Plan Estratégico de Seguridad de la Información
PESI

Instituto Colombiano Agropecuario

Noviembre 2017

Oficina Tecnologías de la Información

TABLA DE CONTENIDO

1 INTRODUCCIÓN

El Gobierno en línea 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 organizaciones, 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 a lograr una producción agropecuaria competitiva, con el fin de aportar al logro de los objetivos de la Apuesta Exportadora de Colombia. Realiza 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 reglamente y controla el uso de organismos vivos modificados por ingeniería genética para el sector agropecuario[1].

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 y de apoyo, continuamente se está procesando, gestionando, almacenando, custodiando, transfiriendo e intercambiando información valiosa que puede ir desde un

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

dato personal hasta secretos empresariales que no deben ser divulgados a personal no autorizado, porque pueden poner en riesgo el comercio nacional, los acuerdos comerciales, las negociaciones bilaterales y el comercio en general.

En atención a lo anterior, la entidad asumió el reto de implementar el Sistema de gestión en seguridad de la información, en adelante SGSI, siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL, a su vez reglamentado a través del Decreto 1078 de 2015 para el sector de tecnologías de la información y comunicaciones y el Decreto 2573 de 2014 por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.

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 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.

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 GTC/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 las partes interesadas.

Por otra parte, el Plan Estratégico de Tecnologías de la Información y Comunicaciones (PETI), es un documento que expresa las intenciones de la organización, en la implementación de iniciativas y acciones que promuevan el uso de las Tecnologías de la Información y las Comunicaciones – TIC’s como contribución al logro de los Objetivos y Lineamientos Estratégicos enmarcados en el Plan Estratégico Institucional, Plan Diamante 2016-2022. El PESI descrito en este documento está alineado completamente con el PETI.

El documento PETI define lineamientos para el mejoramiento del nivel de madurez institucional en la implementación de soluciones tecnológicas que generen valor y promuevan el cumplimiento de la misión con sostenibilidad tecnológica. El fortalecimiento y mejoramiento de la infraestructura tecnológica, el fortalecimiento de una mesa de ayuda, **la implementación de los sistemas de seguridad de la información** y la continuidad de negocio, la optimización en el procesamiento y análisis de información, el fortalecimiento y mejora de los procesos institucionales (Estratégicos, Misionales y de Apoyo) y de gestión de la información y gobernabilidad de TI, de acuerdo con la Estrategia Gobierno en Línea - GEL del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC (Para mayor información ver PETI).

Finalmente, los lineamientos y proyectos para el desarrollo, optimización e implementación efectiva de los Sistemas de Información, así como las iniciativas que permitirán una adecuada gestión de la Infraestructura de Hardware/Software, basados en el Modelo de Seguridad y Privacidad de la Información – MSPI y en las mejores prácticas de Gestión de Servicios y Proyectos de TI, contribuirán no solo con el logro de los objetivos institucionales, sino en la generación de confianza en el uso de los mecanismos tecnológicos para una mejor relación Estado – Ciudadano y la protección de los activos de información (PETI).

2 OBJETIVO

Definir una estrategia de Seguridad de la información, en adelante PESI, liderada por la Oficina de Tecnologías de la Información del Instituto Colombiano Agropecuario, en adelante ICA, a partir de la vigencia 2017 y hasta la vigencia 2022, que responda a las necesidades de preservar la confidencialidad, la integridad y la disponibilidad sobre los activos de información.

3 OBJETIVOS ESPECÍFICOS

1. Comunicar e implementar la Estrategia de seguridad de la información.
2. Incrementar el nivel de madurez en la gestión de la seguridad de la información.

3. Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información – MPSI, con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
4. Hacer uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
5. Asegurar los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

4 ALCANCE DEL PESI

Teniendo en cuenta el análisis del contexto externo, interno y las partes interesadas, el ICA define el alcance de su Sistema de Gestión en Seguridad de la Información (SGSI) y del PESI, 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 Sistema de gestión en seguridad de la información (SGSI) para todos los procesos; Misionales, apoyo y direccionamiento.

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, sin excepción alguna.

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

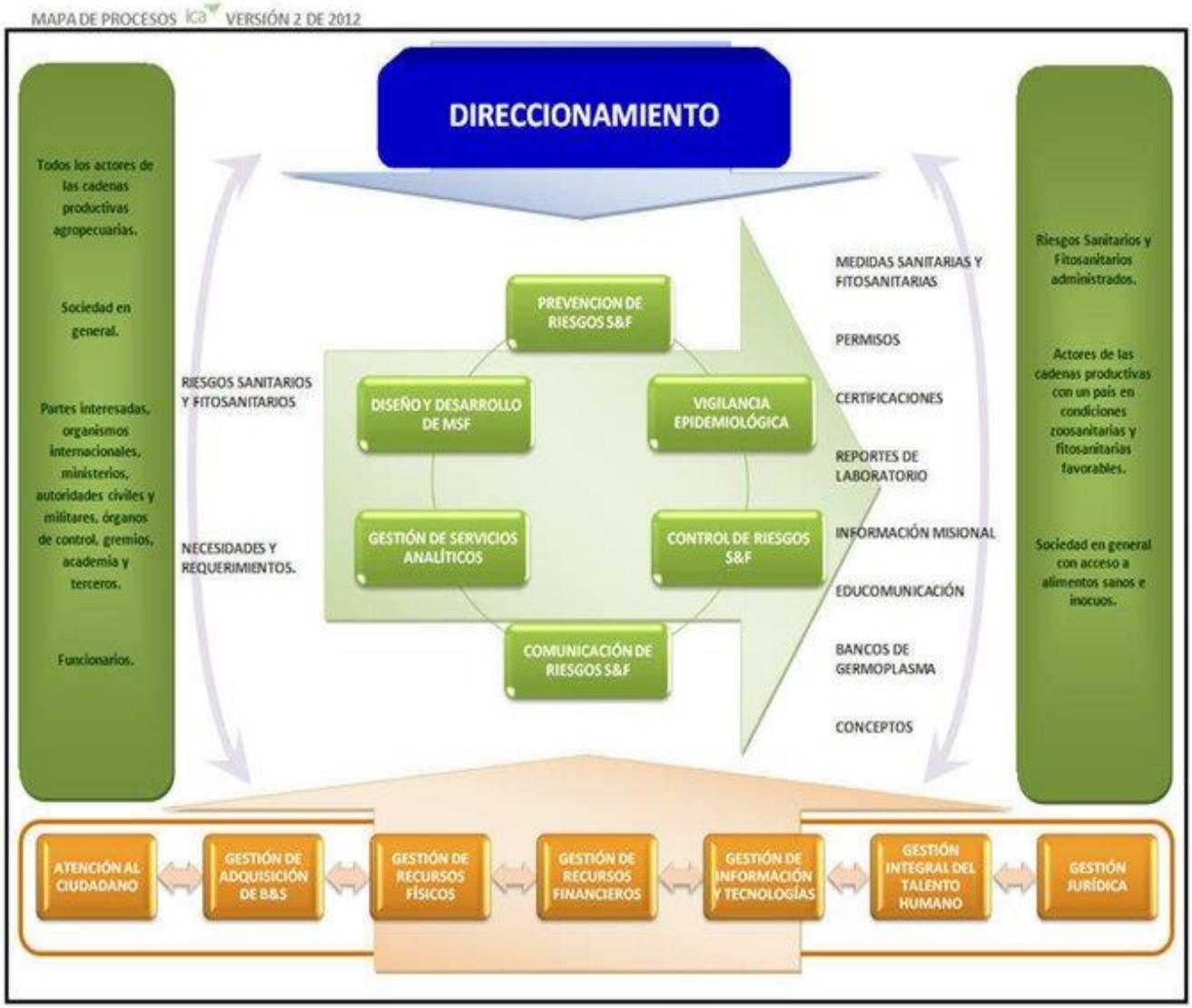


Ilustración 1. Ilustración 1. Mapa de procesos y alcance del SGSI

5 DEFINICIONES

- **Activo**: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Guía**: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Norma**: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- **Parte interesada**: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Política del SGSI:** Manifestación expresa de apoyo y compromiso de la alta dirección con respecto a la seguridad de la información.
- **Política**: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.
- **Procedimiento**: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.
- **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 consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

6 NORMAS APLICABLES

- NTC/ISO 27001:2013
- NTC/ISO 27005:2009
- GTC/ISO 27002:2015
- Modelo de Seguridad y Privacidad de la Información V.3.0.2 – MPSI de la Estrategia de Gobierno en Línea – GEL

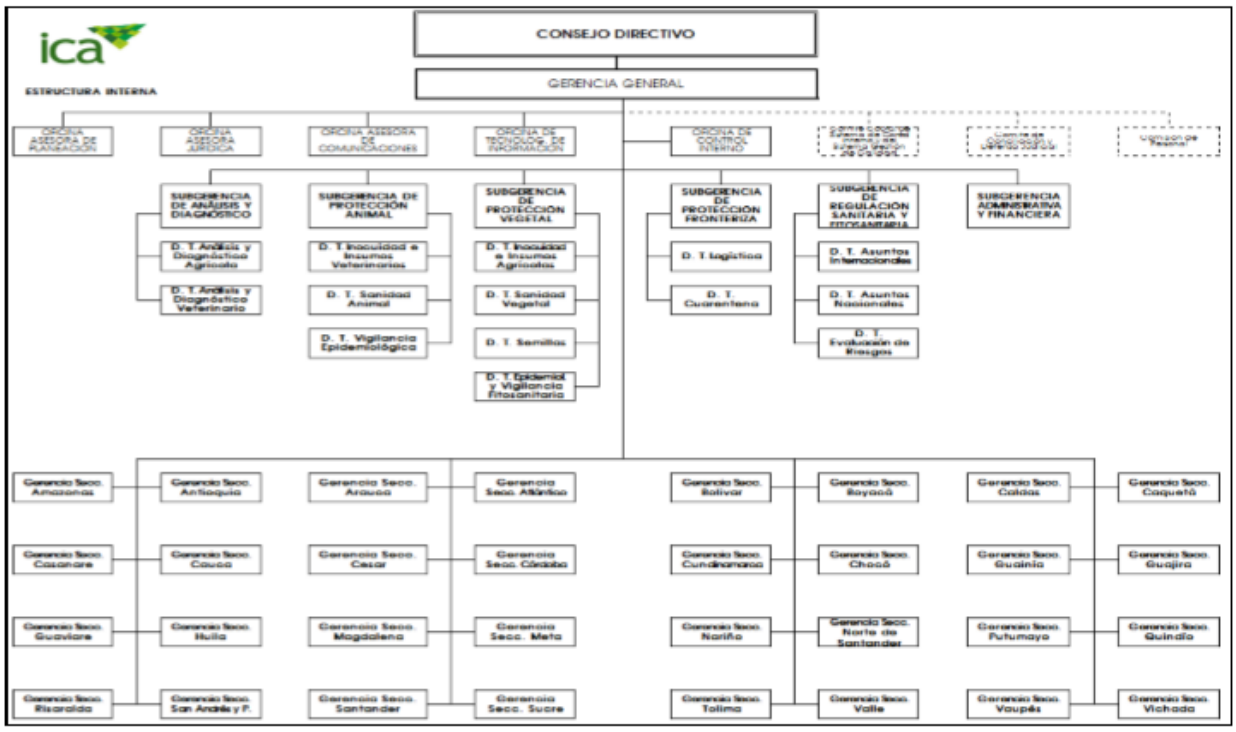
7 ESTRUCTURA ORGANIZACIONAL

El Instituto está compuesto por 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.

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. 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.

7.1 PLANEACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

En la actualidad y de acuerdo con la expedición del Decreto 2573 de 2014 contenida en el 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 de la Estrategia de Gobierno en Línea – GEL con el fin de preservar la integridad, confidencialidad, disponibilidad y privacidad de la información mediante

Ilustración 2. Organigrama ICA

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 listan los componentes de cada una de estas fases del ciclo:

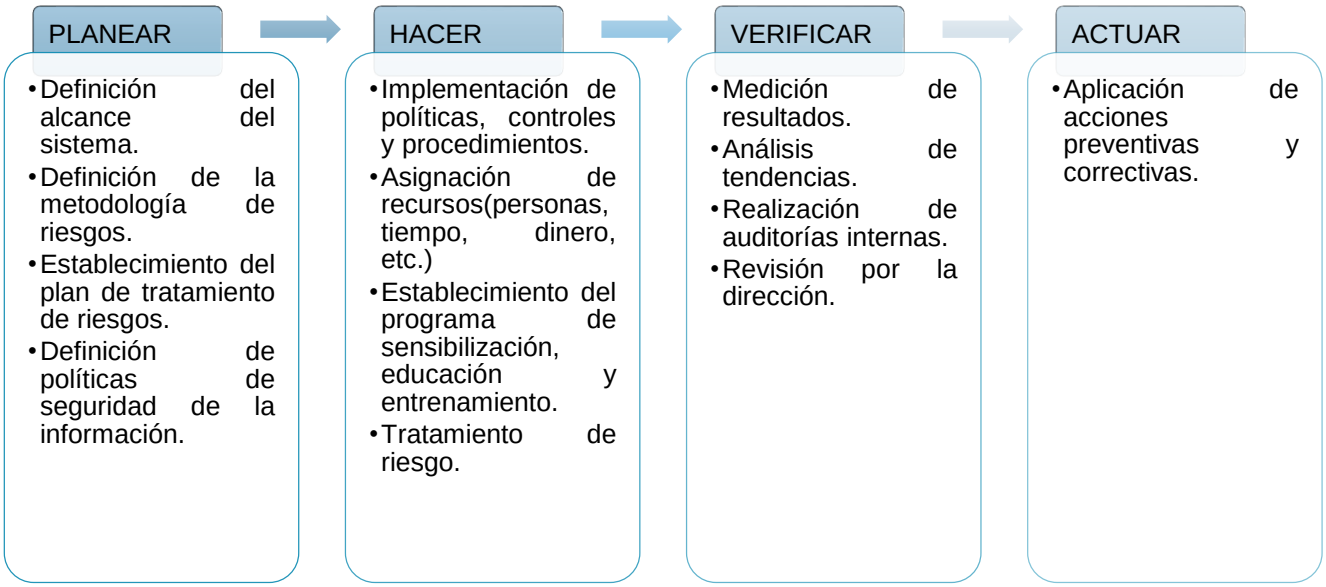


Ilustración 3. Fases del ciclo PHVA

7.2 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, 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.[2]

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.

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

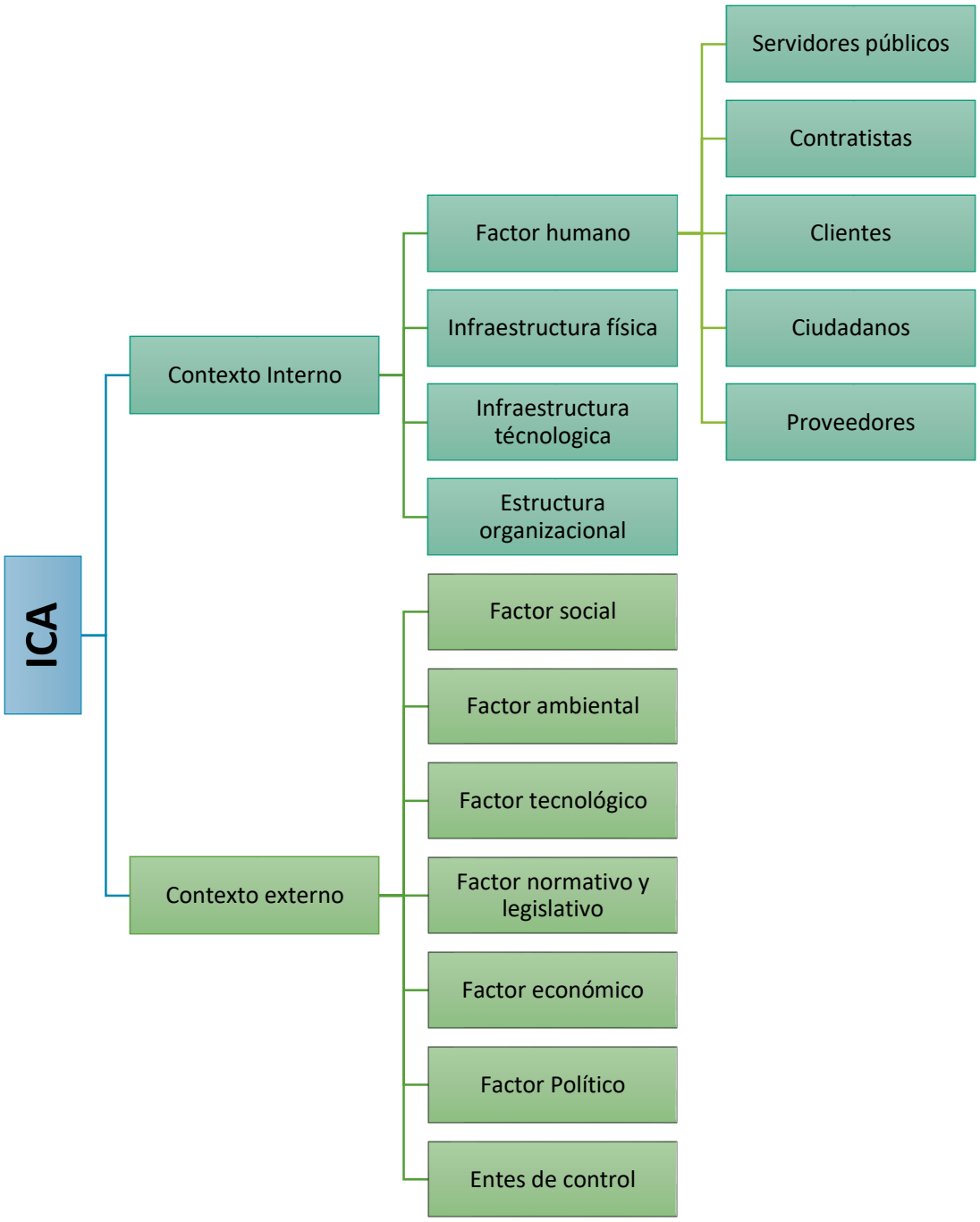


Ilustración 4. Contexto Externo e Interno

7.2.1 CONTEXTO INTERNO

- **Factor Humano**

Las personas también hacen parte de los activos de información más importantes dentro de una organización. En el ICA se encuentran representados en servidores públicos, contratistas, proveedores, clientes y ciudadanos, 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 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.

- **Infraestructura Física:**

La oficina principal u oficina nacional del ICA, ubicada en Bogotá cuenta con unas instalaciones en arriendo, operando en los pisos 1, 6, 7, 8, 9 y 10; dichas oficinas cumplen con controles de seguridad para acceder a la misma, se exige porte del carnet institucional para los servidores públicos, contratistas y registro de ingreso para visitantes y elementos tecnológicos, estos últimos se llevan en la recepción principal y el ingreso por piso.

En cada uno de los pisos donde opera el ICA se cuenta con:

a. Áreas seguras.
b. Sistemas de detección y extinción de incendios.
c. Áreas de evacuación.
d. Señalización de áreas.
e. El edificio cuenta con cuatro (4) ascensores.
f. Para ingresar a los centros de cableado de cada piso, lo realiza únicamente personal autorizado con el uso de llaves y tarjeta de proximidad..
g. Para le ingreso del data center, lo realiza personal autorizado con el uso de sistemas biométricos y de proximidad.

- **Infraestructura Tecnológica**

El ICA cuenta con dos (2) DATACENTER, el primero se encuentra ubicado en las instalaciones de las oficinas nacionales en Bogotá 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 y se utiliza un sistema biométrico, 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 solamente 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.

El segundo 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 en categoría oro.

- **Gestión por procesos**

El ICA tiene definido un enfoque por procesos, por medio de los cuales genera valor agregado a todas las actividades que desarrolla. Con ello garantiza el cumplimiento de lo definido en sus lineamientos estratégicos y por ende su Misión, redundancia en servicios coherentes para la ciudadanía con transparencia y eficiencia. Lo anterior se enmarca en el Sistema de gestión actual, escenario que facilita el diseño, establecimiento e implementación del SGSI.[3]

En cuanto a jerarquía, la dirección del ICA está en cabeza del Consejo Directivo y la Gerencia General, apoyados en las diferentes oficinas, subgerencias y gerencias seccionales, estructura que está comprometida con el SGSI.

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

7.2.2 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.
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.[4]
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.

- **Factor Ambiental**

Datos tomados de CCB Cámara de Comercio de Bogotá (2006).
Las oficinas de ICA se encuentran ubicada en el límite de la localidad de Fontibón. Esta localidad 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

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

medida por el transporte, almacenamiento 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 del ICA.

- **Factor Tecnológico**

El ICA como entidad pública del orden nacional, debe implementar, de manera sistemática y coordinada, la Estrategia de Gobierno en Línea 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.

- **Factor Normativo y Legislativo**

El ICA, como Entidad Pública dispone de un marco normativo y regulatorio en materia de Seguridad de la Información, 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 de Seguridad de la Información*[5]:

- **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[6]**

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:

- Prioridad del gobierno nacional hacia otros sectores empresariales Minero – Energético
- Cierre de mercados internacionales por razones sanitarias y fitosanitarias
- Traslado de funciones/misiones a otras entidades del estado o privadas
- Negociación de una reforma agropecuaria en el marco de los acuerdos de paz
- Falta de incentivos tributarios al sector

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

- 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 estrategia de Gobierno en Línea 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 y/o Contratistas) y Externos (Entidades, agremiaciones, etc.).

- **Entes de Control**

El ICA y sus activos de información están continuamente expuestos a revisiones y seguimientos por parte de los entes de control; 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:

- Contraloría General de la Nación
- Ministerio de Agricultura y Desarrollo Rural
- Ministerio de Hacienda y Crédito Público
- Procuraduría General de la Nación
- Contaduría General de la Nación

7.2.3 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.
	F4.	Implementación del SGSI que promueve la confidencialidad, Integridad y Disponibilidad de la información para los clientes internos (Funcionarios y/o Contratistas) y Externos (Entidades, agremiaciones, etc.).	O4	Participar entre las Entidades Públicas que se encuentran Certificadas en ISO 27001:2013 mediante la apropiación de una Cultura del SGSI.
	F5.	Adecuaciones físicas de nueva sede para oficinas nacionales y Datacenter.	O5.	Garantizar el nivel de seguridad física en las nuevas instalaciones de la Entidad, controlando el ingreso y salida del personal, así como los activos de información de la Entidad.
	Debilidades		**Amenazas**	
Factor Negativo	D1.	La entidad debe fortalecer los programas de divulgación y sensibilización a los Funcionarios y/o Contratistas, proveedores y 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.	Constante rotación del personal operativo responsable de los procesos.	A4.	Dar cumplimiento al Manual del SGSI y a las políticas de seguridad y privacidad de la información.
	D5.	La entidad carece de seguimiento a los Funcionarios y/o Contratistas, proveedores y terceros frente al cumplimiento del SGSI.	A5.	Ataques cibernéticos a las entidades públicas.

Tabla 1. Análisis DOFA

7.3 PARTES INTERESADAS

El ICA reconoce como sus grupos de interés a[7]:

PARTE INTERESADA	DESCRIPCIÓN
Usuarios directos	Productores (ganaderos, agricultores, laboratorios, etc.) exportadores e importadores, comercializadores, transportadores, agentes de intermediación aduanera y los terceros autorizados.
Usuarios Indirectos	Consumidores, las ONG y la ciudadanía.
Entidades publicas	Autoridades del sector y entes del Estado.
Terceros relacionados	Gremios de la producción, la academia, centros de investigación, proveedores y medios de comunicación.
Entidades externas	Entidades homologas de otros países y los organismos internacionales de referencia.

Tabla 2. Partes Interesadas.

8 MARCO CONCEPTUAL DEL PESI

Para el ICA, son muy importantes los resultados obtenidos en el PESI con el fin de apoyar la implementación del SGSI. El PESI se apoya en el Plan Estratégico Institucional en cual a su vez se fundamenta en la metodología del *Balanced Scorecard* o Cuadro de Mando Integral, debido a su gran utilidad en el direccionamiento de las organizaciones

El *Balance Scorecard* es una herramienta útil en la Planeación Estratégica. Esta metodología tiene en cuenta las siguientes fases: el análisis revisión de Misión, objetivos y estrategias, análisis de la propuesta de Valor, recursos financieros, clientes, procesos, crecimiento y aprendizaje; Reporte, Revisión y Comunicación de resultados, cambio y mejoramiento de las Estrategias laborales de cada miembro de la Institución, actualización y adaptación permanente frente a cambios internos y externos del entorno. Asimismo, los objetivos y metas son evaluables y medibles, generando sus propios indicadores, que deberán ser utilizados como herramienta para el seguimiento, control, evaluación y gestión del Instituto Colombiano Agropecuario[8].

[7] **Fuente**: Manual del Sistema de Gestión DIR-MEJ-MSG-001
[8] Plan Estratégico Institucional del ICA o Plan Diamante.

9 METODOLOGIA UTILIZADA

La metodología utilizada para el desarrollo del PESI se muestra y se explica a continuación:

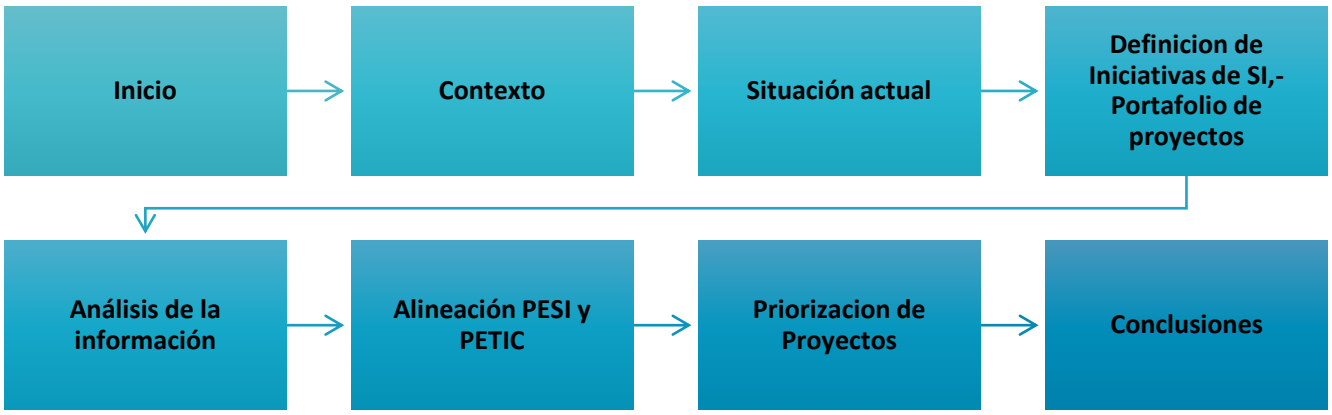


Ilustración 5. Metodología Utilizada

9.1 CONTEXTO

En esta fase inicial del desarrollo del PESI, se busca entender las características principales de la entidad con el fin de que los objetivos de este Plan estén alineados con los objetivos estratégicos de la entidad. Entre los aspectos que se deben considerar para lograr este entendimiento están:

1. La misión
2. La visión
3. Historia y antecedentes
4. Estructura organizacional
5. Procesos
6. Cultura y valores
7. Legislación pertinente

9.2 SITUACIÓN ACTUAL

Por situación actual se entiende el nivel de madurez que posee en este momento el ICA con relación a la seguridad de la información. El proceso por el cual se lleva a cabo esta estimación del nivel de madurez se denomina Instrumento de diagnóstico del MSPI de Mintic. Para poder realizar el PESI es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios (ver figura a continuación) con el fin de plantear prioridades sobre su implementación.

Dominio ISO 27001	Objetivo de control
Política de seguridad de la información.	Objetivo de control A.5
Organización de la seguridad de la información.	Objetivo de control A.6
Seguridad de los RRHH.	Objetivo de control A.7
Gestión de activos.	Objetivo de control A.8
Control de accesos.	Objetivo de control A.9
Criptografía.	Objetivo de control A.10
Seguridad física y del entorno	Objetivo de control A.11
Seguridad en las operaciones.	Objetivo de control A.12
Seguridad en las comunicaciones.	Objetivo de control A.13
Adquisición de sistemas, desarrollo y mantenimiento.	Objetivo de control A.14
Relación con proveedores.	Objetivo de control A.15
Gestión de los incidentes de seguridad de la información	Objetivo de control A.16
Aspectos de seguridad de la información en la Continuidad del negocio.	Objetivo de control A.17
Cumplimiento con requerimientos legales y contractuales.	Objetivo de control A.18

Ilustración 6. Dominios.

La metodología utilizada para realizar el GAP se presenta a continuación:

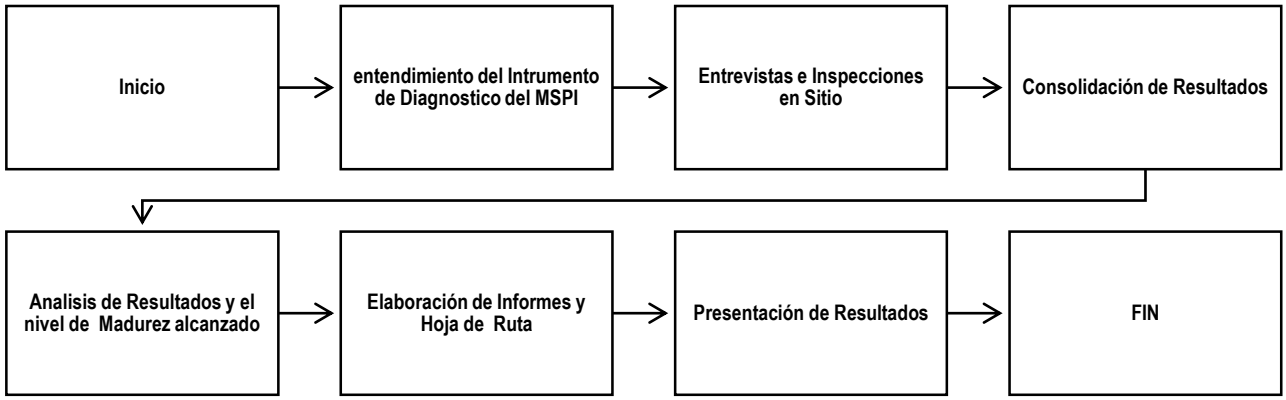


Ilustración 7. Metodología utilizada en el GAP.

El nivel de madurez permite establecer las bases para la mejora continua del proceso de Seguridad de la Información del ICA, e identificar las iniciativas de seguridad de la información, los cuales deben estar alineadas a las necesidades que se identificaron en Plan Estratégico de tecnologías de información y comunicaciones y la estrategia de información (PETI).

En seguida, se presenta el nivel de madurez del modelo de seguridad y privacidad de la información y el porcentaje de cumplimiento de la Entidad frente a los 14 dominios de la norma ISO/IEC 27001:2013 y ISO/IEC 27002:2013.

Ilustración 8. Diagrama tipo radar por Dominio

Analizando el gráfico, se puede observar que el dominio con mayor nivel de madurez es el *A.5 Política de seguridad de la información* (Optimizado), A.7 Seguridad de los recursos humanos (Optimizado[9]), seguido de A.16 gestión de incidentes de seguridad (Gestionado), A.11 Seguridad física (Gestionado [10]), A.18 Cumplimiento con requerimientos legales y contractuales (Gestionado), A.6 organización de seguridad de la información (Efectivo), A.8 gestión de activos (Efectivo), A.9 control de acceso (Efectivo), A.10 criptografía (Efectivo), A.12 seguridad de la operaciones (Efectivo) , A.13 seguridad de las comunicaciones (Efectivo), A.15 relaciones con los proveedores (Efectivo) Los demás dominios se encuentran por debajo del 40 % que corresponde a un estado Repetible.

En conclusión el nivel de madurez alcanzado por el ICA está en 58%, lo que significa que la compañía está en nivel efectivo, Los procesos y los controles se documentan y se comunican. Los

[9] En este nivel se realizan mediciones sobre la efectividad de los controles.
[10] En este nivel el control esta implementado y además es soportado por un documento que contiene una política de alto nivel y otras políticas operativas debidamente aprobadas.

controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.

A continuación se presenta la evaluación de efectividad de controles :

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	80	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	52	80	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	98	80	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	45	80	EFECTIVO
A.9	CONTROL DE ACCESO	44	80	EFECTIVO
A.10	CRIPTOGRAFÍA	60	80	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	63	80	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	42	80	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	54	80	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	36	80	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	50	80	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	71	80	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	40	80	REPETIBLE
A.18	CUMPLIMIENTO	63,5	80	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**58**	**80**	EFECTIVO

Ilustración 9. Resultados por Dominio.

Nivel de cumplimiento general – ISO 27001:2013

Con base en los resultados obtenidos a continuación, se presentan los resultados generales de cumplimiento de la norma ISO 27001:2013.

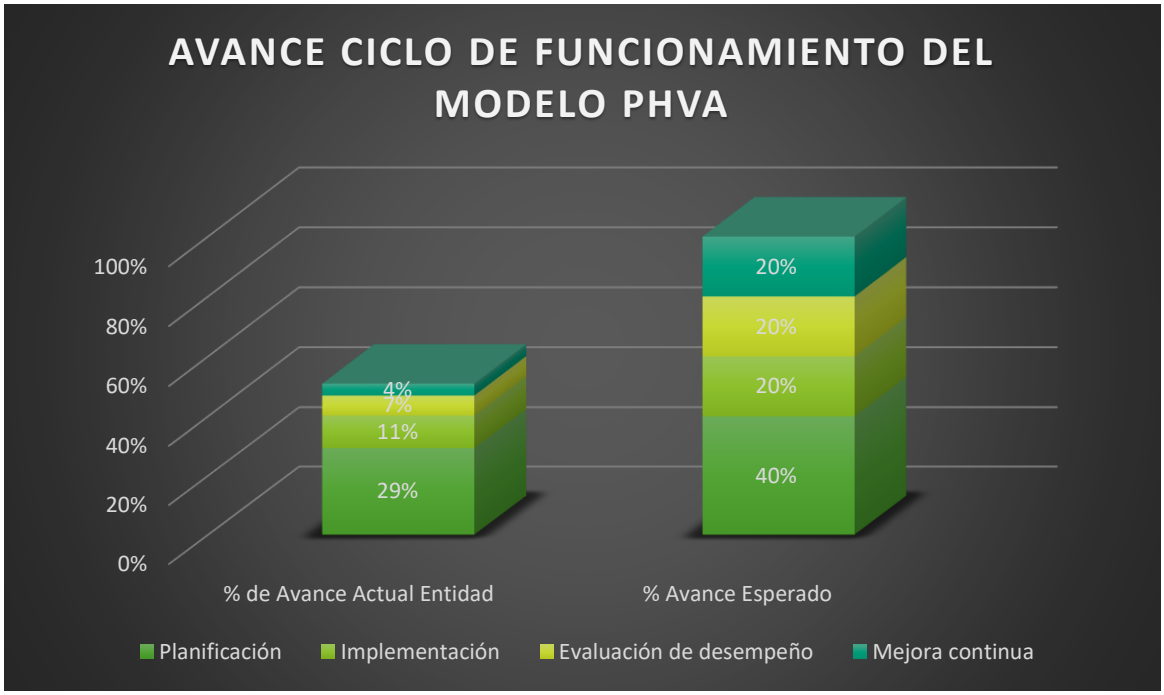


Ilustración 10. Resultado grafico del cumplimiento ISO 27001:2013 PHVA

Se puede concluir que se observan importante oportunidad de mejora, con respecto a la norma internacional ISO/IEC 27001:2013 se obtuvo un puntaje de cumplimiento del 51%, y para la efectividad de los controles de seguridad 27002:2013 se obtuvo un 58%. Por lo anterior, es perentorio que el portafolio de proyectos de seguridad de la información debe incluir un proyecto que permita el fortalecimiento y mejoramiento del sistema de gestión de seguridad de la información para el ICA.

9.3 ANALISIS Y PRIORIZACION DE INICIATIVAS DE SEGURIDAD DE LA INFORMACION

Teniendo en cuenta el resultado anterior, se identifican las iniciativas de seguridad de la información, los cuales deben estar alineadas al plan estratégico del ICA , y a los resultados de la calificación actual del instrumento de diagnóstico del Modelo de seguridad y privacidad de la

información . De otra parte, es importante que las iniciativas estén enmarcadas dentro de los controles sugeridos para garantizar una adecuada arquitectura de seguridad de la información y un esquema de defensa a profundidad utilizando soluciones y tendencias de seguridad de la información y de tecnología. Estas iniciativas fueron seleccionadas de acuerdo al nivel de madurez de cada Dominio teniendo como referencia la calificación actual obtenida menor al 60 % de efectividad :

INICIATIVAS	DESCRIPCION DE LAS INICIATIVAS	Estrategia Seguridad de la Información			
		Gobierno o Modelo de seguridad de información	Gestión de riesgos de Seguridad	Desarrollo y gestión del programa de seguridad de la información.	Gestión de incidentes de seguridad de la información.
I.00	Planificación y control operacional, Elaborar el plan estratégico de seguridad de la información .	X			
I.01	Definir e integrar la seguridad de la información en el ciclo de vida de los proyectos para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.	X			
I.02	Diseñar y documentar un programa anual de capacitación y sensibilización en seguridad de la información para empleados, proveedores y terceros del ICA	X			
I.03	Implementar el programa anual de capacitación y sensibilización en seguridad de la información para empleados, proveedores y terceros del ICA	X			

I.04	Definir y adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles y el teletrabajo.			X	
I.05	Actualizar los activos de información y realizar su valoración según la criticidad para la compañía, igualmente identificar los riesgos de seguridad de la información asociados .		X		
I.06	Identificar los riesgos de seguridad de la información para cada uno de los procesos .		X		
I.07	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.		X		
I.08	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos de la Entidad.		X		
I.09	Implementar , Documentar y realizar pruebas de los planes de continuidad de negocio, así mismo Aprobar los planes de continuidad por la alta dirección.		X		
I.10	Diseñar y documentar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.	X			
I.11	Ejecutar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad	X			
I.12	Implementar arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.			X	

I.13	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la confidencialidad de la información.			X	
I.14	Definir y establecer la metodología de desarrollo seguro			X	
I.15	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.			X	
I.16	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.			X	
I.17	Definir e implementar una política sobre el uso de controles criptográficos para la protección de la información en la organización.			X	
I.18	Monitorear a los terceros periódicamente para verificar que los controles de seguridad, los acuerdos de servicio definidos y demás requerimientos de seguridad que se contrataron están siendo implementados, operados y mantenidos.				X
I.19	Implementar la gestión centralizada de usuarios para todos los aplicativos del negocio .			X	
I.20	Implementar una solución de gestión de identidades para usuarios privilegiados			X	
I.21	Implementar una solución como servicio de borrado seguro de información			X	

I.22	Implementar como servicio una solución de anti malware avanzado para la protección contra amenazas avanzadas persistentes (APT).			X	
I.23	Establecer e implementar pruebas, análisis y gestión de vulnerabilidades a los elementos de mayor criticidad tanto a nivel de infraestructura como a nivel de aplicaciones web.			X	
I.24	Establecer e implementar pruebas de Hacking Ético sobre los aplicativos críticos.			X	
I.25	Implementar una solución que permite la transferencia segura de archivos, mediante protocolos de cifrado de comunicaciones.			X	
I.26	Implementar una solución de DLP (Data Loss Prevention), con el fin de controlar y monitorear el intercambio de información confidencial y/o sensible.			X	
I.27	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web			X	
I.28	Implementar un correlacionador de eventos (SIEM) como servicios para monitorear el comportamiento de activos de información críticos.			X	
I.29	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la compañía.			X	
I.30	Asegurar el uso y adaptación e entornos de computación en la nube			X	
I.31	Implementar y monitorear los indicadores del sistema de gestión de seguridad de la información				X
I.32	Entrenamiento a los equipos de recuperación de los procesos críticos del negocio	X			

Tabla 3. Iniciativas de Seguridad de la información versus objetivos estratégicos de SI.

9.4 DEFINICIÓN DEL PORTAFOLIO DE PROYECTOS DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa, después del análisis y priorización de iniciativas, se define el portafolio de proyectos del plan estratégico PESI , agrupados en proyectos relacionados con:

- ✓ Gobierno o modelo de seguridad de información.
- ✓ Gestión de riesgos de Seguridad.
- ✓ Desarrollo y gestión del plan de seguridad de la in formación.
- ✓ Gestión de incidentes de seguridad de la información.

PROYECTOS DE SEGURIDAD DE LA INFORMACION

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
P00	Elaboración plan estratégico de seguridad de la información.	I.00	Planificación y control operacional, Elaborar el plan estratégico de seguridad de la información .	EN PROCESO	NO
P.01	Integrar los componentes del sistema de gestión de seguridad de la información en el ciclo de vida de	I.01	Definir e integrar la seguridad de la información en el ciclo de vida de los proyectos para asegurar que los	NO INICIADO	NO

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
	los proyectos del ICA		riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.		
P.02	Desarrollar el programa de capacitación y sensibilización en seguridad de la información para empleados , contratistas proveedores y terceros.	I.02	Diseñar y documentar un programa anual de capacitación y sensibilización en seguridad de la información para empleados, proveedores y terceros del ICA	EN PROCESO	SI
		I.03	Implementar el programa anual de capacitación y sensibilización en seguridad de la información para empleados, proveedores y terceros del ICA		
P.03	Sistema de control de acceso para dispositivos móviles e Implementación VPN'S en Teletrabajo.	I.04	Definir y adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el	NO INICIADO	SI

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
			uso de dispositivos móviles y el teletrabajo.		
P.04	Gestión de Riesgos de Seguridad de la información	I.05	Actualizar los activos de información y realizar su valoración según la criticidad para la compañía, igualmente identificar los riesgos de seguridad de la información asociados .	EN PROCESO	NO
		I.06	Identificar los riesgos de seguridad de la información para cada uno de los procesos .		
		I.07	Gestionar el Tratamiento de riesgos de seguridad de la información de los riesgos identificados en cada uno de los procesos.		

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
P.05	Desarrollo y Gestión del plan de continuidad del Negocio	I.08	Diseñar los planes de continuidad del negocio que contemplen los procesos críticos de la Entidad.	NO INICIADO	SI
		I.09	Implementar y Documentar los planes de continuidad de negocio, así mismo Aprobar los planes de continuidad por la alta dirección.		
P.06	Desarrollo y Gestión del programa de Recuperación ante desastres.	I.10	Diseñar y documentar el programa de ejercicios al plan de recuperación ante desastres, ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad.	NO INICIADO	SI
		I.11	Ejecutar el programa de ejercicios al plan de recuperación ante desastres,		

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
			ante escenarios de fallas de las tecnologías, garantizando que se mantengan los controles de seguridad		
P.07	Gestionar la adquisición de herramientas para soportar la infraestructura del Datacenter , en esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.	I.12	Implementar arquitecturas redundantes en dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.	NO INICIADO	SI
P.08	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.13	Definir y establecer un procedimiento formal para el tratamiento de información de producción en ambientes de desarrollo y prueba, en el cual se establezcan controles para proteger la	INICIADO	NO

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
			confidencialidad de la información.		
P.09	Adaptación de metodología para el desarrollo Seguro en las aplicaciones.	I.14	Definir y establecer la metodología de desarrollo seguro	NO INICIADO	NO
P.10	Gestión de accesos y privilegios de TI	I.15	Definir y establecer las políticas y procedimientos relacionados con la gestión de usuarios privilegiados que administren las plataformas tecnológicas (servidores, elementos de red, bases de datos), así como a las funciones de negocio que requieren el uso de privilegios.	NO INICIADO	NO

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
		I.16	Monitorear el cumplimiento del ciclo de vida de gestión de usuarios (creación, modificación, activación, desactivación, eliminación, entre otros) verificando que se cumple para todas las aplicaciones.		
P.11	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.17	Definir e implementar una política sobre el uso de controles criptográficos para la protección de la información en la organización.	INICIADO	NO
P.12	Evaluación y desempeño de proveedores y terceras partes .	I.18	Monitorear a los terceros periódicamente para verificar que los controles de seguridad, los acuerdos de servicio definidos y demás requerimientos de seguridad que se	INICIADO	NO

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
			contrataron están siendo implementados, operados y mantenidos.		
P.13	Gestión de accesos y privilegios de TI	I.19	Implementar la gestión centralizada de usuarios para todos los aplicativos del negocio .	NO INICIADO	NO
P.14	Gestión de herramienta para cuentas privilegiadas	I.20	Implementar una solución de gestión de identidades para usuarios privilegiados	NO INICIADO	SI
P.15	Implementación de Software para borrado seguro de Información	I.21	Implementar una solución como servicio de borrado seguro de información	NO INICIADO	SI
P.08	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.22	Implementar como servicio una solución de anti malware avanzado para la protección contra amenazas avanzadas persistentes (APT).	INICIADO	NO

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
P.16	Adquisición de Software o servicio de análisis de vulnerabilidades y hacking Ético	I.23	Establecer e implementar pruebas, análisis y gestión de vulnerabilidades a los elementos de mayor criticidad tanto a nivel de infraestructura como a nivel de aplicaciones web.	EN PROCESO	NO
		I.24	Establecer e implementar pruebas de Hacking Ético sobre los aplicativos críticos.		
P.17	Herramientas de cifrado de información automatizados , Repositorio centralizado de información cifrada.	I.25	Implementar una solución que permite la transferencia segura de archivos, mediante protocolos de cifrado .	EN PROCESO	NO
P.18	Gestionar una solución de DLP (Data Loss Prevention) para el correo Electrónico y equipos críticos.	I.26	Implementar una solución de DLP (Data Loss Prevention), con el fin de controlar y monitorear el intercambio de	INICIADO	SI

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
			información confidencial y/o sensible.		
P.19	Gestionar una herramienta WAF para la protección de las aplicaciones WEB del ICA	I.27	Implementar una solución como servicio de Firewall de aplicaciones Web para la protección de aplicaciones Web	NO INICIADO	SI
P.20	Gestionar una solución de correlacionador de eventos (SIEM) como servicio, para monitorear el comportamiento de activos de información críticos.	I.28	Implementar un correlacionador de eventos (SIEM) como servicios para monitorear el comportamiento de activos de información críticos.	NO INICIADO	SI
P.07	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información ,incluyendo todos los procesos de la compañía.	I.29	Operar y mantener el sistema de gestión de seguridad de la información SGSI, incluyendo todos los procesos de la compañía.	EN PROCESO	NO

No. PROYECTO	DESCRIPCION DEL PROYECTO	INICIATIVA	DESCRIPCION DE INICIATIVAS	AVANCES	RECURSOS FINANCIEROS
P.07	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	I.30	Asegurar el uso y adaptación e entornos de computación en la nube	EN PROCESO	NO
P.11	Evaluación y desempeño del sistema de Gestión de seguridad de la información	I.31	Implementar y monitorear los indicadores de gestión y desempeño del sistema de gestión de seguridad de la información	INICIADO	NO
P.05	Desarrollo y Gestión del programa de continuidad del Negocio.	I.32	Entrenamiento a los equipos de recuperación de los procesos críticos del negocio	NO INICIADO	NO

Tabla 4. Portafolio de proyectos

10 ALINEACIÓN PESI Y PETIC

La alineación del PESI y PETI busca sincronizar los objetivos estratégicos de TI (PETI), el cual define lineamientos para el mejoramiento del nivel de madurez institucional en la implementación de soluciones tecnológicas que generen valor y promuevan el cumplimiento de la misión con sostenibilidad tecnológica. Así mismo el PESI define objetivos que permiten asegurar la confidencialidad, integridad

y disponibilidad de los activos de información . para ello se establecen los objetivos de TI que están directamente involucrados en el plan estratégico de seguridad de la información.

# de objetivo PETI	Objetivo
1.	Alinear la estrategia de TI con la estrategia del ICA y del sector agricultura, así como del Gobierno Nacional
2.	Maximizar el aporte de las TIC a los procesos internos para la transformación del ICA.
3.	Ejercer el Gobierno de las TIC del ICA.
4.	Posicionarse como aliado estratégico de todos los procesos internos del ICA.
5.	Mejorar la satisfacción de los usuarios, así como la del ciudadano que utiliza los servicios del ICA.
6.	Proveer información oportuna y de calidad para la toma de decisiones en los procesos internos del ICA.
7.	Entregar oportunamente sistemas de información de calidad, funcionales, eficientes y confiables fortaleciendo los procesos internos del ICA.
8.	Fortalecer la Gestión de las TIC y de la seguridad de la información en los procesos internos del ICA.
9.	Fortalecer las competencias y desarrollo profesional del equipo de TI del ICA.
10.	Desarrollar la capacidad de innovación y prospectiva tecnológica.

.

Tabla 5. Alineación PESI con PETIC.

De los anteriores objetivos del PETI el número 8 y 9 están relacionados con el sistema de gestión de seguridad de la información.

Dominio	Objetivo del PESI	# de objetivo del PETIC	Estado Actual	Nivel
A.5. Políticas de la seguridad de la información	La adopción de políticas de seguridad de la información debe obedecer a una decisión estratégica, las cuales servirán de directrices para proteger la información de propiedad del ICA.	8	**100%**	**OPTIMIZADO**
A.6. Organización de la seguridad de la información	La definición de los roles y responsabilidades para la seguridad de la información es el aspecto fundamental para iniciar y controlar la implementación y la operación de lo relacionado con la protección de la información propiedad del ICA.	8	**52%**	**EFECTIVO**
A.7. Seguridad de los recursos humanos	Las personas son el componente más importante en todo el modelo de seguridad de la información, por lo tanto, antes de su contratación, durante su permanencia y en el proceso de finalización o cambios de cargo, la entidad debe asegurar que los funcionarios y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	8 y 9	**98%**	**OPTIMIZADO**
A.8. Gestión de activos	Identificar los activos de información y definir las responsabilidades de protección apropiadas, asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización y evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios; son las principales razones de la entidad para garantizar la gestión adecuada de los activos y la asignación de las respectivas responsabilidades sobre los mismos.	8	**45%**	**EFECTIVO**
A.9. Control de acceso	Las técnicas de control de acceso permiten proteger la información en términos de la confidencialidad, la integridad y la disponibilidad.	8	**44%**	**EFECTIVO**
A.10. Criptografía	Las técnicas de cifrado ayudan a proteger la información de acuerdo a su nivel de clasificación, la implementación de éstas, el uso apropiado y eficaz de la criptografía permiten proteger la confidencialidad, la autenticidad y/o la integridad de la información propiedad de la entidad.	8	**60%**	**EFECTIVO**
A.11. Seguridad física y del entorno	La debida protección de los centros de datos, archivos documentales, equipos, oficinas, entre otros, es un aspecto que se debe considerar cuando se trate de la seguridad de la información.	8	**63%**	**GESTIONADO**
A.12. Seguridad de las operaciones	Lograr que las operaciones protejan la información debe ser un compromiso de la entidad.	8	**42%**	**EFECTIVO**
A.13. Seguridad de las comunicaciones	La transferencia de información está expuesta a múltiples riesgos, por ello la entidad debe implementar medidas preventivas para evitar su divulgación o modificación.	8	**54%**	**EFECTIVO**
A.14. Adquisición, desarrollo y mantenimiento de sistemas	Mantener la seguridad de la información durante el ciclo de desarrollo requiere contar con una metodología de desarrollo seguro. Las aplicaciones normalmente mantienen información importante de la entidad, por esta razón se deben implementar controles de seguridad dentro de ellas.	8	**36%**	**REPETIBLE**
A.16. Gestión de incidentes de seguridad de la información	La adecuada gestión de los incidentes de seguridad de la información permite proteger los tres pilares de la seguridad: la confidencialidad, la integridad y la disponibilidad de la información. La implementación de estos controles permite asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.	8	**71%**	**GESTIONADO**
A.17. Aspectos de seguridad de la información de la gestión de continuidad de negocio	Poder contar con planes para la continuidad del negocio y la recuperación ante desastres es importante para preservar la disponibilidad de la información. La entidad debe adoptar estos controles para asegurar la disponibilidad de las instalaciones de procesamiento de información durante una situación adversa, adicionalmente debe verificar a intervalos regulares dichos controles con el fin de asegurar que son válidos y eficaces.	8	**40%**	**REPETIBLE**
A.18. Cumplimiento	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad es importante para no incurrir en demandas, multas u otra clase de afectación a la imagen o a las finanzas de la entidad.	8	**63.5%**	**GESTIONADO**

Tabla 6. Alineación del PESI con PETIC.

11 INFORME DE RESULTADOS

11.1 PRIORIZACION DEL PORTAFOLIO DE PROYECTOS

Una vez identificadas las iniciativas y los proyectos con base en el resultado de diagnóstico de la situación actual del instrumento del MSPI de MINTIC, es necesario priorizar los proyectos , para lo cual se tuvo en cuenta la estrategia de seguridad de la información (Gobierno o Modelo de seguridad de información, Gestión de riesgos de Seguridad , Desarrollo y gestión del programa de seguridad de la información y Gestión de incidentes de seguridad de la información). Para ello se construyeron las siguientes categorías de prioridad que permiten evaluar y determinar una secuencia sistemática para el desarrollo del Plan Estratégico de seguridad de la Información (PESI):

PRIORIDAD	
PRIORIDAD	**DESCRIPCION**
0	Elaboración del presente Plan Estratégico de Seguridad de la Información.
1	Gobierno o Modelo de seguridad de información, el cual Incluye las iniciativas que soportan el desarrollo del modelo de seguridad de la informacion .
2	Gestion de Riesgos Operacionales: Hace referencia a los proyectos y actividades que mitigan los riesgos de seguridad de la información catalogados como relevantes, garantizando salvaguardar la información en su confidencialidad, disponibilidad e integridad.
3	Desarrollo y gestión del programa de seguridad de la información; hace refencia aquellos proyectos que permiten la Operación y mantenimiento del Sistema de Gestión de Seguridad de la información .
4	Desempeño: Soportan aquellos proyectos que permiten la evaluacion del desempeño y mejora continua del SGSI.

Tabla 7. Criterios para priorización de proyectos.

A continuación, se presenta por prioridad los proyectos que se deben desarrollar a partir de la vigencia 2017 y hasta la vigencia 2022.

PRIORIZACION DE LOS PROYECTOS

No. PROYECTO	NOMBRE DEL PROYECTO	PRIORIDAD (0) Año 2017	PRIORIDAD (1) Año 2018	PRIORIDAD (2) Año 2019	PRIORIDAD (3) Año 2020 - Año 2021	PRIORIDAD (4) Año2021 - Año 2022
P00	Elaboración plan estratégico de seguridad de la información	X				
P.01	Integrar los componentes del sistema de gestión de seguridad de la información en el ciclo de vida de los proyectos del ICA		X			
P.02	Desarrollar el programa de capacitación y sensibilización en seguridad de la información para empleados , contratistas proveedores y terceros .	X	X			
P.03	Sistema de control de acceso para dispositivos móviles e Implementación VPN'S en Teletrabajo.		X			
P.04	Gestión de Riesgos de Seguridad de la información	X	X			
P.05	Desarrollo y Gestión del programa de continuidad del Negocio.		X	X		

P.06	Desarrollo y Gestión del programa de Recuperación ante desastres.		X	X		
P.07	Gestionar la adquisición de herramientas para soportar la infraestructura del Datacenter en esquemas de alta disponibilidad para dispositivos de seguridad Firewall y Dispositivos de comunicaciones Core.		X			
P.08	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	X	X			
P.09	Adaptación de metodología para el desarrollo Seguro en las aplicaciones.		X	X		
P.10	Gestión de accesos y privilegios de TI		X	X	X	
P.11	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	X	X			
P.12	Evaluación y desempeño de		X			

	proveedores y terceras partes .					
P.13	Gestión de accesos y privilegios de TI		X	X	X	
P.14	Gestión de herramienta para cuentas privilegiadas				X	
P.15	Implementación de Software para borrado seguro de Información				X	
P.08	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información	X	X			
P.16	Adquisición de Software o servicio de análisis de vulnerabilidades y hacking Ético	X	X	X	X	X
P.17	Herramientas de cifrado de información automatizados , Repositorio centralizado de información cifrada.	X	X			
P.18	Gestionar una solución de DLP (Data Loss Prevention) para el correo Electrónico y equipos críticos.				X	
P.19	Gestionar una herramienta WAF para la protección de las aplicaciones WEB del ICA			X		

P.20	Gestionar una solución de correlacionador de eventos (SIEM) como servicio, para monitorear el comportamiento de activos de información críticos.				X	
P.07	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información ,incluyendo todos los procesos de la compañía.	X	X			
P.07	Operación y mantenimiento del Sistema de Gestión de Seguridad de la información					X
P.11	Evaluación y desempeño del sistema de Gestión de seguridad de la información				X	X
P.05	Desarrollo y Gestión del programa de continuidad del Negocio.		X	X		

Tabla 8. Prioridad de Proyectos año 2017- año 2022

12 PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

El plan estratégico corresponde a la ejecución de los proyectos definidos en el portafolio de proyectos de seguridad de la información que aportan al cumplimiento de los objetivos de seguridad de la información y al plan estratégico TIC (PETI).

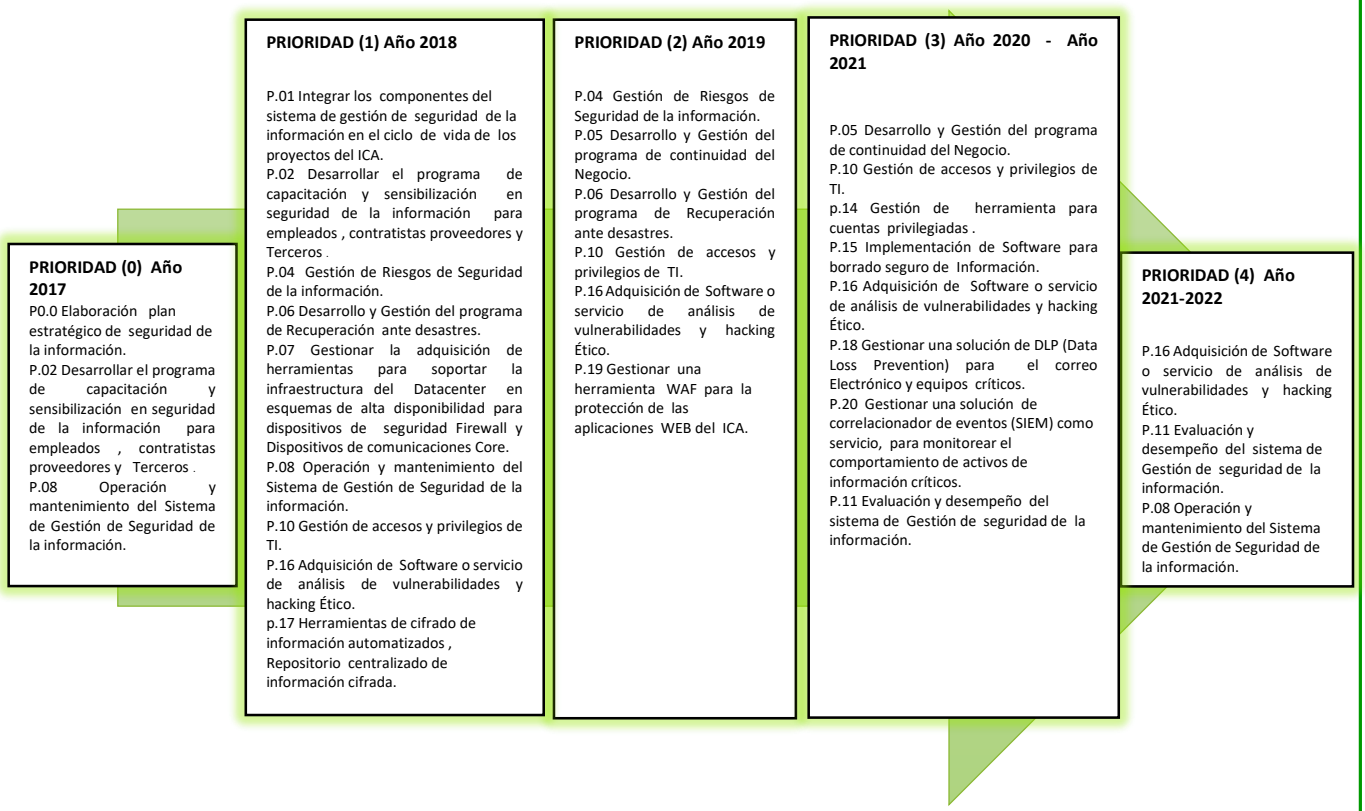


Ilustración 11. Plan estratégico de seguridad de la información PESI

13 CONCLUSIONES

El diseño de un plan Estratégico para la Gestión de Seguridad de la Información basado en el modelo de mejores prácticas y lineamientos de seguridad, como es la Norma internacional ISO/IEC 27001:2013 y la ISO/IEC 27002:2013, y el alineamiento del plan estratégico del ICA con los objetivos estratégicos de seguridad de la información, El PESI un herramienta de gran ayuda que permite identificar los diferentes proyectos de seguridad de la información que debe adelantar el ICA de manera que permita cumplir y mantener el Sistema de gestión de Seguridad de la información y el modelo de seguridad y privacidad de la información , todo lo anterior, se cumple si se forja en el tiempo un adecuado y sostenible Sistema de Gestión de Seguridad de la Información.

Ahora es muy importante contar desde el inicio con el apoyo y la aprobación de la alta dirección del ICA y con el compromiso de todas las áreas involucradas en el proceso, el portafolio de proyectos que tendrá el plan estratégico deben ser desarrollados y ejecutados para lograr un sistema de seguridad de la información conforme a los más altos estándares de seguridad, cumpliendo los requisitos y temas regulatorios y lo más relevante, lograr apalancar el cumplimiento de los objetivos estratégicos de la entidad.

14 ANEXOS

14.1 INDICE DE ILUSTRACIONES

14.2 INDICE DE TABLAS