SISTEMA DE GESTIÓN INTEGRADO

PROCESO GOBERNABILIDAD TICS	
SUBPROCESO O ACTIVIDAD SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	

Plan de Seguridad y Privacidad de la Información

Instituto Colombiano Agropecuario - ICA

Marzo 2022

El presente Plan hace parte integral del Sistema de Gestión de Seguridad de la información – SGSI.
Aprobado en Sesión III – 2022. Comité Institucional de Gestión y Desempeño (Ordinaria) del 18 de Marzo de 2022.

TABLA DE CONTENIDO

INTRODUCCIÓN

El Instituto Colombiano Agropecuario – ICA, establece el Plan de Seguridad y Privacidad de la Información con el fin de dar cumplimiento a los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, frente a la aplicación de la Política de Seguridad y Privacidad de la Información propia del Instituto Colombiano Agropecuario ICA, la Política de Gobierno Digital y la implementación del Sistema de Gestión de Seguridad de la Información "SGSI" de la entidad.

1. TERMINOS Y DEFINICIONES

- **Acceso lógico:** Es un acceso en red a través de la ICAnet de la Entidad o de Internet.

- **Activos de Información:** Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensitivos o críticos para los objetivos del proceso.

- **Almacenamiento:** Se refiere a la forma en la que se almacena el activo, como en medios magnéticos, salas, cajas, PC's, Servidores, CD's, DVD's, USBs, Cintas magnéticas, etc.

- **Área solicitante[1]:** Es la dependencia del Instituto Colombiano Agropecuario ICA que solicita al Funcionario competente y/u ordenador del gasto, la contratación de Bienes o Servicios para satisfacer necesidades o solucionar problemas.

- **Autorización[2]:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

- **Base de Datos[3]:** Conjunto organizado de datos personales que sea objeto de Tratamiento;

- **Cifrado:** Es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación (letras, símbolos o números) del contenido que solo pueden comprenderse si se dispone de la clave necesaria para descifrarlos).

- **Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la Entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado. La información debe clasificarse en términos de sensibilidad e importancia para la Entidad.

- **Complementario**: Hace referencia a todo aquel elemento, objeto, individuo o fenómeno que se caracteriza por unirse a otro elemento para completarlo y, en lo posible, mejorarlo.

- **Confidencialidad**: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

- **Contraseña**: Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.

---

[1] **Fuente**: Definiciones - Manual de Contratación GRFT-GC-MP-001
[2] Fuente: Definiciones Ley 1581 de 2012
[3] Fuente: Definiciones Ley 1581 de 2012

- **Contratista**: Persona natural o jurídica que se vincula a la entidad con el objeto de prestar al Instituto un bien o un servicio determinado.

- **Control o Medida:** Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

- **Creación:** Se refiere a la concepción de documentos o datos, el momento en el cual se origina el contenido (digital o físico) de un medio de información.

- **Custodio**: Persona delegada para ejercer el cuidado o vigilancia sobre un activo que le ha sido encargado.

- **Dato personal[4]:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **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.

- **Destrucción:** Se refiere a la actividad para la destrucción de la información que se maneja sobre el activo en el momento en el que este finaliza su ciclo de vida:

  - Incineración: Destrucción de información exponiéndola a altas temperaturas para quemarla.

  - Borrado Seguro: Aplica solo para medio magnéticos, es un borrado a bajo nivel.

  - Trituración: Esto aplica más que todo a la destrucción de papel por medio de máquinas trituradoras.

- **Dominio**: Áreas en las que se desarrolla la NTC/ISO 27001.

- **Encargado del Tratamiento[5]:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

- **Etiquetado**: Colocar una etiqueta o rótulo para identificar un elemento.

- **Evento de Seguridad de la Información:** Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Excepciones**: Todo aquello que se excluye de la generalidad o regla común.

- **ICAnet:** Hace referencia a la Intranet del Instituto Colombiano Agropecuario – ICA.

- **Incidente de seguridad de la Información:** Un evento o serie de eventos de seguridad de la Información no deseados o inesperados, que tiene una la probabilidad significativa de comprometer las

[4] Fuente: Definiciones Ley 1581 de 2012
[5] Fuente: Definiciones Ley 1581 de 2012

operaciones del negocio o amenazar la seguridad de la información de los activos críticos que almacenen, procesen y/o gestionen información.

- **Integridad**: Propiedad de Salvaguardar la exactitud y estado completo de los activos.
- **Inventario de activos:** Listado de recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.)
- **Lineamientos**: Describe en orden numérico y de acuerdo a su importancia las directrices específicas establecidas para la aplicación de la política.
- **Medio Removible:** Dispositivos de almacenamiento independientes del computador que pueden ser transportados libremente. Los dispositivos móviles más comunes son: Memorias USB, discos duros extraíbles, DVD y CD.
- **Política de seguridad de la información:** Establece a alto nivel los objetivos y metas relacionados con la seguridad de la información.
- **Programas Utilitarios**: Los utilitarios o utilidades, son programas diseñados para realizar una función determinada, por ejemplo, un editor, un depurador de código o un programa para recuperar datos perdidos o borrados accidentalmente en el disco duro.
- **Propietario de la información**: Es el responsable de 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.
- **Responsable del Tratamiento[6]:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.
- **Rol:** El papel que desempeña un individuo o un grupo en una actividad determinada.
- **Seguridad de la Información:** Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.
- **Servidor Público**: Es una persona que desempeña un empleo público. Se trata de un trabajador que cumple funciones en el organismo del estado.
- **Sistema de procesamiento de información**: Es un sistema que transforma los datos en información organizada, significativa y útil.
- **Teletrabajador:** Es la persona que utiliza las tecnologías de la información y comunicación como medio para realizar su actividad laboral fuera del local del empleador, en el marco de un contrato de trabajo o de una relación laboral dependiente, en la cual le sean garantizados todos sus derechos laborales.
- **Teletrabajo:** Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la

[6] Fuente: Definiciones Ley 1581 de 2012

información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo[7].

- **Titular**[8]: Persona natural cuyos datos personales sean objeto de Tratamiento.
- **Token de seguridad:** (también token de autenticación o token criptográfico) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación. Los tokens electrónicos se usan para almacenar claves criptográficas como firmas digitales o datos biométricos, como las huellas digitales.
- **Transporte de datos:** Considera las diferentes formas en la que se transporta la información de un lado a otro y los cuidados que se debe tener en este proceso, según su nivel de clasificación.
- **Tratamiento**[9]**:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Usuario**: Es un individuo que utiliza una computadora, un sistema operativo o cualquier sistema informático. Por lo general es una única persona.
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.
- **VPN**: (Virtual Private Network) Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

2. OBJETIVO

- Definir y aplicar los lineamientos para tratar de manera integral los Riesgos de Seguridad y Privacidad de la información, Seguridad Digital y continuidad de la Operación de los Servicios de la Entidad, que pueda afectar al Instituto Colombiano Agropecuario “ICA”, con el fin de alcanzar los objetivos, la misión y la visión institucional, preservando la Confidencialidad, Integridad y Disponibilidad de la información.
- Gestionar Riesgos de Seguridad y Privacidad de la información identificados de acuerdo al tratamiento establecido.
- Fortalecer y apropiar el conocimiento al interior de los procesos referente a la gestión de Riesgos Seguridad y Privacidad de la información.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.

7 Fuente: Definiciones Ley 1221 de 2008
8 Fuente: Definiciones Ley 1581 de 2012
9 Fuente: Definiciones Ley 1581 de 2012

3. ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información se aplica a todos los procesos del Instituto Colombiano Agropecuario - ICA, en concordancia con el alcance del Sistema de Gestión de Seguridad de la Información – SGSI, el cual hace parte del Sistema Integrado de Gestión “SIG” de la Entidad.

4. POLÍTICA DE ALTO NIVEL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI.

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** para prevenir incidentes y propender por la continuidad de los servicios, con el fin de dar cumplimiento a 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”.

4.1. OBJETIVOS DEL SGSI

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:

- 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.
- Identificar y valorar los Activos de Información con los que cuenta la entidad, en términos de Confidencialidad, Integridad y Disponibilidad.
- Divulgar las Políticas de Seguridad y Privacidad de la Información definida a todos Funcionarios, Contratistas, Proveedores y/o Terceros de la Entidad.
- Controlar y prevenir los incidentes de Seguridad de Información.
- Desarrollar un Plan de Cultura de Seguridad de Información al interior de la Entidad.

4.2. 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.

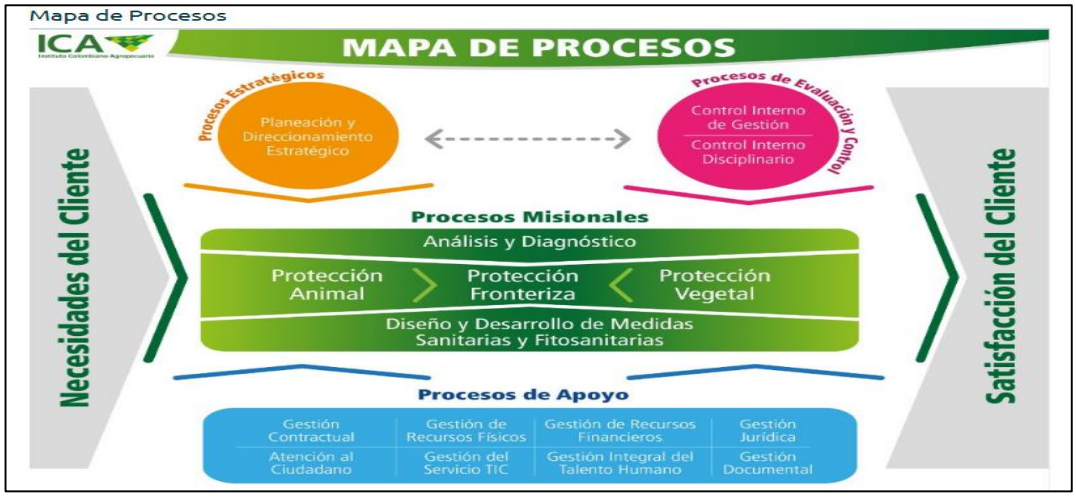

Imagen No. 1- Mapa de procesos y alcance del SGSI

5. 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:

Imagen No. 2 - Interfaces y dependencias del SGSI[10]

6. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones del Comité de Seguridad de la Información son asumidas por el Comité de Gestión y Desempeño del Instituto Colombiano Agropecuario "ICA", de acuerdo al Decreto 1499 de 2017 por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015, en el artículo 2.2.22.3.8 Comités Institucionales de Gestión y desempeño.

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

7. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFROMACION

Para la vigencia 2022, se definen las siguientes actividades para el desarrollo del Plan de Seguridad y Privacidad de la Información:

GESTIÓN	ACTIVIDAD	TAREA	RESPONSABLE DE LA TAREA	RECURSOS	ENTREGABLE	FECHAS PROGRAMADAS	
						FECHA INICIO	FECHA FIN
Activos de Información.	Definir lineamiento para el levantamiento de activos de información	Actualización del Procedimiento e instrumento (formato) de levantamiento de activos de información.	Oficina de Tecnología de la Información	Recursos Humanos	Procedimiento de activos de información. Instrumento (formato) de activos de información	Marzo 2022	Abril 2022
		Aprobación del Procedimiento e instrumento (formato) de levantamiento de activos de información.	Jefe Oficina de Tecnologias de la Información	Recursos Humanos	Publicación del procedimiento e instructivo (formato) de activos de información	Abril 2022	Abril 2022
	Actualización del inventario de activos de información.	Validar los activos de información con la matriz de activos de la vigencia anterior. Identificar nuevos activos de información en cada dependencia	Oficina de Tecnología de la Información Dueños de Procesos	Recursos Humanos	Instrumento (formato) de activos de información diligenciado y actualizado	Abril 2022	Junio 2022
		Realizar consolidado de activos de información	Oficina de Tecnología de la Información	Recursos Humanos	Consolidado del Instrumento (formato) de activos de información diligenciado y actualizado.	Abril 2022	Junio 2022
	Aceptación de Activos de Información.	Notificar a las dependencias la actualización de activos de información para su aceptación y posterior publicación.	Oficina de Tecnología de la Información	Recursos Humanos	Envío del total de activos pro área, grupo oficina y/o proceso.	Abril 2022	Junio 2022
	Aprobación de Activos de Información.	Entregar consolidado de activos de información para aprobación del Comité de Gestión y Desempeño del ICA, para proceder a realizar el esquema de publicación y clasificación.	Oficina de Tecnología de la Información	Recursos Humanos	Consolidado del Instrumento (formato) de activos de información diligenciado y actualizado.	Abril 2022	Junio 2022
		Entregar del consolidado final de activos de información a la OAP, OAC y OAJ.	Oficina de Tecnología de la Información	Recursos Humanos	Consolidado del Instrumento (formato) de activos de información diligenciado y actualizado.	Junio 2022	Junio 2022

	Publicación de Activos de Información.	Realizar el esquema de publicación de la información.	Oficina Asesora de Comunicaciones – OAC Oficina Asesora de Planeacion OAP -	Recursos Humanos	Publicación en la página web de la entidad, espacio de transparencia.	Junio 2022	Julio 2022
		Realizar índice de información clasificada y reservada – IICR.	Oficina Asesora de Jurídica – OAJ.	Recursos Humanos		Junio 2022	Julio 2022
Gestión de Riesgos.	Definir lineamiento para la identificación de Riesgos de Seguridad.	Actualización de la Guía para la Administración en el capítulo de Riesgos de Seguridad Digital y el instrumento para diligenciamiento de Riesgos de Seguridad Digital.	Oficina de Tecnología de la Información.	Recursos Humanos	Guía para la Administración de Riesgos de Seguridad Digital. Instrumento (formato) de Riesgos de seguridad Digital.	Marzo 2022	Abril 2022
		Aprobación y publicación de la Guía para la Administración en el capítulo de Riesgos de Seguridad Digital.	Oficina Asesora de Planeación – OAP.	Recursos Humanos	Publicación de la Guía para la Administración.	Marzo 2022	Abril 2022
	Identificación de Riesgos de Seguridad Digital.	Identificación, análisis y evaluación de Riesgos de Seguridad Digital.	Oficina de Tecnología de la Información. Dueños de los Procesos.	Recursos Humanos	Instrumento (formato) de Riesgos de seguridad Digital. diligenciado y actualizado.	Abril 2022	Junio 2022
	Aceptación y aprobación de Matriz de Riesgos de Seguridad y Planes de Tratamiento.	Aceptación y aprobación de la Matriz de Riesgos de Seguridad Digital y sus Planes de Tratamiento.	Dueños de los Procesos.	Recursos Humanos Recursos Financiero	Envío del total de Riesgos de Seguridad Digital por área, oficina, grupo y/o proceso	Abril 2022	Junio 2022
	Publicación de la Matriz de Riesgos de Seguridad.	Publicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Oficina Asesora de Planeación – OAP.	Recursos Humanos	Espacio definido por la Oficina Asesora de planeación – OAP.	Julio 2022	Julio 2022
	Seguimiento al Tratamiento de Riesgos de Seguridad.	Seguimiento al estado de los planes de tratamiento de Riesgos de Seguridad identificados y verificación de evidencias.	Oficina de Tecnología de la Información.	Recursos Humanos	Instrumento (formato) de Riesgos de seguridad Digital donde se visualiza el seguimiento Plan de Tratamiento	Julio 2022	Dic 2022
	Evaluación de los Riesgos Residuales.	Evaluación de los Riesgos Residuales.	Oficina de Tecnología de la Información.	Recursos Humanos	Informe de los Riesgos Residuales. Instrumento (formato) de	Julio 2022	Dic 2022

			Oficina Asesora de planeación – OAP.		Riesgos de seguridad Digital donde se visualiza los Riesgos Residuales		
	Mejoramiento.	Identificar las oportunidades de mejora, acorde a los resultados obtenidos durante la evaluación de riesgos Residuales	Oficina de Tecnología de la Información. Oficina Asesora de planeación – OAP.	Recursos Humanos	Informes requeridos para las oportunidades de mejora, acorde a los resultados obtenidos durante la evaluación de riesgos Residuales.	Julio 2022	Dic 2022
	Monitoreo y Revisión.	Generación, presentación y reportes de indicadores.	Oficina de Tecnología de la Información	Recursos Humanos	Registro en indicadores. Presentaciones o informes requeridos.	Julio 2022	Dic 2022
Gestión de Incidentes de Seguridad de la Información.	Gestionar los Incidentes de Seguridad de la Información.	Gestionar los Incidentes de Seguridad de la Información reportados.	Oficina de Tecnología de la Información. Responsables de Infraestructura de TI. Responsables de Mesa de Ayuda.	Recursos Humanos	Reporte mensual de Incidentes de Seguridad de Información reportados.	Enero 2022	Dic 2022
	CSIRT.	Socializar los boletines Informativos de Seguridad, Integrar con CSIRT de Gobierno.	Oficina de Tecnología de la Información Oficina Asesora de Comunicaciones.	Recursos Humanos	Boletines emitidos por CSIRT-PONAL	Enero 2022	Dic 2022
Gestión de Control de Cambios.	Ejecución del Procedimiento de Control de Cambios.	Reporte de control de cambios a realizar sobre la Plataforma Tecnológica del ICA, con la documentación requerida.	Oficina de Tecnología de la Información Líderes de servicio TI.	Recursos Humanos	Reporte de Control de Cambios mensuales registrados.	Enero 2022	Dic 2022
Plan de Cultura y Sensibilización de Seguridad y Privacidad de la Información.	Realizar y aprobar el Plan de Cultura y Sensibilización de Seguridad de la Información.	Formular el Plan de Cultura y Sensibilización de Seguridad de la Información.	Oficina de Tecnología de la Información	Recursos Humanos	Documento de Plan de Cultura de Seguridad de la Información de la Entidad.	Marzo 2022	Abril 2022
		Aprobar Plan de Cultura y Sensibilización de Seguridad de la Información.	Comité Institucional de Gestión y Desempeño.	Recursos Humanos		Marzo 2022	Abril 2022
	Ejecutar el Plan de Cultura y Sensibilización de Seguridad de la Información.	Realizar las actividades del Plan de Cultura y Sensibilización de Seguridad de la Información.	Oficina de Tecnología de la Información	Recursos Humanos	Seguimiento del cronograma del Plan de Cultura y sensibilización de Seguridad	Enero 2022	Dic 2022

					de la Información.		
Gobierno Digital.	Gobierno Digital.	Actualizar el documento de autodiagnóstico MSPI de la Entidad.	Oficina de Tecnología de la Información	Recursos Humanos	Instrumento de Diagnostico del MSPI.	Abril 2022	Mayo 2022
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI.	Oficina de Tecnología de la Información	Recursos Humanos	Documentos actualizados	Enero 2022	Dic 2022
	Infraestructuras Criticas Cibernéticas – ICC.	Participa en reuniones de Infraestructuras Criticas Cibernéticas.	Oficina de Tecnología de la Información	Recursos Humanos	Actas de Asistencia o agenda de participación.	Enero 2022	Dic 2022
Auditorías Internas y Externas.	Participación en las auditorías internas y externas.	Participar en las auditorías internas y externas.	Oficina de Tecnología de la Información Responsables de los servicios de la OTI.	Recursos Humanos	Actas de Asistencia o agenda de participación. Respuesta a requerimientos realizados.	Enero 2022	Dic 2022
Indicadores del SGSI.	Indicadores de medición del SGSI.	Formular y actualizar los indicadores del SGSI.	Oficina de Tecnología de la Información	Recursos Humanos	Formato de indicadores del SGSI.	Marzo 2022	Abril 2022
		Aprobar los indicadores del SGSI.	Comité Institucional de Gestión y Desempeño.	Recursos Humanos	Acta aprobación del Comité de gestión	Marzo 2022	Abril 2022
		Registrar los indicadores del SGSI.	Oficina de Tecnología de la Información	Recursos Humanos	Formato de indicadores del SGSI.	Enero 2022	Dic 2022
Actualización de documentación del SGSI.	Actualización de documentación del SGSI.	Actualizar Manuales, Políticas, Planes, Procedimientos, Guías, Instructivos, Formatos, Indicadores del Sistema de Gestión de Seguridad de la Información – SGSI.	Oficina de Tecnología de la Información	Recursos Humanos	Manuales, Políticas, Planes, Procedimientos, Guías, Instructivos, Formatos,	Ene-20	Dic-20

Tabla 1 Plan de Seguridad y Privacidad de la Información

7.1. RECURSOS.

En el marco del Plan de Seguridad y privacidad de la Información del instituto colombiano agropecuario "ICA", se establece los siguientes recursos:

RECURSOS	DEFINICIÓN
Humanos	La Oficina de Tecnologías de la Información "OTI" a través del personal de Seguridad de la Información serán los responsables de: - coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en materia de Seguridad y Privacidad de la Información lo cual contribuye a la mejora continua.

Técnicos	Se basa en los instrumentos definidos como: - Procedimiento para la identificación y clasificación de activos - Instrumento para la identificación de Activos de Información (Matriz de Activos SGSI). - Guía para la Clasificación de Activos de Mintic.
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento.
Financiero	Gestión financiera para la adquisición de logísticos, recursos humanos, técnicos, entre otros.

Tabla 2 Recursos.

8. 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.

9. DOCUMENTOS ASOCIADOS

- Procedimiento de Identificación, Valoración y Clasificación de Activos de Información.
- Guía Administración de Riesgos.
- Manual de Políticas de Seguridad y Privacidad de la Información.
- Manual del Sistema de Gestión de Seguridad de la Información – SGSI.

Versión	Descripción del cambio	Fecha
1	Creación del Plan de Seguridad y privacidad de la Información.	28 Feb 2022

Nombre de quien Elabora:	Nombre de quien Revisa:	Nombre de quien Aprueba:
Danny Peter Gutierrez Beltran	Jonathan Ardila Galvis	Jonathan Ardila Galvis
Firma:	**Firma**	**Firma**
Cargo: Líder de Seguridad de la Información	**Cargo:** Jefe de Oficina de Oficina de Tecnología de Información	**Cargo:** Jefe de Oficina de Oficina de Tecnología de Información