

## **UNIDAD DE PLANIFICACIÓN RURAL AGROPECUARIA (UPRA)**

### **PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.**

**BOGOTA D.C., ENERO DE 2023**



## 1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información de la Unidad de Planificación Rural Agropecuaria –UPRA-, se encuentra alineado con i) la Política de Gobierno Digital, específicamente con 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) con la Norma ISO NTC/IEC ISO 27001:2013 de Seguridad de la Información.

Este Plan se implementa a través del Sistema de Gestión de Seguridad de la Información el cual hace parte del Sistema de Gestión Integrado y tiene como finalidad el fortalecimiento de las capacidades institucionales para gestionar, tratar y mitigar los riesgos a los cuales se encuentran expuestos sus activos de información, a través de la aplicación de mecanismos y controles técnicos y administrativos que propenden por la confidencialidad, integridad y disponibilidad de estos



## 2. DEFINICIONES<sup>1</sup>

- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- 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 para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- 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.
- 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).
- Vulnerabilidad Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

<sup>1</sup> Tomado de la sección "Glosario" del documento Modelo de Seguridad y Privacidad de la Información



### 3. OBJETIVOS

#### 3.1. GENERAL

Establecer las acciones a desarrollar durante la vigencia 2023, en el marco de la actualización del Sistema de Gestión de Seguridad de la Información – SGSI institucional, que se encuentran alineadas con la normatividad vigente aplicable en materia de seguridad y privacidad de la información.

#### 3.2. ESPECÍFICOS

- Ejecutar el ciclo de mejora continua del SGSI, mediante la actualización de los instrumentos, procesos y procedimientos institucionales de seguridad de la información, en procura del fortalecimiento y optimización de la gestión de seguridad y privacidad de la información en la entidad.
- Gestionar de manera efectiva los riesgos de seguridad de la información de la Unidad de Planificación Rural Agropecuaria – UPRA.
- Propender por la adopción en todos los colaboradores de la entidad, de una cultura de seguridad de la información.
- Implementar y optimizar la implementación de controles técnicos y organizaciones, que permitan fortalecer la seguridad digital y ciberseguridad en la UPRA.

#### 4. ALCANCE

El Plan de Seguridad y Privacidad de la Información de la Unidad de Planificación Rural Agropecuaria - UPRA, comprende la actualización del Sistema de Gestión de Seguridad de la Información en sus fases del modelo de mejora continua (Planear, Hacer, Verificar y Actuar) aplicable a los procesos institucionales, y a todos los usuarios internos, externos, proveedores y a la ciudadanía en general, mediante la implementación de una estrategia integral de seguridad de la información que parta desde las políticas, prácticas y aborde toda la cadena de valor, en torno a los objetivos estratégicos de la Entidad, con el fin de diagnosticar, planear e implementar de manera coordinada acciones que sean pertinentes para que la entidad cuente con un escenario donde se apliquen buenas prácticas en materia de seguridad de la información, que conlleven a la seguridad de los sistemas, los procesos, las personas que los ejecutan y los datos, bajo los únicos propósitos de reducir las vulnerabilidades a las que se encuentran expuestos los activos de información institucionales.

#### 5. MARCO NORMATIVO

| Marco Normativo              | Descripción   |
|------------------------------|---|
| 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 de 2014 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 se aprueba el “Convenio sobre la   |

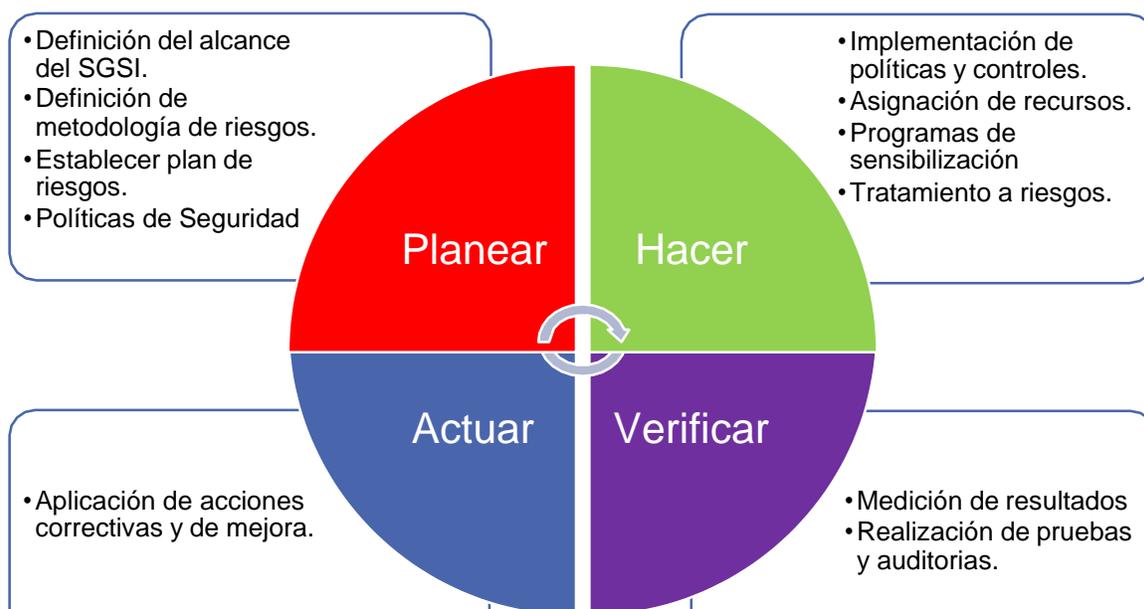
|                         |   |
|-------------------------|---|
|                         | Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest.   |
| CONPES 3995 de 2020     | Política Nacional De Confianza y Seguridad Digital  |
| Resolución 1519 de 2020 | Por la cual se definen los 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.  |
| 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   |

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

El Sistema de Gestión de Seguridad de la Información de la UPRA, se implementa y actualiza a través del ciclo PHVA, de esta manera se garantiza que sea efectivo y esté acorde con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).

Se cuenta entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.

A continuación, se listan los elementos que hacen parte de cada una de las fases del ciclo PHVA del SGSI:



En la siguiente imagen se detallan las actividades a desarrollar durante cada una de las fases del ciclo de mejora continua:

| PLANEAR   | HACER                                      | VERIFICAR                                   | ACTUAR  |
|---|--|---|---|
| Definir alcance SGSI                                      | Ejecutar el plan de tratamiento de riesgos | Ejecutar el plan operacional                | Implementar las mejoras identificadas   |
| Definir la política de Seguridad de la Información        | Documentar controles                       | Verificar el inventario de activos          | Tomar medidas preventivas y correctivas   |
| Levantamiento de inventario de <b>activos información</b> | Implementar políticas                      | Revisar revisiones de la eficacia           | Aplicar lecciones aprendidas  |
| Realizar análisis de riesgos                              | Implementar entrenamiento                  | Realizar revisiones del riesgo residual     | Comunicar los resultados  |
| Seleccionar controles a implementar                       | Gestión de la operación y recursos         | Realizar revisión interna del SGSI          | Garantizar el objetivo del SGSI   |
| Definir <b>plan de tratamiento de riesgos</b>             | Implementar las respuestas a incidentes    | Realizar revisión por la dirección del SGSI | Revisar la política de seguridad, alcance del SGSI, Activos de la información y riesgo residual |
| Preparar la declaración de aplicabilidad                  |  | Registrar el impacto del SGSI               |   |

## 7. DESARROLLO DE LA METODOLOGÍA.

| FASE    | ACTIVIDAD   | DESCRIPCIÓN  | RESPONSABLE   |
|---------|---|--|---|
| Planear | Autodiagnóstico de implementación del MSPI                                | A partir de los instrumentos dispuestos por el Ministerio de Tecnologías de la Información y las Comunicaciones, determinar el estado actual de la UPRA frente a la implementación del Modelo de Seguridad y Privacidad de la Información. | Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información. |
|         | Actualización de la política de seguridad de la información institucional | Actualizar la política de seguridad de la información institucional, teniendo en cuenta la misión institucional, la normatividad vigentes y la dinámica del negocio.   | Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información. |

|           |   |   |  |
|-----------|---|---|--|
|           | Actualizar el inventario de activos de información                              | Actualizar el inventario de activos de información alineado con las Tablas de Retención Documental y los instrumentos de gestión de información pública | Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información – Líderes de procesos – Grupo de gestión documental   |
|           | Actualizar el análisis de riesgos   | A partir del inventario de activos de información, actualizar el análisis de riesgos identificando vulnerabilidades y amenazas                          | Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información – Líderes de procesos   |
|           | Actualizar la declaratoria de aplicabilidad y el plan de tratamiento de riesgos | Actualizar la declaratoria de aplicabilidad identificando los controles aplicables y no aplicables  | Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información.  |
| Hacer     | Implementar el plan de tratamiento de riesgos                                   | Implementar los controles técnicos y organizacionales contenidos en la declaratoria de aplicabilidad  | 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. |
|           | Sensibilizar y divulgar   | Ejecutar actividades de sensibilización y comunicación de seguridad de la información   | Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información y grupo de uso y apropiación  |
|           | Revisión de indicadores   | Revisar y actualizar en caso de ser necesario, los indicadores asociados al Sistema de Gestión de Seguridad de la Información                           | Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información   |
| Verificar | Presentación a la dirección   | Presentar ante la Dirección, las actividades realizadas en el marco de la actualización del SGSI  | Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información   |

|        |                           |  |  |
|--------|---------------------------|--|--|
|        |                           |  | información  |
|        | Medición de indicadores   | Realizar la medición de indicadores asociados al Sistema de Gestión de Seguridad de la Información                       | Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información   |
| Actuar | Implementación de mejoras | A partir de los resultados de la medición de indicadores, implementar las acciones u oportunidades de mejora requeridas. | 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. |

## 8. RECURSOS.

### 8.1. HUMANOS.

Las actividades definidas en el Plan de Seguridad y Privacidad de la Información serán ejecutadas por los integrantes de cada uno de los grupos responsables definidos, entre los que se encuentran perfiles idóneos y con conocimientos relacionados con los diferentes procesos institucionales y de seguridad de la información.

### 8.2. ECONÓMICOS.

El desarrollo del Plan de Seguridad y Privacidad de la Información de la Unidad de Planificación Rural Agropecuaria, se encuentran respaldados 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, actividades 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 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.

### 8.3. FÍSICOS.

Son todos aquellos recursos de infraestructura tecnológica desplegados en la UPRA y en funcionamiento, requeridos para la ejecución de Plan de Seguridad y Privacidad de la Información.