ANEXO 12. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOGOTA D.C., ENERO DE 2026

Unidad de Planificación Rural Agropecuaria (UPRA)
Carrera 10 No. 28-49 Torre A, pisos 11, 12 y 19. Bogotá, Colombia.
+57 310 801 6445
atencionalusuario@upra.gov.co
www.upra.gov.co

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información de la Unidad de Planificación Rural Agropecuaria –UPRA-, establece directrices, actividades y mecanismos necesarios para garantizar la protección integral de los activos de información de la entidad. Este plan se encuentra alineado con i) la Política de Gobierno Digital y la implementación del Modelo de Seguridad y Privacidad de la Información; ii) con la Política de Seguridad Digital en lo referente a la gestión de riesgos de seguridad digital; y iii) lineamientos y buenas prácticas de la Norma ISO NTC/IEC ISO 27001:2022 para la gestión de Seguridad de la Información.

El Plan se ejecuta a través del Sistema de Gestión de Seguridad de la Información (SGSI) de la UPRA, el cual hace parte del Sistema de Gestión de UPRA y responde al enfoque de mejora continua. Su finalidad es fortalecer las capacidades institucionales para identificar, evaluar tratar y mitigar los riesgos que pueden afectar la confidencialidad, integridad y disponibilidad de la información, mediante la implementación de controles técnicos, administrativos y organizacionales.

Con este plan, la UPRA consolida un marco estratégico y operativo para asegurar la protección de su información misional, garantizar la continuidad operativa, promover la cultura de seguridad digital en todos los colaboradores y cumplir con las exigencias normativas nacionales e internacionales aplicables.

Unidad de Planificación Rural Agropecuaria (UPRA)
Carrera 10 No. 28-49 Torre A, pisos 11, 12 y 19. Bogotá, Colombia.
+57 310 801 6445
atencionalusuario@upra.gov.co
www.upra.gov.co

2. DEFINICIONES

•**Activo de Información**: Elemento, recurso o componente —hardware, software, infraestructura, datos o procedimientos— que una entidad utiliza, procesa o controla, y que tiene valor para la consecución de sus objetivos institucionales o para la protección de la información, incluyendo datos personales, operativos o misionales.

•**Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

•**Análisis de Riesgo**: Proceso sistémico para comprender la naturaleza del riesgo y determinar el nivel, considerando la probabilidad de ocurrencia y el impacto de sus consecuencias. (ISO/IEC 27000).

•**Control**: Políticas, procedimiento, práctica estructura organizativa diseñada para gestionar un riesgo reduciendo la probabilidad de que una amenaza explote una vulnerabilidad y/o mitigando su impacto, con el fin de mantener el riesgo dentro de niveles aceptables.

•**Confidencialidad**: Propiedad de la información por la cual se asegura que solo personas, procesos o sistemas autorizados tienen acceso o pueden divulgar dicha información.

•**Disponibilidad**: Propiedad de la información que garantiza que los usuarios autorizados puedan acceder y utilizar los activos de información cuando lo requieran.

•**Infraestructura Crítica Cibernética (ICC)**: Sistemas, activos de información, redes o servicios esenciales para la prestación de funciones o servicios públicos, cuya interrupción o destrucción podría provocar un impacto

Unidad de Planificación Rural Agropecuaria (UPRA)
Carrera 10 No. 28-49 Torre A, pisos 11, 12 y 19. Bogotá, Colombia.
+57 310 801 6445
atencionalusuario@upra.gov.co
www.upra.gov.co

significativo en la seguridad nacional, bienestar social, economía o continuidad de servicios esenciales.

•**Integridad**: Propiedad de la información que garantiza que esta sea exacta, completa y que no ha sido modificada o destruida de forma no autorizada.

•**Mapa de Calor de Riesgos**: Representación gráfica o matricial que permite visualizar los riesgos clasificados según su nivel de probabilidad e impacto, facilitando su priorización para tratamiento.

•**Método de Tratamiento del Riesgo**: Enfoque adoptado por la organización para gestionar un riesgo específico, que puede consistir en aceptar, reducir, transferir o evitar el riesgo.

•**Nivel de Riesgo**: Valor o calificación que se asigna a un riesgo, como resultado de la combinación de la probabilidad de ocurrencia del evento y la magnitud del impacto que este pueda generar.

•**Privacidad de la Información**: Derecho que tienen las personas a que sus datos personales sean tratados de forma adecuada, con respeto por su intimidad y conforme a la normativa aplicable (por ejemplo, Ley 1581 de 2012 y sus reglamentaciones).

•**Riesgo**: Es la posibilidad de que ocurra un evento o situación que, al aprovechar una debilidad en los sistemas o procesos, afecte la confidencialidad, integridad o disponibilidad de la información institucional. (ISO/IEC 27000).

•**Seguridad de la información**: Conservación de la confidencialidad, integridad, y disponibilidad de la información, así como de los sistemas que la procesan, en cualquiera de sus formatos. (ISO/IEC 27000).

•**Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (incluyendo políticas, procesos,

Unidad de Planificación Rural Agropecuaria (UPRA)
Carrera 10 No. 28-49 Torre A, pisos 11, 12 y 19. Bogotá, Colombia.
+57 310 801 6445
atencionalusuario@upra.gov.co
www.upra.gov.co

recursos, estructura organizativa) permiten a una entidad establecer, implementar, mantener y mejorar continuamente su seguridad de la información, conforme a estándares como ISO/IEC 27001.Tratamiento del Riesgo: Conjunto de actividades seleccionadas y aplicadas para modificar el nivel de riesgo, mediante uno o varios métodos de gestión de riesgos.

•**Vulnerabilidad:** Debilidad de un activo, control o conjunto de controles que puede ser explotada por una o más amenazas para generar un incidente o daño. (ISO/IEC 27000).

Unidad de Planificación Rural Agropecuaria (UPRA)
Carrera 10 No. 28-49 Torre A, pisos 11, 12 y 19. Bogotá, Colombia.
+57 310 801 6445
atencionalusuario@upra.gov.co
www.upra.gov.co

3. OBJETIIVOS

3.1 GENERAL

Establecer las acciones a desarrollar durante la vigencia 2026, en el marco de la actualización y fortalecimiento del Sistema de Gestión de Seguridad de la Información – SGSI, asegurando su alineación con la normatividad vigente en materia de seguridad digital, privacidad de la información y gestión de riesgos, así como con estándares internacionales y buenas prácticas reconocidas, para garantizar la protección integral de los activos de información de la Unidad de Planificación Rural Agropecuaria – UPRA.

3.2 ESPECÍFICOS

- Fortalecer el ciclo de mejora continua del SGSI, mediante la actualización periódica de instrumentos, documentos, procesos y procedimientos institucionales de seguridad de la información, asegurando la optimización de la gestión de riesgos y la protección de los activos de información
- Gestionar proactivamente los riesgos de seguridad de la información, mediante la identificación, evaluación, tratamiento y monitoreo constante de amenazas y vulnerabilidades, apoyados en herramientas de aprendizaje continuo y en la aplicación de lineamientos nacionales de seguridad digital.
- Promover la cultura de seguridad de la información en todos los colaboradores de la entidad mediante estrategias permanentes de socialización y sensibilización, apoyados por las áreas de: Uso y Apropiación de la Oficina TIC y del área de Comunicaciones, asegurando que cada usuario comprenda y actúe de acuerdo con los riesgos asociados a su función y responsabilidad dentro de la entidad.

Unidad de Planificación Rural Agropecuaria (UPRA)
Carrera 10 No. 28-49 Torre A, pisos 11, 12 y 19. Bogotá, Colombia.
+57 310 801 6445
atencionalusuario@upra.gov.co
www.upra.gov.co

- Implementar y optimizar controles técnicos, administrativos y organizaciones, asegurando la protección frente a ciber amenazas y la continuidad de los procesos críticos de la entidad, alineados con los lineamientos de la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y los estándares de ciberseguridad del Estado Colombiano.
- Promover la interoperabilidad y el fortalecimiento de la seguridad de los sistemas de información institucionales, garantizando que las iniciativas tecnológicas consideren criterios de confiabilidad, disponibilidad y cumplimiento normativo, en articulación con la Oficina TIC y las directrices nacionales en materia de Gobierno Digital.

Unidad de Planificación Rural Agropecuaria (UPRA)
Carrera 10 No. 28-49 Torre A, pisos 11, 12 y 19. Bogotá, Colombia.
+57 310 801 6445
atencionalusuario@upra.gov.co
www.upra.gov.co

4. MARCO NORMATIVO

Ley Estatutaria 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos.
Ley Estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de2014 y se dictan otras disposiciones
Decreto 1078 de 2015	Modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de seguridad y Privacidad - MSPI de MINTIC.
CONPES 3854 de 2016	Política de Seguridad Digital del Estado Colombiano
Decreto 1499 de 2017	El cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
Ley 1928 de 2018	Por medio de la cual s e aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.
CONPES 3995 de 2020	Política Nacional De Confianza y Seguridad Digital
Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Resolución 746 de 2022	Complementa lineamientos sobre proveedores y servicios de seguridad digital.
Decreto 338 de 2022	Lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones
Decreto 767 de 2022	Define lineamientos de gobernanza de infraestructura de datos.

Resolución 02277 de 2025	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021, adoptando los lineamientos de la norma ISO/IEC 27001:2022 y derogando otras disposiciones.
Estrategia Nacional de Seguridad Digital 2025–2027	Documento estratégico del MinTIC que define ejes de gobernanza, ciberseguridad y actualización normativa.

5. ALCANCE

El Plan de Seguridad y Privacidad de la Información de la Unidad de Planificación Rural Agropecuaria - UPRA, establece el marco de acción para la actualización, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) conforme al ciclo de gestión (Planear, Hacer, Verificar y Actuar) y a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) adoptado por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante la Resolución 02277 de 2025.

Este plan aplica a todas las dependencias, proceso, sistemas, servicios y actores que intervienen en la gestión de información institucional, incluyendo:

Servidores públicos y contratistas de la UPRA.

Proveedores y terceros que administren, procesen o custodien información de la entidad.

Usuarios externos y ciudadanía que interactúan con los sistemas de información institucionales.

El alcance funcional comprende todos los procesos institucionales sujetos al SGSI, tanto misionales como de apoyo, que involucren activos de información en formato digital o físico.

El alcance técnico incluye la infraestructura tecnológica, las plataformas de información, los sistemas y aplicaciones bajo control de la UPRA, así como los servicios en la nube y redes institucionales que soportan el tratamiento de la información.

Este Plan busca garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional, mediante la gestión de riesgos, la implementación de controles técnicos y administrativos, y la adopción de buenas prácticas conforme a la norma ISO/IEC 27001:2022 y las políticas nacionales de seguridad digital.

El Plan no cubre sistemas o infraestructuras que no estén bajo administración, control o gestión contractual de la UPRA, aunque sí promueve la adopción de controles mínimos por parte de terceros con quienes se mantenga intercambio de información.

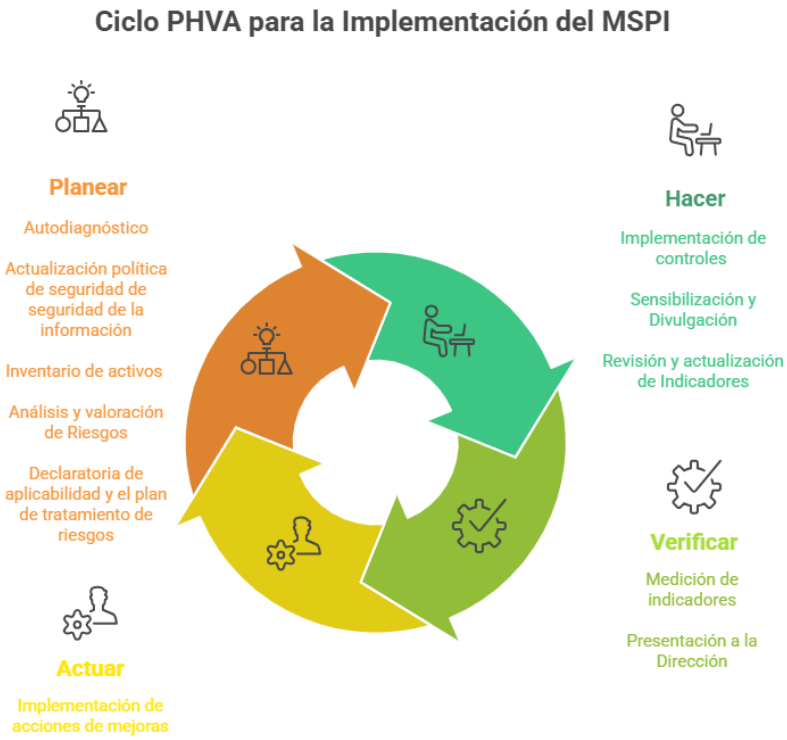
En conjunto, el alcance definido permite asegurar que la seguridad de la información sea gestionada de forma integral, transversal y continua dentro del Sistema de Gestión de la Entidad.

6. METODOLOGÍA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI) de la Unidad de Planificación Rural Agropecuaria - UPRA, se implementa y actualiza a través del ciclo de mejora: Planear, Hacer, Verificar, Actuar (PHVA), garantizando la efectividad y su alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI), adoptado mediante la Resolución 02277 de 2025 del MinTIC, y con los principios de la norma ISO/IEC 27001:2022.

Este enfoque permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI de manera sistemática y sostenible.

A continuación, se describen las fases que conforman la metodología:



En las siguientes imágenes se detallan las actividades a desarrollar durante cada una de las fases del ciclo de mejora continua:

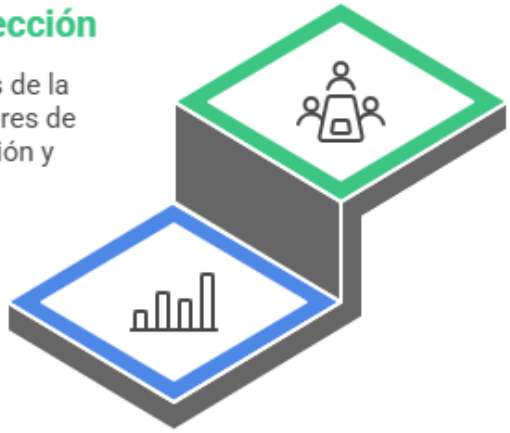
Verificar

2 Presentar a la Dirección

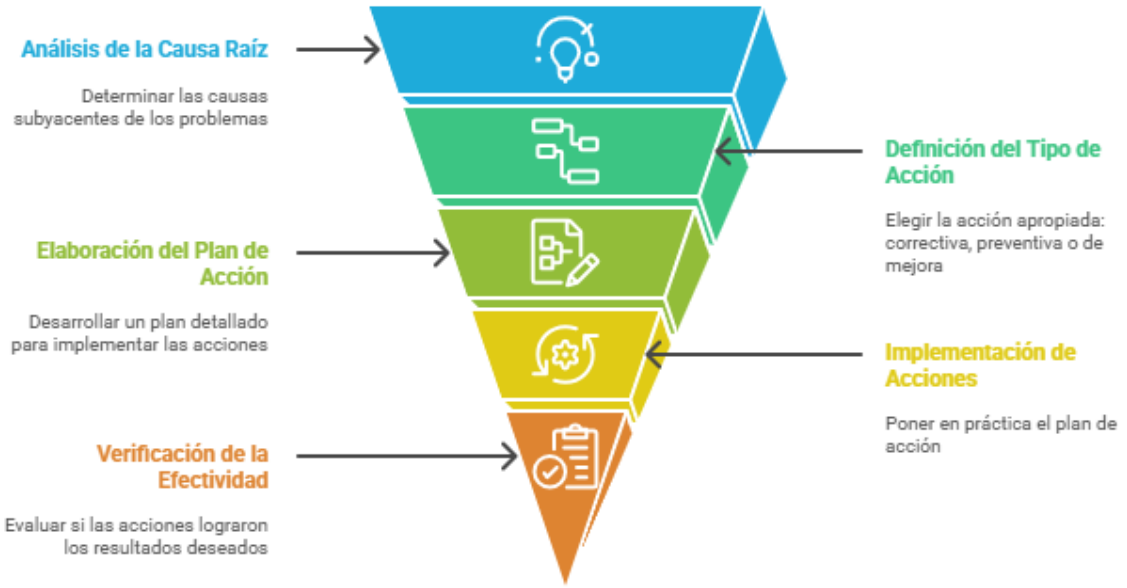
Comunicar los hallazgos de la evaluación a los tomadores de decisiones para su revisión y acción.

1 Medir Indicadores

Recopilar y analizar datos para evaluar el desempeño de los controles de seguridad.



Actuar



6.1 DESARROLLO DE LA METODOLOGIA

FASE	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
Planear	Aplicación y revisión del autodiagnóstico del MSPI	Evaluar semestralmente el estado del SGSI frente a los lineamientos del MSPI, utilizando los instrumentos oficiales del MinTIC.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información.

FASE	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
PLANEAR	Actualización de la política de seguridad de la información institucional	Revisar y actualizar la política de seguridad de la información cuando se presenten cambios en el contexto organizacional, normativo o tecnológico; la aparición de nuevas amenazas o vulnerabilidades; o la emisión de lineamientos y estándares actualizados por el MinTIC, el DAFP o los organismos internacionales (ISO, NIST). Esta revisión garantizará su alineación con el Modelo de Seguridad y Privacidad de la Información (MSPI) y con los objetivos estratégicos de la entidad.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información.
	Actualizar el inventario de activos de información	Revisar y mantener actualizado el inventario de activos de información, clasificando según tipo, criticidad y responsable.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información.
	Análisis y valoración de Riesgos	Identificar amenazas y vulnerabilidades sobre los activos de información, determinar niveles de riesgo e impactos potenciales.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información.

	Declaratoria de aplicabilidad y el plan de tratamiento de riesgos	Revisar controles aplicables según la ISO/IEC 27001:2022 y definir acciones de mitigación.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información.

HACER	Implementación de controles	Ejecutar los controles técnicos, administrativos y organizacionales definidos en el plan de tratamiento.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información, grupo de servicios tecnológicos, de sistemas de información y de gestión y análisis de información, servicios administrativos y almacén.
	Sensibilización y Divulgación	Ejecutar actividades de sensibilización y comunicación orientadas a fortalecer la cultura de seguridad de la información en todos los colaboradores de la entidad.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información y grupo de uso y apropiación
	Revisión y actualización de Indicadores	Revisar, los indicadores del SGSI y ajustarlos de acuerdo con los resultados obtenidos.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información

FASE	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE
VERIFICAR	Medición de indicadores	Realizar la medición y análisis de los indicadores asociados al Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de evaluar su desempeño, eficacia y cumplimiento de los objetivos establecidos.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información
	Presentación a la Dirección	Presentar ante la Dirección los resultados de la medición de indicadores y las actividades desarrolladas en la actualización del SGSI, con el propósito de	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información

		facilitar la revisión del sistema, la toma de decisiones y la definición de acciones de mejora.	
ACTUAR	Implementación de acciones de mejoras	Definir e implementar acciones correctivas, preventivas y de mejora derivadas de las revisiones, auditorías, eventos o incidentes.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información, grupo de servicios tecnológicos, de sistemas de información y de gestión y análisis de información, servicios administrativos y almacén.

7. RECURSOS

7.1 HUMANOS

Las actividades definidas en el Plan de Seguridad y Privacidad de la Información serán ejecutadas por los grupos y equipos establecidos por la entidad, conformados por personal con competencias y conocimientos en seguridad de la información, gestión tecnológica y procesos institucionales.

7.2 ECONÓMICOS

El desarrollo del Plan de Seguridad y Privacidad de la Información de la Unidad de Planificación Rural Agropecuaria (UPRA), se encuentran respaldas por los proyectos de inversión gestionados por la Oficina de Tecnologías de la Información y las Comunicaciones TIC de la Entidad, que se listan a continuación:

- Fortalecimiento de la gestión de información y sus tecnologías para la planificación y orientación de la política de gestión del territorio para usos agropecuarios en el ámbito nacional, con código BPIN: 2019011000039, objetivo específico Fortalecer la capacidad tecnológica de los sistemas de información.
    - Actividad 4.1.2. Implementación de soluciones tecnológicas innovadoras de manejo de información, con atributos de calidad e interoperabilidad (escalabilidad, seguridad, confiabilidad y articulación de sistemas información) y Actividad 4.1.3. Realizar la actualización y mantenimiento de los sistemas de información que soportan la planificación rural.
- Fortalecimiento de la capacidad en la gestión de información estratégica sectorial para la orientación de la política agropecuaria nacional, con código BPIN: 2022011000020, objetivo específico Mejorar la información de productividad y precios agropecuarios.

- Actividad 2.1.2 Implementar soluciones tecnológicas innovadoras de manejo de información de productividad y precios agropecuarios de calidad e interoperabilidad.

Estos proyectos aseguran la disponibilidad de recursos económicos necesarios para la ejecución, mantenimiento y mejora continua del SGSI y las acciones previstas en este plan.

7.3 FÍSICOS

Comprenden los recursos de infraestructura tecnológica y de soporte, requeridos para la implementación y operación del Plan de Seguridad y Privacidad de la Información, tales como:

- Centros de datos, servidores y sistemas de respaldo.
- Equipos de red, comunicaciones y seguridad perimetral.
- Puestos de trabajo, equipos de cómputo y estaciones de usuario.
- Sistemas de climatización, energía y control de acceso físico en las instalaciones.

Estos recursos se encuentran desplegados y en funcionamiento en la UPRA, garantizando la disponibilidad, integridad y confidencialidad de los activos de información institucionales.