto Nivel del Sistema de Gestión de Seguridad de la Información - SGSI, la entidad define como objetivos de seguridad y privacidad de la información los siguientes:

[11] Ver Manual de Políticas de seguridad de la información del ICA

a) Adoptar una Metodología de análisis de riesgos con el fin de identificar, valorar y mitigar los mismo, en pro de prevalecer la Confidencialidad, Integridad y Disponibilidad de la Información.

b) Identificar y valorar los Activos de Información con los que cuenta la entidad, en términos de Confidencialidad, Integridad y Disponibilidad.

c) Divulgar las Políticas de Seguridad y Privacidad de la Información definida a todos Funcionarios, Contratistas, Proveedores y/o Terceros de la Entidad.

d) Controlar y prevenir los incidentes de Seguridad de Información.

e) Desarrollar un Plan de Cultura de Seguridad de Información al interior de la Entidad.

4.5 ALCANCE DEL SGSI

Teniendo en cuenta el análisis del contexto interno y externo y las partes interesadas, el ICA define el alcance de SGSI, en términos de las características de la entidad, su ubicación, sus activos y su tecnología, así:

Alcance: "El Instituto Colombiano Agropecuario -ICA adopta, establece, implementa, opera, verifica y mejora el SGSI para los procesos misionales, apoyo, estratégicos y de evaluación que componen el mapa de procesos de la entidad".

El ICA acorde con su naturaleza jurídica, misión y visión, encontró aplicables todos los requisitos de la NTC/ISO 27001:2013 y todos los controles del Anexo A, de acuerdo a la aplicabilidad y excepciones definidas en la "Declaración de Aplicabilidad".

En la siguiente ilustración se resaltan los procesos que hacen parte del alcance del SGSI.

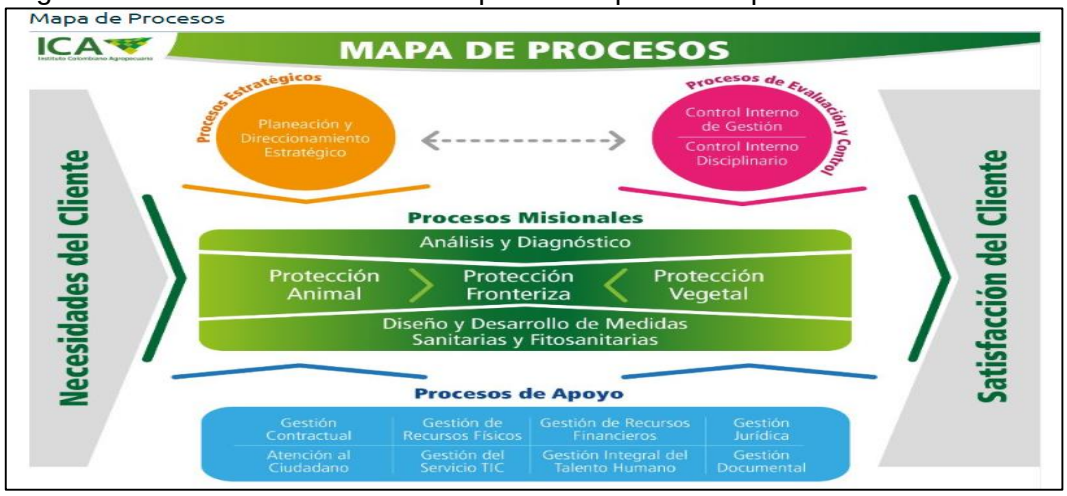


Ilustración 7. Mapa de procesos y alcance del SGSI

4.5.1 INTERFACES Y DEPENDENCIAS DEL SGSI

Con base en las caracterizaciones de los procesos, a continuación, se detallan las interfaces y dependencias que de una u otra manera tienen interacción con los procesos incluidos en el alcance del SGSI:

Tabla 3. Interfaces y dependencias del SGSI[12]

[12] **Fuente**: Caracterizaciones de los procesos incluidos en el alcance del SGSI

4.6 GESTIÓN DE RIESGOS

La metodología adoptada por el ICA para la gestión de riesgos, comprende las siguientes actividades principales: establecimiento del contexto, identificación del riesgo, estimación del riesgo, evaluación del riesgo, tratamiento del riesgo y aceptación del riesgo según la metodología de Gestión de Riesgos utilizada por la entidad.

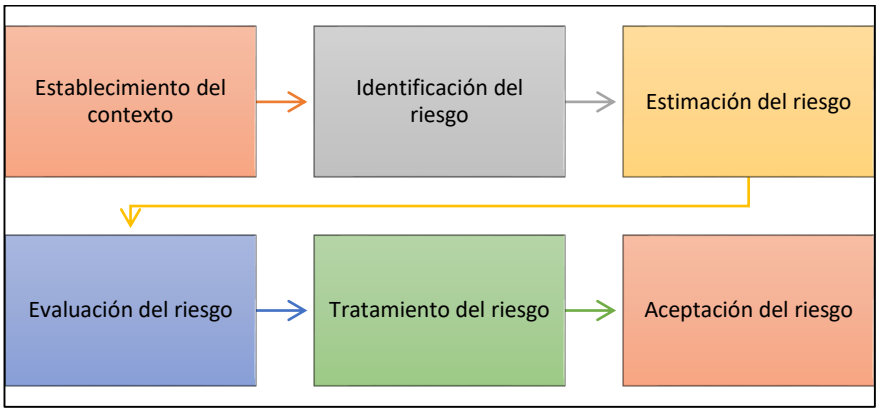


Ilustración 8. Estructura general de la metodología de riesgos

Entre los beneficios de analizar, identificar y tratar adecuadamente los riesgos, se encuentran:

- Aumenta la probabilidad de alcanzar los objetivos.
- Cumple con los requisitos legales y reglamentarios pertinentes y con las normas Internacionales.
- Mejora la prestación del servicio interno y externo.
- Establece una base confiable para la toma de decisiones y la planificación estratégica.
- Mejora los controles existentes.
- Mejora la eficacia y la eficiencia operativa.
- Incrementa el desempeño frente al SGSI.
- Mejora la gestión de incidentes.
- Minimiza las pérdidas.
- Aporta una buena base de conocimiento frente a la solución de incidentes y riesgos[13].

4.7 DECLARACION DE APLICABILIDAD

La declaración de aplicabilidad es un documento basado en el anexo A de la norma ISO 27001:2013 que agrupa 114 controles en 14 dominios. A través de la declaración de aplicabilidad el ICA identifica los controles aplicables que serán implementados como parte del SGSI y sus excepciones., conforme lo indica el Anexo de Declaración de Aplicabilidad.

[13] Ver Metodología para la Gestión de Riesgos del ICA

Elementos que forman parte de la declaración de aplicabilidad:

- Los objetivos de control.
- La aplicabilidad del control.
- La justificación de la inclusión o exclusión.
- Tipo de control
- Los requisitos aplicables[14].

4.8 ORGANIZACIÓN DEL SGSI

Para el diseño, establecimiento, implementación, operación y mejora del SGSI, el ICA adopta el modelo de una organización de tipo centralizada o unidad central, de donde se emite la política de seguridad y privacidad de la información, se asegura el despliegue de las directrices de seguridad a las demás dependencias de la entidad y se monitorea su cumplimiento.

Para tal fin, el ICA ha delegado el liderazgo a la oficina de Tecnologías de la Información, el cual desarrollara a través de los procesos de “Gestión de Gobernabilidad Tics, Gestión de información y del conocimiento tics, Gestión de servicios tics “en cabeza del Jefe de la Oficina de Tecnologías de la información.

A continuación, se ilustra el modelo centralizado adoptado por el ICA, en donde las directrices y políticas son resultado de la participación de las diferentes áreas de la entidad, sin embargo, el poder de decisión está en los procesos Gestión de Gobernabilidad Tics, Gestión de información y del conocimiento tics, Gestión de servicios tics y se despliegan en los demás procesos.

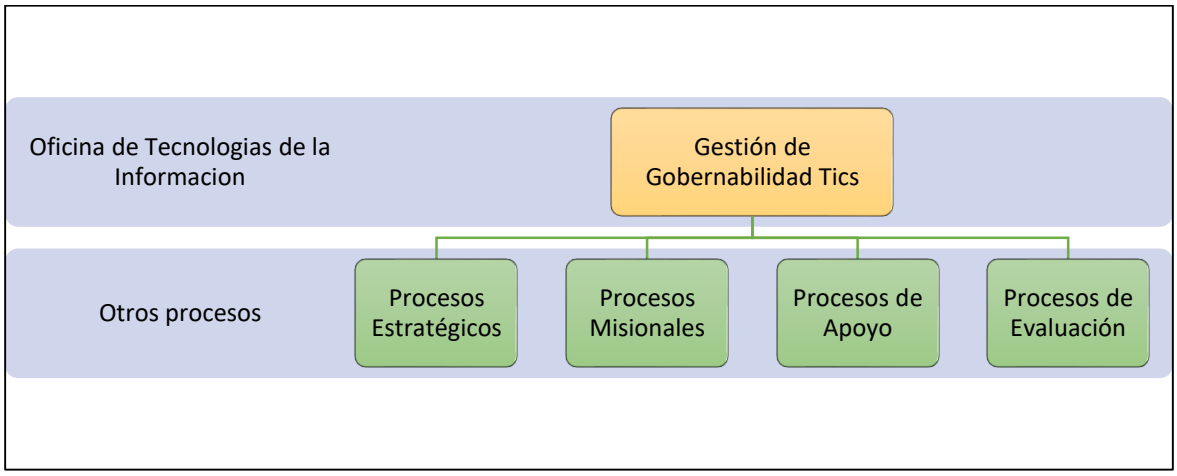


Ilustración 9. Organización Centralizada

[14] Ver Declaración de Aplicabilidad del ICA

4.9 AUTORIDADES, ROLES Y RESPONSABILIDADES

4.9.1 AUTORIDADES DE SEGURIDAD DE LA INFORMACIÓN

- **Consejo Directivo**

  El Consejo Directivo en conjunto con la Gerencia General, apoyan activamente la seguridad de la información dentro de la entidad, definiendo las directrices y lineamientos bajo los cuales debe operar el SGSI; entre sus responsabilidades se encuentran:

  a) Asegurar que el Comité de Coordinación del Sistema de Control Interno y del Sistema de gestión de la calidad[15] contemple todas las funciones de un Comité del SGSI.
  b) Mantener dentro de la planta de personal del ICA, un funcionario que responda al perfil de Líder u Oficial de Seguridad de la información, quien será el encargado gestionar todo lo relacionado con la seguridad de la información en la entidad.
  c) Incluir al Líder u Oficial de Seguridad de la información como uno de los integrantes activos del comité.
  d) Establecer los lineamientos y políticas del SGSI, asegurando su integración con los demás procesos de la entidad, el Plan Estratégico y el Plan Nacional de Desarrollo actual.
  e) Velar por el cumplimiento de la Política de Seguridad y Privacidad de la Información, comprometiéndose para que los Funcionarios, Contratistas, Proveedores y/o Terceros, a su cargo, y partes interesadas conozcan y apliquen los controles de seguridad establecidos.
  f) Asignar a las demás Oficinas, Subgerencias y Gerencias Seccionales del ICA, las responsabilidades asociadas a la seguridad de la información.
  g) Velar para que se ejecute el programa de auditorías internas, al menos una vez al año, y para que se realicen las mejoras correspondientes.
  h) Definir el nivel de tolerancia al riesgo.
  i) Asignar los recursos necesarios para la eficacia del SGSI.

- **Comité de Coordinación del Sistema de Control Interno y del Sistema de gestión de la calidad[16]**

  Para establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI, el Comité debe incluir dentro de sus funciones las siguientes acciones:

  a) Evaluar y aprobar las estrategias y la política de seguridad y privacidad de la información que requiera la entidad de acuerdo con la dinámica y condiciones de la misma.
  b) Fijar directrices institucionales para la aplicación de los mecanismos de protección de seguridad de la información.

[15] Resolución 1361 del 16 de Abril del 2010
[16] Resolución 1361 de 2010

c) Evaluar y aprobar las políticas básicas y específicas de seguridad y privacidad de la información; garantizando su difusión y aplicación en la entidad.
a) Participar en las decisiones sobre arquitecturas y soluciones de seguridad de la información y continuidad del negocio.
b) Evaluar y aprobar Planes de Continuidad de la seguridad de la información que ante una situación crítica pueda verse amenazada de manera parcial o total.
c) Aprobar los programas periódicos de ejercicios y pruebas de la Infraestructura Tecnológica y del negocio.
d) Apoyar la identificación de los procesos críticos de la entidad, así como analizar y proponer soluciones tecnológicas que requiera la misma.
e) Generar y apoyar los planes de socialización, sensibilización y transferencia de conocimiento en los temas relacionados con el SGSI.

- **Líder u Oficial de Seguridad de la Información**

El Jefe de la Oficina de Tecnologías de Información asignará la responsabilidad correspondiente al rol del "Líder u Oficial de Seguridad de la Información" a un servidor público o tercero para efectos de garantizar y liderar la implementación, mantenimiento y mejora del SGSI. El Líder u Oficial de Seguridad de la información actúa bajo las directrices que establezca el Comité de Coordinación del Sistema de Control Interno y del Sistema integrado de G*estión* del ICA, así:

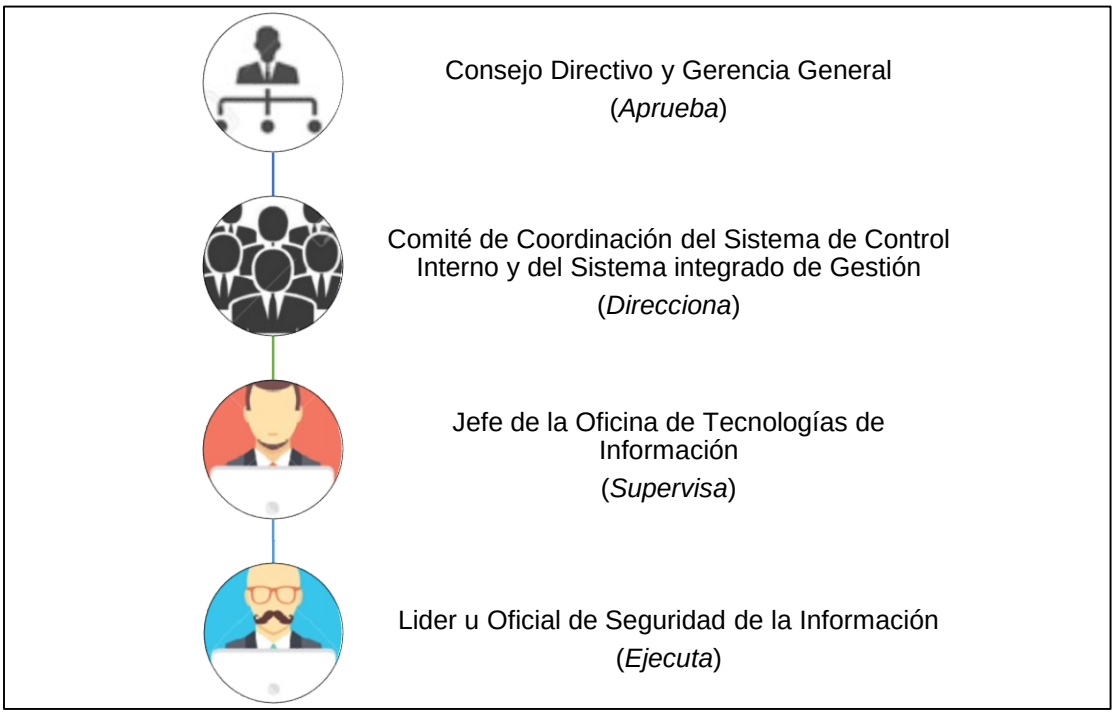


Ilustración 10. Modelo de Operación del Líder u Oficial de Seguridad de la Información

En consecuencia, el Líder u Oficial de Seguridad de la información Planea, diseña e implementa el SGSI de la entidad a través de Políticas, lineamientos, controles, requerimientos legales y buenas prácticas.

Los roles de Lideres de servicios de Tics y Cumplimiento, implementan y validan los lineamientos del Sistema de Gestión de seguridad de la información.

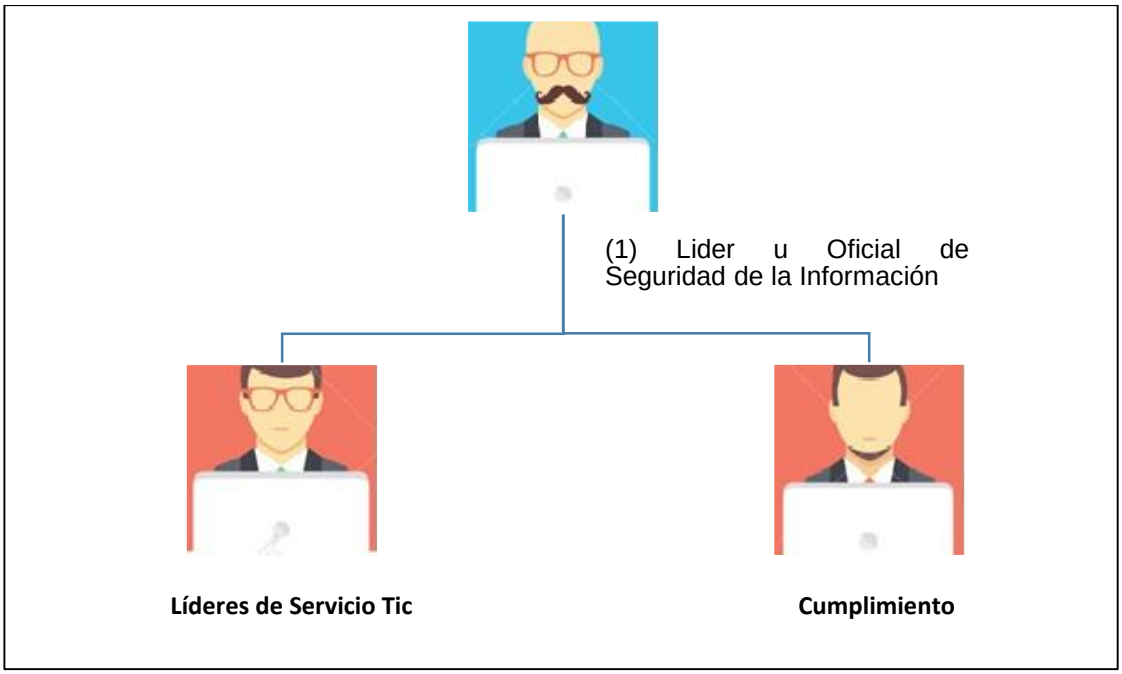


Ilustración 11. Estructura jerárquica subproceso del SGSI

Entre las responsabilidades y funciones del Oficial de Seguridad de la información, Lideres de servicios de Tics y los líderes de cumplimiento para cada fase del ciclo PHVA, se encuentran:

PHVA	Líder u Oficial de Seguridad de la Información	Líderes de Servicio Tic	Cumplimiento
P	1. Planificar, diseñar e implementar el SGSI de la entidad, sus Políticas, lineamientos y controles, los requerimientos legales y buenas prácticas.	-	-
P	2. Planificar y diseñar el Modelo de Seguridad y Privacidad de la Información acorde con la Política de Gobierno Digital.	-	-

P	3. Planear las actividades correspondientes a la Política de Gobierno Digital y de Ciberseguridad definida por el Ministerio de Defensa Nacional.	-	-
H	1. Desarrollar las actividades de coordinación de la Seguridad de la Información y seguridad Informática de la entidad.	1. Supervisar las herramientas de seguridad perimetral de la entidad.	1. Verificar las actividades definidas de Seguridad de la Información y Seguridad Informática de la entidad.
H	2. Establecer directrices y hacer seguimiento a los controles definidos en los procedimientos, estándares, guías, instructivos y buenas practicas relacionadas con la Seguridad de la Información y la Seguridad Informática.	2. Implementar los controles definidos en los procedimientos, estándares, guías, instructivos y buenas practicas relacionadas con la Seguridad de la Información y la Seguridad Informática.	2. Hacer verificación de los controles definidos en los procedimientos, estándares, guías, instructivos y buenas practicas relacionadas con la Seguridad de la Información y la Seguridad Informática.
H	3. Revisar y actualizar la documentación definida para el Sistema de Gestión de Seguridad de la Información SGSI.	3. Actualizar la documentación correspondiente, e implementar los cambios en el Servicio que lideran.	3. Verificación de la actualización de los documentos y la aplicación del mismo.
H	4. Diseñar Planes de sensibilización para los Funcionarios, Contratistas, Proveedores y/o Terceros, frente a la Cultura de Seguridad de la Información de la entidad.	4. Participar en la apropiación de Planes de sensibilización frente a la Cultura de Seguridad de la Información de la entidad.	4. Evaluar y acompañar en la sensibilización frente a la Cultura de Seguridad de la Información de la entidad.
H	5. Evaluar la efectividad del control definido en el Plan de Tratamiento de Riesgos referente a la Seguridad de la Información de la Entidad.	5. Implementar los controles definidos en el Plan de Tratamiento de Riesgos referente a la Seguridad de la Información del a Entidad.	5. Realizar seguimiento al Plan de Tratamiento de Riesgos referente a la Seguridad de la Información de la Entidad.
H	6. Evaluar, los concepto técnicos de requerimientos de Seguridad Informática.	6. Implementar los de requerimientos de Seguridad Informática.	6. elaborar el concepto técnicos de requerimientos de Seguridad Informática.
H	7. Elaborar la Metodología del Plan de Recuperación de Desastres "DRP".	7. Implementar el Plan de Recuperación de Desastres "DRP".	7. Apoyar en la elaboración de la Metodología del Plan de Recuperación de Desastres "DRP".
H	8. Asesorar a los Procesos de la Entidad en el desarrollo de la Metodología del Plan de Continuidad del Negocio "BCP".	-	8. Acompañar al Oficial de Seguridad de La Información en el Plan de Continuidad del Negocio "BCP".

H	9. Coordinar las acciones necesarias para identificar, controlar, reducir y evaluar los Incidentes de Seguridad de la Información de la entidad.	9. Realizar y documentar las acciones necesarias para mitigar los Incidentes de Seguridad de la Información de la entidad.	9. Evaluar las actividades realizadas para mitigar los Incidentes de Seguridad de la Información del a entidad.
H	10. Gestionar el Análisis de vulnerabilidades y remediación a la Infraestructura Tecnológica de la entidad.	10. Realizar las actividades para el análisis de vulnerabilidades y remediación a la Infraestructura Tecnológica de la entidad.	10. Hacer seguimiento a las actividades definidas para realizar el análisis de vulnerabilidades y remediación a la Infraestructura Tecnológica de la entidad.
H	11. Definir los indicadores de Gestión y cumplimiento del Sistema de Gestión de Seguridad de la Información de la entidad.	11. Entregar el reporte de la Gestión y cumplimiento del Servicio a su cargo.	11. Apoyar al Oficial de Seguridad en la definición de los indicadores de Gestión y cumplimiento del Sistema de Gestión de Seguridad de la Información de la entidad.
V	1. Verificar el cumplimiento del Sistema de Gestión de Seguridad de la Información de la entidad.	-	1. Acompañar al Oficial de Seguridad de la Información en el cumplimiento del Sistema de Gestión de seguridad de la Información de la entidad.
V	2. Verificar el documento de análisis de vulnerabilidades y el Plan de Remediación.	-	2. Verificar el documento de análisis de vulnerabilidades y el Plan de Remediación.
A	1. Reportar los Incidentes de alto Impacto a la Gerencia de la entidad.	-	1. Acompañar al Oficial de Seguridad de la Información en la elaboración del reporte de los Incidentes de alto Impacto a la Gerencia de la entidad.
A	2. Reportar al Jefe de la Oficina OTI el incumplimiento de las actividades del Sistema de Gestión de Seguridad de la Información de la entidad.	-	2. Acompañar al Oficial de Seguridad de la Información en la elaboración del reporte al Jefe de la Oficina OTI el incumplimiento de las actividades del Sistema de Gestión de Seguridad de la Información de la entidad.
A	3. Fomentar la mejora continua del Sistema de Gestión de Seguridad de la Información de la entidad.	-	3. Acompañar al Oficial de seguridad de la Información durante las actividades definidas en la mejora continua del Sistema de Gestión de Seguridad de la Información de la entidad

Tabla 4. Funciones estructura subproceso del SGSI

4.9.2 ROLES DE SEGURIDAD DE LA INFORMACIÓN[17]

Las siguientes son funciones específicas de seguridad de la información que pueden ser asignadas a cargos ya establecidos en la entidad.

- **Administrador de recursos informáticos**
  El Administrador de Recursos Informáticos de la entidad es responsable de aplicar y mantener los estándares de seguridad en los recursos informáticos de su responsabilidad (Ejemplo: Sistema Operativo, Red, Firewall, Aplicación, Base de datos, Middleware, etc.) acorde con el modelo del SGSI de la entidad y bajo la autorización del propietario de la información correspondiente.

- **Administrador de control de acceso lógico**
  El Administrador del control de acceso lógico a la información es responsable de ejecutar los procedimientos operativos de identificación, autenticación y control de acceso tendientes a proteger los activos de información, así como de actualizar los sistemas de acuerdo con el modelo del SGSI de la entidad.

- **Operador de seguridad de la información**
  El Operador de seguridad de la información es responsable de ejecutar los procedimientos de administración de la Operación en los elementos de seguridad, como monitoreo de alertas, de incidentes de seguridad y de vulnerabilidades, que se presenten en los recursos de información de la entidad. Su función debe estar alineada con los procesos operativos de TI.

- **Propietarios de activos de información**
  El propietario de un activo de información, tiene entre sus responsabilidades:

  a) Definir el nivel de clasificación de la información, dar las directrices de uso del activo, autorizar privilegios y definir el ciclo de vida del mismo.
  b) Informar al Líder u Oficial de Seguridad de la información, cuando detecte cualquier incidente de seguridad de la información, para que sea tratado y corregido mediante la aplicación de controles.
  c) Implementar las medidas de seguridad de la información necesarias en su área para evitar fraudes, robos o interrupción en los servicios o activos de información.
  d) En los casos en que aplique, asegurarse de que el personal: Funcionarios, Contratistas, Proveedores y/o Terceros, tienen cláusulas de confidencialidad en los contratos y son conscientes de sus responsabilidades.

- **Usuarios de la información**
  Se entiende por usuario de la información cualquier servidor público, contratista, proveedor o tercero, que utiliza la información procesada y suministrada por el ICA para ejercer sus funciones. Entre las responsabilidades de los usuarios de la información se encuentran:

[17] **Rol**: papel, función que alguien o algo desempeña.

a) Conocer, comprender y aplicar las políticas de seguridad de la información establecidas por el ICA.
b) Llevar a cabo su trabajo asegurándose de que sus acciones no afecten la seguridad de la información.
c) Comunicar al Líder u Oficial de Seguridad de la información, los incidentes de seguridad de la información que detecte durante el desarrollo de sus actividades.
d) Hacer uso de las mejores prácticas definidas en la entidad para todos los temas relacionados con seguridad de la información.
e) Cumplir con la cláusula de confidencialidad y manejo de la información contenida en el contrato firmado con la entidad.

4.9.3 RESPONSABILIDADES DE OTRAS DEPENDENCIAS U OFICINAS

4.9.3.1 OFICINA TECNOLOGÍAS DE LA INFORMACIÓN

En el marco de seguridad de la información, esta oficina debe cumplir con las siguientes responsabilidades:

a) Realizar el levantamiento, actualización y mantenimiento de los activos de información pertenecientes al proceso de Gestión de Información y Tecnologías.
b) Realizar la gestión del riesgo del proceso teniendo en cuenta la metodología de la entidad.
c) Cumplir con las disposiciones normativas vigentes aplicables al Sistema de Gestión de Seguridad de la Información, así como a cualquier requerimiento de seguridad de la entidad.
d) Aplicar los controles necesarios que garantizan la disponibilidad, confidencialidad e integridad de la información de los activos de información tecnológicos y recursos informáticos del ICA.
e) Evitar la divulgación, modificación, retiro, destrucción no autorizada de la información que se encuentra almacenada en medios magnéticos.
f) Autorizar la creación o modificación de las cuentas de acceso o recursos de la entidad.
g) Concientizar a los usuarios para que sigan buenas prácticas de seguridad en el uso de contraseñas.
h) Realizar y mantener copias de seguridad de la información en medio digital.
i) Garantizar la instalación de software antivirus que brinde protección contra código malicioso en todos los recursos informáticos.
j) Velar para que el software que se utilice en la entidad sea licenciado y no atente contra la normatividad vigente.
k) Ser los únicos autorizados para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes.
l) Establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red.

m) Establecer un procedimiento que asegure la desactivación o bloqueo de los privilegios de acceso sobre los recursos tecnológicos, los servicios de red y los sistemas de información, cuando el servidor público, contratista o usuario haya sido desvinculado o haya terminado el contrato con la entidad.
n) Evitar el acceso físico no autorizado, perdida, robo o exposición al peligro de los recursos de la plataforma tecnológica del ICA.
o) Mantener mecanismos de control de acceso físico al centro de datos y centros de cableado, controlando su ingreso mediante una bitácora.
p) Aplicar el procedimiento para la gestión de los cambios que se presenten al interior de la entidad, en los procesos, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
q) Planificar periódicamente actividades que involucren auditorias de los sistemas en producción y asegurar que los documentos, dispositivos y medios utilizados para las auditorias de los sistemas de información estén custodiados y protegidos de accesos no autorizados.
r) Asegurar la privacidad y la protección de la información de datos personales, almacenados en las bases de datos, como se exige en la legislación y la reglamentación pertinentes.
s) Documentar los resultados de las auditorias de los sistemas de Información.
t) Apoyar en la identificación y gestión para garantizar la protección de la información al momento de ser transferida o comunicada a un tercero.
u) Garantizar que los activos de información se encuentren ubicados y protegidos de tal modo que se reduzcan los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
v) Ejecutar las copias de seguridad de los activos de información devueltos.
w) Ejecutar el procedimiento de borrado seguro de los activos de información devueltos.
x) Reportar incidentes de seguridad de acuerdo con el procedimiento definido por el Instituto.

4.9.3.2 SUBGERENCIA ADMINISTRATIVA Y FINANCIERA

4.9.3.2.1 Gestión Integral del Talento Humano

En el marco de seguridad de la información, las dependencias relacionadas con el proceso de gestión integral del talento humano, deben cumplir con las siguientes responsabilidades de acuerdo con sus competencias:

a) Realizar el levantamiento, actualización y mantenimiento de los activos de información pertenecientes al proceso de Gestión Integral de Talento humano.
b) Realizar la gestión del riesgo del proceso teniendo en cuenta la metodología de la entidad.
c) Cumplir con las disposiciones normativas vigentes aplicables al Sistema de Gestión de Seguridad de la Información, así como a cualquier requerimiento de seguridad de la entidad. Verificar los antecedentes de todos los candidatos de acuerdo con las leyes, reglamentos y ética pertinentes, los cuales deben ser proporcionales a los

requisitos del negocio, a la clasificación de la información a la que se va a tener acceso, y a los riesgos percibidos.

d) Asegurar que los Funcionarios cumplan a cabalidad lo prescrito en el Manual de Funciones relacionado con el Sistema de Gestión de Seguridad de la Información de la entidad.
e) Comunicar la existencia del Sistema de Gestión de Seguridad de la Información del Instituto Colombiano Agropecuario a todo el personal y por consiguiente efectuar la legalización del Acta de compromiso sobre la seguridad de la información institucional que hará parte de su hoja de vida y anexo al acta de posesión.
f) Determinar y garantizar las competencias específicas requeridas a los Funcionarios cuyos roles se encuentren enmarcados en la estructura jerárquica del Sistema de Gestión de Seguridad de la Información - SGSI del Instituto.
g) Asegurar que los Funcionarios sean competentes, basándose en la educación, formación y/o experiencia requerida.
h) Evaluar a los Funcionarios en relación al desempeño de la seguridad de la información, impulsar la toma de acciones para adquirir y/o fortalecer las competencias necesarias y evaluar la eficacia de las acciones tomadas.
i) Archivar y custodiar las historias laborales de acuerdo a las tablas de retención documental, conservando la información documentada apropiada como evidencia de la competencia del cargo.
j) Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación vigente.
k) Liderar los programas de inducción, reinducción, capacitación y sensibilización enfocados a fortalecer la toma de conciencia en relación a seguridad de la información.
l) Establecer las responsabilidades para asegurar que la salida, desvinculación o cambio de cargo del Funcionario o pasante del ICA, se realice aplicando la política de seguridad y privacidad de la información.
m) Reportar a la Oficina de Tecnologías de la Información, las novedades de Funcionarios: (vacaciones, incapacidad, cambio de cargo, desvinculación total, encargo, licencias remuneradas y no remuneradas, suspensión) para cambios en el acceso a las aplicaciones y plataformas tecnológicas de la entidad.
n) Informar a la oficina Asesora de Tecnologías de la Información, cuando un funcionario inicie y culmine la comisión de estudios, con la finalidad de realizar los cambios en el acceso a las aplicaciones. Mantener la reserva, custodia y confidencialidad de la información personal de los funcionarios.
o) Reportar a la Oficina de Tecnologías de la Información las novedades que surjan con ocasión a la vinculación de pasantes al Instituto.
p) Adelantar las investigaciones disciplinarias a que haya lugar en contra de los Funcionarios, por los presuntos incumplimientos de las políticas del Sistema de Gestión de Seguridad de la Información del Instituto.
q) Reportar incidentes de seguridad de acuerdo con el procedimiento definido por el Instituto.

4.9.3.2.2 Gestión de Adquisición de bienes y servicios

En el marco de seguridad de la información, las dependencias relacionadas con el proceso de Gestión de Adquisición de Bienes y Servicios, deben cumplir con las siguientes responsabilidades de acuerdo con sus competencias:

a) Realizar el levantamiento, actualización y mantenimiento de los activos de información pertenecientes al proceso de Gestión de Adquisición de bienes y servicios.
b) Realizar la gestión del riesgo del proceso teniendo en cuenta la metodología de la entidad. Cumplir con las disposiciones normativas vigentes aplicables al Sistema de Gestión de Seguridad de la Información, así como a cualquier requerimiento de seguridad de la entidad.
c) Verificar los antecedentes de todos los candidatos de acuerdo con las leyes, reglamentos y ética pertinentes, los cuales deben ser proporcionales a los requisitos del negocio, a la clasificación de la información a la que se va a tener acceso, y a los riesgos percibidos.
d) Asegurar que los Funcionarios que tienen acceso a información reservada o confidencial, firmen un acuerdo confidencial, derechos de autor y/o protección de datos, según aplique.
e) Adelantar las medidas correspondientes de acuerdo con sus competencias funcionales, ante los presuntos incumplimientos que se deriven frente a lo dispuesto en el marco del Sistema de Gestión de Seguridad de la Información.
f) Verificar y gestionar con la Oficina de Tecnologías de Información que cualquier contratación de Servicios de TI generada por las dependencias de la entidad cumplan con las disposiciones legales, contractuales y técnicas.
g) Incorporar dentro de las minutas de contratos cláusulas de seguridad de la información, propiedad intelectual y acuerdos de confidencialidad.
h) Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
i) Comunicar a las autoridades competentes acerca de los presuntos incumplimientos de las políticas del Sistema de Gestión de Seguridad de la Información del Instituto, por parte de los Contratistas, Proveedores y/o Terceros.
j) Reportar a la Oficina de Tecnologías de la Información las novedades de suspensión, prórrogas, adición, lugar de ejecución, cesiones, cambio de forma de pago, terminación anticipada (en cualquiera de sus modalidades), entre otras, de los contratos de prestación de servicios personales y de apoyo a la gestión, con la finalidad de realizar los cambios en el acceso a las aplicaciones y ajustes en las plataformas tecnológicas de la entidad.
k) Reportar incidentes de seguridad de acuerdo con el procedimiento definido por el Instituto.

4.9.3.2.3 Gestión de Recursos Físicos

En el marco de seguridad de la información, las dependencias relacionadas con el proceso de Gestión de Recursos Físicos, deben cumplir con las siguientes responsabilidades de acuerdo con sus competencias:

a) Realizar el levantamiento, actualización y mantenimiento de los activos de información pertenecientes al proceso de Gestión de Recursos Físicos.
b) Realizar la gestión del riesgo del proceso teniendo en cuenta la metodología de la entidad.
c) Cumplir con las disposiciones normativas vigentes aplicables al Sistema de Gestión de Seguridad de la Información, así como a cualquier requerimiento de seguridad de la entidad.
d) Disponer de un sistema de información de bienes actualizado, ágil, claro, oportuno, veraz y confiable.
e) Promover la cultura para la correcta gestión sobre los bienes en servicio, con el fin de que cada persona asuma en forma individual la responsabilidad de los bienes bajo su cargo.
f) Velar por el uso adecuado de los bienes asignados en toda la entidad, saber dónde se encuentran dichos bienes y efectuar los correspondientes movimientos (traslados, devoluciones).
g) Velar y garantizar que los Funcionarios y contratistas devuelvan todos los activos de la entidad que se encuentran en su poder a la terminación del vínculo por virtud del cual se tuvo acceso a los mismos.
h) Coordinar con la mesa de ayuda, la realización de una copia de respaldo de la información del activo previamente devuelto la cual será entregada al responsable del área solicitante con el objeto de ejecutar el procedimiento de borrado seguro sobre el activo devuelto conforme lo expuesto en la Política de Seguridad y privacidad de la Información
i) Evitar el acceso físico no autorizado, pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica del ICA, daño e interferencia para la información que se encuentren dentro o fuera de las instalaciones de procesamiento de información.
j) Garantizar que los activos de información se encuentren ubicados y protegidos de tal modo que se reduzcan los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
k) Aplicar medidas de seguridad a los activos que se encuentren fuera de las instalaciones de la entidad, teniendo en cuenta los diferentes riesgos asociados.
l) Verificar que sea registrado el ingreso y salida de los visitantes y dispositivos tecnológicos en el punto de vigilancia del Instituto, de acuerdo con la información requerida, asegurando con ello el cumplimiento de las disposiciones normativas vigentes en cuanto a la protección de datos personales, en lo que respecta a su tratamiento y custodia.
m) Velar por que los visitantes estén siempre acompañados por la persona a quien visitan durante la permanencia en el edificio.

n) Promover que todos los Funcionarios, contratistas (prestación de servicios personales), Proveedores y/o Terceros, porten el carnet o el documento, según sea el caso, que los identifica como tal, mientras permanezcan en las instalaciones del Instituto.
o) Verificar que las áreas seguras se encuentren protegidas mediante controles de entrada adecuados para garantizar que se le permita el acceso únicamente al personal autorizado.
p) Programar, ejecutar y controlar los mantenimientos de los equipos, asegurando que se protejan contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
q) Reportar incidentes de seguridad de acuerdo con el procedimiento definido por el Instituto.

4.9.3.2.4 Gestión Documental

En el marco de seguridad de la información, esta dependencia debe cumplir con las siguientes responsabilidades:

a) Asegurar que todos los activos de información sean clasificados según el contenido y la importancia para la entidad, de acuerdo con su grado de criticidad, requisitos legales, valor y sensibilidad a divulgación o a modificación no autorizada.
b) Aplicar medidas de protección durante el ciclo de vida de la información, desde su creación, durante su uso autorizado y hasta su apropiada disposición o destrucción, sin importar el medio, formato o lugar donde se encuentre.
c) Asegurar que la información que se encuentra en documentos físicos sea protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.
d) Verificar que los Funcionarios y contratistas cumplan con los lineamientos de la guía de rotulación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física.
e) Verificar que la información física, digital y magnética tenga un periodo de almacenamiento alineado con las tablas de retención documental y cuando se cumpla el periodo de expiración, validar que toda la información sea eliminada adecuadamente.
f) Reportar incidentes de seguridad de acuerdo con el procedimiento definido por el Instituto.

4.9.3.3 OFICINA ASESORA JURIDICA

En el marco de seguridad de la información, esta dependencia debe cumplir con las siguientes responsabilidades:

a) Orientar a las demás áreas y/o dependencias del Instituto para que en ejercicio de sus funciones de cumplimiento a las disposiciones normativas constitucionales y legales relacionadas con la seguridad de la información.

b) Asesorar a las áreas y/o dependencias del Instituto en la interpretación de las normas constitucionales y legales relacionadas con el tema del Sistema de Gestión de Seguridad de Información, para garantizar una adecuada toma de decisiones y mantener la unidad de criterio en la aplicación de dichas disposiciones en el campo de acción del Instituto.
c) Brindar apoyo jurídico en el desarrollo e implementación de los mecanismos que contribuyan a la confidencialidad, integridad y disponibilidad de la información de la entidad.
d) Reportar incidentes de seguridad de acuerdo con el procedimiento definido por el Instituto.

4.9.3.4 OFICINA ASESORA DE PLANEACIÒN

En el marco de seguridad de la información, esta dependencia debe cumplir con las siguientes responsabilidades:

a) Revisar y controlar los documentos (políticas, procedimientos, manuales, guías, estándares, entre otros.) que se segreguen del SGSI.
b) Establecer los lineamientos y controles necesarios para la mejora del SGSI.
c) Consolidar y analizar la información del desempeño de la gestión de los procesos de la Entidad.
d) Mejorar continuamente la eficacia del SGSI mediante el uso de la política de seguridad y privacidad de la información, los objetivos de seguridad de la información, los resultados de auditorías, el análisis de los eventos a los que se le ha hecho seguimiento, las acciones correctivas y la revisión por la dirección.

4.9.3.5 OFICINA DE CONTROL INTERNO

En el marco de seguridad de la información, esta dependencia debe cumplir con las siguientes responsabilidades:

a) Practicar auditorias periódicas sobre los sistemas de información y toda la plataforma tecnológica instalada y en operación (software y hardware), las actividades vinculadas con la seguridad de la información, reportando el nivel de cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por el modelo del SGSI y por las políticas, normas, procedimientos y prácticas que de él se deriven.
b) Realizar auditorías periódicas en el Instituto sobre el cumplimiento del Sistema de Gestión de Seguridad de la Información.

4.9.3.6 OFICINA ASESORA DE COMUNICACIONES

En el marco de seguridad de la información, esta dependencia debe cumplir con las siguientes responsabilidades:

a) Disponer los medios técnicos necesarios para comunicar a todo el personal, las políticas, los lineamientos, las normas, los procedimientos, etc., relacionados con seguridad de la información.
b) Mantener a los Funcionarios y Contratistas informados y actualizados sobre los avances del SGSI, a través de los mecanismos de comunicación que disponga la entidad con el apoyo del Líder u Oficial de Seguridad de la información.

5 FORMACIÓN Y CAPACITACIÓN

En el marco del proceso de Gestión Integral del Talento humano, el cual tiene por objetivo "Garantizar la disponibilidad y competencia del recurso humano necesario para la operación del ICA", la entidad selecciona, vincula y evalúa a los Funcionarios con base en su educación, experiencia, formación y habilidades determinadas en el Manual especifico de funciones y competencias laborales adoptado por la Resolución No. 000712 del 9 de marzo de 2015.

De la misma forma la entidad realiza evaluaciones de desempeño laboral y diagnóstico de necesidades de capacitación que permiten medir y analizar la gestión de la entidad para el mejoramiento continuo y la seguridad de la información, que a su vez son fuente para la elaboración anual del *Cronograma de capacitación, entrenamiento y reentrenamiento*. Lo anterior soportado en planes de sensibilización periódicos y en consonancia con las directrices del Plan Nacional de desarrollo y el Plan estratégico institucional, crean una entidad más efectiva y segura en la prestación del servicio público y fortalece el cumplimiento no solo de la misión institucional, sino también de la Política del SGSI.

En el marco del proceso de Gestión de adquisición de bienes y servicios cuyo objeto es "garantizar la compra u obtención correcta y oportuna de los bienes y servicios requeridos para la operación del ICA" el Instituto selecciona, vincula y evalúa el recurso humano (Contratistas, Proveedores y/o Terceros) en función de los requisitos de educación, experiencia, formación y habilidades que se encuentran determinadas en los estudios de seguridad previos a la contratación, para la prestación de servicios profesionales y de apoyo. En el desarrollo de sus labores, el supervisor del contrato realiza las evaluaciones al cumplimiento de las obligaciones contractuales siguiendo los lineamientos del Manual de Procedimiento contratos de Prestación de Servicios Profesionales y de Apoyo a la Gestión (SISCOP) ABS-P-001.

5.1 INFORMACIÓN DOCUMENTADA

La información documentada requerida por la NTC/ISO 27001:2013 y la información documentada que la entidad ha determinado que es necesaria para la eficacia del SGSI, se crea, se actualiza y se controla siguiendo los lineamientos de los procedimientos Control de Documentos GIT-GCD-P-001 y Control de Registros GIT-GCD-P-002.

5.2 MANTENIMIENTO Y MEJORA DEL SGSI

5.2.1 MEDICIÓN DE LA EFICACIA DEL SGSI

Para evaluar el desempeño de la seguridad de la información y la eficacia del SGSI, en el documento de *Métricas e Indicadores del SGSI*, la entidad identifica los controles objeto de medición y los lineamientos para llevar a cabo el seguimiento, análisis y evaluación de los mismos.

5.2.2 AUDITORIA INTERNA

Con el propósito de verificar el cumplimiento del SGSI y el seguimiento a los compromisos derivados de este, la entidad llevará a cabo, por lo menos una vez al año, el programa de auditorías internas, para lo cual se ha implementado el procedimiento *Administración y Desarrollo de Auditorías Internas DIR-EVA-P-001*, que contribuye a asegurar la eficiencia, eficacia y efectividad del SGSI y a su vez está alineado con la norma ISO 19011.

5.2.3 REVISIÓN POR LA DIRECCIÓN

La revisión por la Dirección tiene como finalidad asegurar la conveniencia, adecuación y eficacia del sistema, en donde se evalúan las oportunidades de mejora y la necesidad de realizar ajustes a la estructura o los lineamientos del SGSI. En el ICA, el *Comité de Coordinación del Sistema de Control Interno y del Sistema de gestión de la calidad,* coordina y asegura que se realice como mínimo, una vez al año, la revisión por la dirección, con el objeto de dar cumplimiento a lo dispuesto por la normatividad vigente y que con ello se documenten los compromisos para avanzar con el modelo de madurez del SGSI.

Todo lo anterior, sobre la base de que la alta dirección del Instituto desde sus funciones, garantiza la ejecución presupuestal de cada uno de los compromisos que ese deriven de dicha revisión.

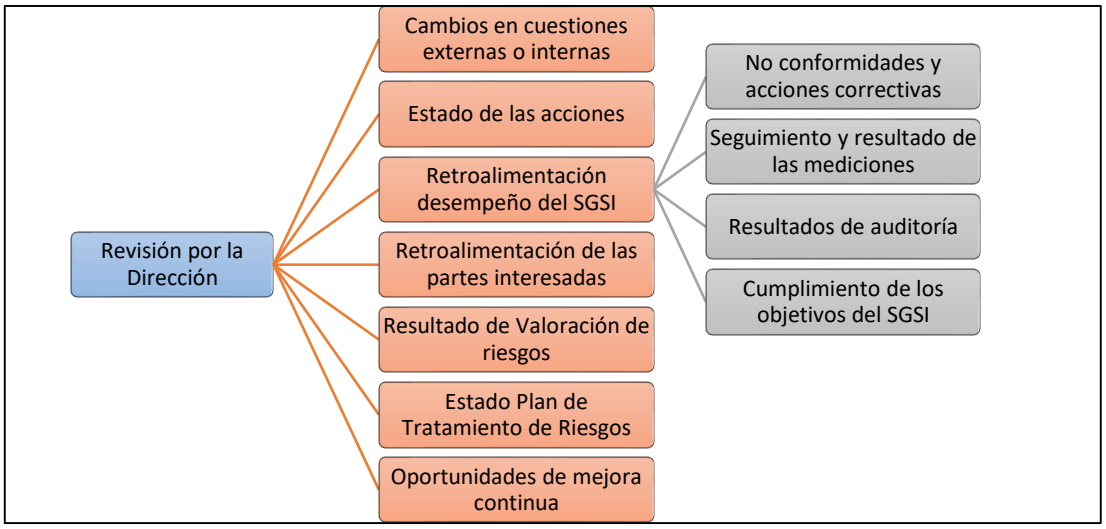


Ilustración 12. Consideraciones para la Revisión por la Dirección

5.2.4 MEJORA DEL SGSI

A partir de hallazgos o situaciones de mejora identificadas por diferentes fuentes, la entidad define la metodología a seguir para eliminar las causas de las no conformidades reales o potenciales con el objeto de evitar nuevamente su ocurrencia, dicha gestión finaliza con la validación de la efectividad de las acciones previstas en el plan de acción hasta su cierre. Estas disposiciones se establecen en el procedimiento Implementación de Acciones de Mejora DIR-MEJ-P-001.

6 FORMAS

N/A

7 ANEXOS

7.1 INDICE DE ILUSTRACIONES

Ilustración 1. Organigrama ICA 7
Ilustración 2. Modelo de seguridad de la información 8
Ilustración 3. Fases del ciclo PHVA 9
Ilustración 4. SGSI desde la perspectiva de sus componentes 9
Ilustración 5. Principios de seguridad de la información 10
Ilustración 6. Contexto interno y externo de ICA 13
Ilustración 7. Mapa de procesos y alcance del SGSI 23
Ilustración 8. Estructura general de la metodología de riesgos 25
Ilustración 10. Organización Centralizada 26
Ilustración 11. Modelo de Operación del Líder u Oficial de Seguridad de la Información 28
Ilustración 12. Estructura jerárquica subproceso del SGSI 29
Ilustración 13. Consideraciones para la Revisión por la Dirección 41

7.2 INDICE DE TABLAS

Tabla 1. Análisis DOFA 21
Tabla 2. Partes Interesadas 22
Tabla 3. Interfaces y dependencias del SGSI 24
Tabla 4. Funciones estructura subproceso del SGSI 31