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

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

**BOGOTA D.C., DICIEMBRE DE 2021**

# 1. INTRODUCCIÓN

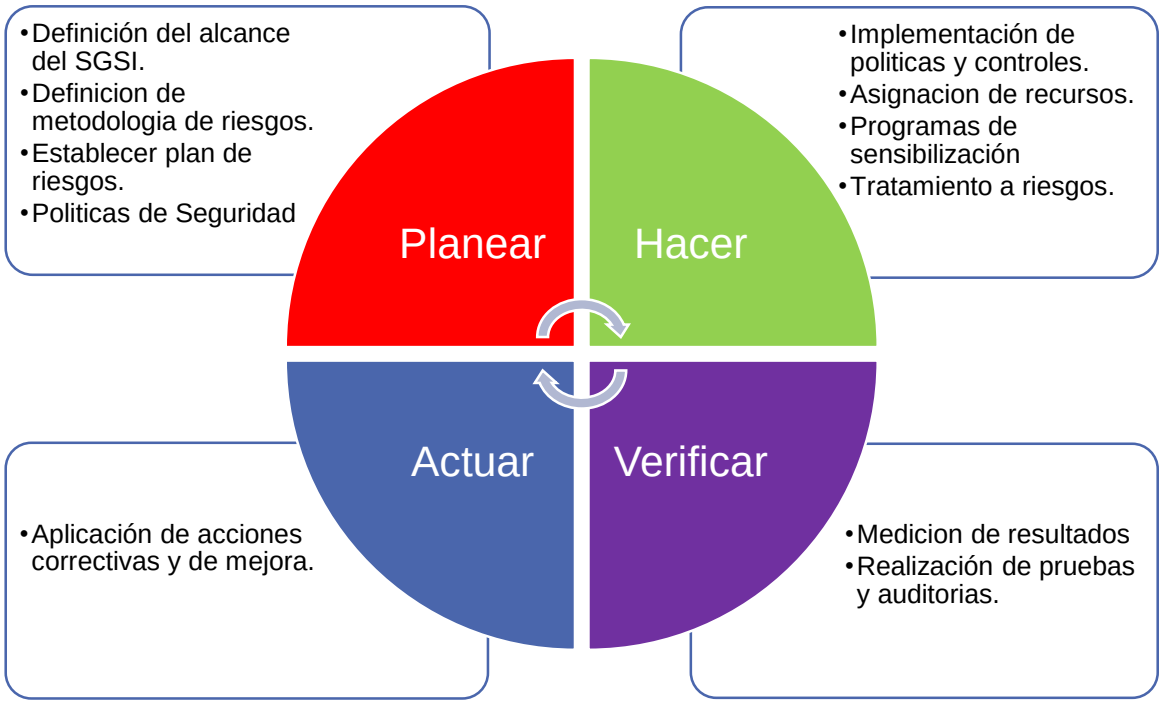
El Plan de Seguridad y Privacidad de la Información de la UPRA, está representado a través del sistema de gestión de seguridad de la información (SGSI), que a su vez se encuentra alineado con el modelo de seguridad y privacidad de la información (MSPI), el marco de referencia de arquitectura TI y soporta transversalmente la Política de Gobierno Digital.

El Sistema de Gestión de Seguridad de la Información de la UPRA, permite fortalecer las capacidades de la entidad para gestionar, tratar y mitigar los riesgos a los cuales se encuentran expuestos sus activos de información. Para tal fin se implementan controles técnicos y administrativos, que junto con el uso de las mejores prácticas, aseguran la confidencialidad, integridad y disponibilidad de los activos de información de la UPRA, garantizando su buen uso y la privacidad de los mismos.

## 2. ESTADO DEL ARTE.

El Sistema de Gestión de Seguridad de la Información de la UPRA, se fortalece a través del ciclo PHVA, de esta manera se garantiza que el sistema implementado en la entidad sea efectivo y este acorde a 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:

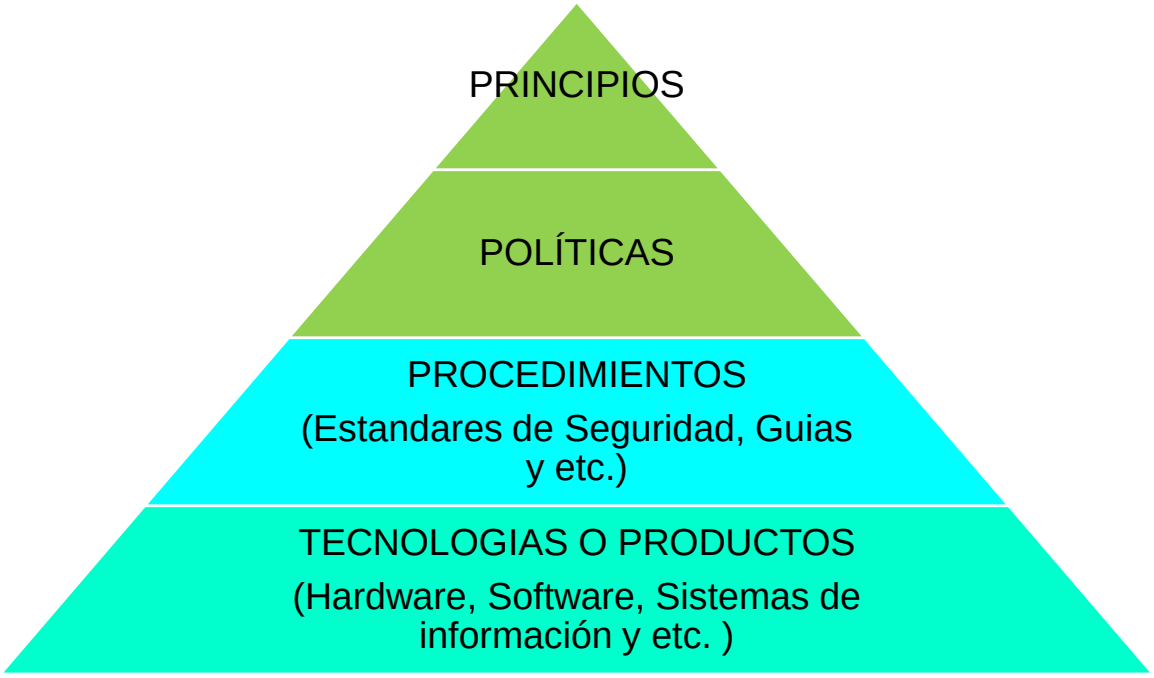



Con el fin de afianzar un marco de gestión de riesgos y proteger los activos de información de la Entidad, el Sistema de Gestión de Seguridad de la Información de la UPRA se encuentra alineado con la política nacional de seguridad digital “CONPES 3854 del 11 de abril de 2016” y con la familia de normas ISO27000:2013, que certifican y proporcionan el

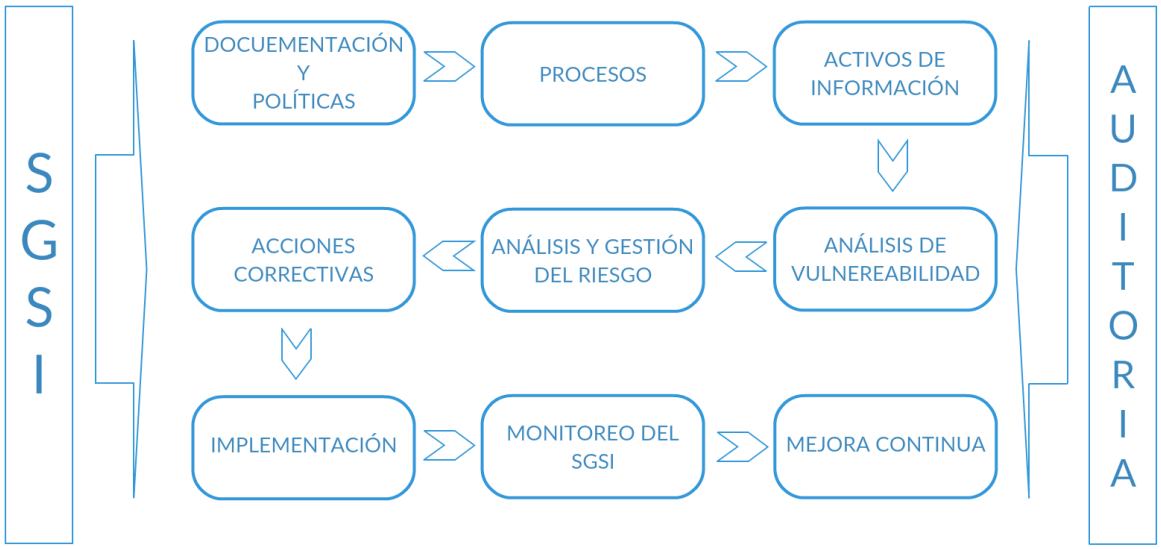
aseguramiento de la confidencialidad, la integridad y la disponibilidad de los activos de información, mediante la implementación de una estrategia integral de seguridad de la información que parta desde las políticas, procedimientos, instrumentos, formatos, guías y mejores prácticas, en torno a los objetivos estratégicos de la Entidad.

En el siguiente grafico se describen los niveles en que se encuentra la seguridad de la información al interior de la entidad y la tabla de los dominios aplicados al sistema de seguridad de la información:

| Control | Descripción |
|---|---|
| A.5 | Política de Seguridad |
| A.6 | Organización de la Información de Seguridad |
| A.7 | Administración de recursos |
| A.8 | Seguridad de los recursos humanos |
| A.9 | Seguridad física y del entorno |
| A.10 | Administración de las comunicaciones y operaciones |
| A.11 | Control de accesos |
| A.12 | Adquisición de sistemas de información, desarrollo y mantenimiento |
| A.13 | Administración de los incidentes de seguridad |
| A.14 | Administración de la continuidad de negocio |
| A.15 | Cumplimiento (legales, de estándares, técnicas y auditorías) |



En el siguiente grafico se describe el proceso que se sigue para la operación del Sistema de Gestión de Seguridad de la Información de la UPRA:




## 3. METODOLOGÍA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN.

### 3.1. Integración del SGSI con el SGI de la UPRA.

Dado que el Sistema de Gestión de Seguridad de la Información se enmarca dentro de un Modelo de Mejora Continua, es uno de los elementos que se desarrollan en el Sistema de Gestión Integrado, por tal razón hace parte del manual del SGI de la UPRA.

### 3.2. Compromiso de la Dirección.

El Plan de Seguridad de la Información de la UPRA cuenta con el respaldo de la Dirección General, el cual se ve reflejado en la definición y actualización del alcance del SGSI, la política general y los objetivos de seguridad de la información.

### 3.3. Alcance del SGSI.

El alcance del SGSI de la UPRA se define en función de los procesos institucionales, su aplicación es responsabilidad de todos los funcionarios directos e indirectos, así como de aquellos terceros e involucrados internos y externos, que tengan acceso a los diferentes activos de información de la entidad.

### 3.4. Política General de Seguridad de la Información.

La política de seguridad de la información de la UPRA enmarca lo qué se va a proteger en términos generales, y se encuentra alineada con la política de calidad institucional, que a su vez debe apoyar el cumplimiento de la misión. Está enfocada a la protección de los activos de información en términos de confidencialidad, integridad y disponibilidad, y contempla la aplicación de diferentes contramedidas que permitan la gestión de los riesgos de seguridad de la información. Así mismo está alineada con los niveles de clasificación de los activos de información de la UPRA y no va en contravía con las leyes y normatividad aplicable al sector.

### 3.5. Objetivo General de Seguridad de la Información.

El objetivo general de seguridad de la información de la UPRA busca establecer una política de seguridad de la información, que contiene el compromiso de la dirección en la implementación y operación del SGSI, además de la disposición de recursos financieros, tecnológicos y humanos necesarios para tal fin.

### 3.6. Gestión de Riesgos.

La gestión de riesgos de seguridad de la información en la UPRA se realiza a través, de la identificación, análisis, valoración y gestión de los activos de información, con el propósito de identificar las amenazas y vulnerabilidades a las que la entidad puede estar expuesta, a su vez fortalecer los controles que la organización tiene en su sistema de gestión de seguridad de la información (SGSI).

## 4. ARQUITECTURA DE SEGURIDAD DE LA INFORMACIÓN.

La implementación de una Arquitectura de Seguridad de Información en la UPRA, es un reto para la entidad, ya que en esta metodología se involucran todos los procesos de la organización, alrededor de un sistema de seguridad integral, en la siguiente grafica se visualiza como serían los procesos de esta arquitectura:


### 4.1. Organización o Negocio.

El objetivo principal de este elemento de la arquitectura de seguridad de la información es el de alinear la seguridad de la información con los elementos de estrategia del negocio o la organización, como “misión, visión, metas y objetivos” que tiene la compañía, esto definirá unas metas claras para la arquitectura de seguridad de la información.

### 4.2. Marco Normativo, Políticas y estándares.

Este elemento de la arquitectura de seguridad de la información se enfoca en la definición de las directrices regulatorias organizacionales y de seguridad de la información, razón por la cual se involucra desde la normativa corporativa hasta lo normativa de seguridad de la información y las normativas a nivel gubernamental que apliquen a la seguridad de la información.

La normativa organizacional es, por ejemplo: código de ética, código de buen gobierno, reglamento interno de trabajo, normativa antifraude, acuerdos entre las partes.

La normativa en seguridad de la información está enmarcada por ejemplo en: políticas, normas y procedimientos.

La normativa desde lo gubernamental está enmarcada por ejemplo en: leyes, decretos, artículos, estándares y lineamientos.

### 4.3. Sistema de Gestión de Seguridad de la Información.

El sistema de gestión de la seguridad de la información como elemento fundamental de la arquitectura, está basado en un modelo PHVA, el cual permite gestionar los riesgos a través de un ciclo que es análisis, monitorización, capacitación, mantenimiento y actualización.

### 4.4. Infraestructura TI.

En el marco de infraestructura TI la seguridad de información se basa en el modelo de defensa en profundidad, el cual establece que se deben garantizar la seguridad de los siguientes niveles: Datos, Aplicación, Equipos de Cómputo, Red y Perímetro.

### 4.5. Acuerdos de Seguridad de la Información

Este elemento establece las reglas con las cuales la seguridad de la información y la organización, van a alinear sus esfuerzos operacionales, tácticos y estratégicos del negocio. Adicionalmente establece los niveles de responsabilidades de la organización frente a la seguridad de la información.

## 5. PRUEBAS DE SEGURIDAD.

Como parte del sistema de gestión de seguridad de la información de la UPRA, se deben proyectar la ejecución de un plan de pruebas de hacking ético o pruebas de penetración y análisis de vulnerabilidades a los sistemas de información de la entidad, adicionalmente una auditoria a los permisos y privilegios que tienen los usuarios de la entidad.

### 5.1. Pruebas de intrusión a la infraestructura IT.

Realizar análisis de vulnerabilidades a los equipos activos de la UPRA, es la mejor opción para evidenciar debilidades y vulnerabilidades de una manera segura, consiste en realizar una evaluación activa de las medidas de seguridad de los equipos de red de la entidad.

A través de la prueba de penetración es posible detectar el nivel de Seguridad Interna y Externa de los equipos activos de la entidad, determinando el grado de acceso que tendría un atacante con intenciones maliciosas.

### 5.2. Pruebas de seguridad a los sistemas de información (OWASP).

El propósito principal de realizar pruebas de seguridad a los sistemas de información de la UPRA es encontrar errores y defectos que puedan existir en el uso de los sistemas a fin de corregirlos.

Asimismo, verificar que los validadores de datos funcionen y limiten el ingreso de información, para que no se puedan ingresar datos que no estén permitidos (sólo números en campos numéricos, por ejemplo). Se quiere comprobar además que el sistema cumple con los requerimientos establecidos por el usuario, tiene un rendimiento adecuado en el ambiente donde se encuentra instalado.

Otro aspecto importante para evaluar son las características de seguridad relacionadas con el ingreso no autorizado de usuarios, de manera que no puedan realizar modificaciones donde no sean permitidas.

### 5.3. Auditoría de privilegios y permisos a usuarios.

Básicamente este tipo de auditorías, están orientadas a realizar una muestra o verificación de los privilegios que tienen los usuarios de acceso a la información y que tipo de acciones pueden realizar en los activos de información.

## 6. MONITOREO DE LA SEGURIDAD.

A pesar de las medidas de seguridad que pueda tomar a nivel interno la UPRA, los ataques hacia los activos de información de las entidades son cada vez más complejos y sofisticados, por lo que la ciberseguridad se ha convertido en una prioridad y un reto para las organizaciones.

En atención a esto la UPRA y con el fin de proteger sus activos de información a su vez la infraestructura TI, implementa controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la información.

En este contexto se implementan herramientas de monitoreo, que se encargan de realizar un seguimiento y analizar la actividad en redes, servidores, equipos activos, bases de datos, aplicaciones, sitios web, entre otros, buscando actividades anómalas que puedan ser detectadas como un incidente o brecha de seguridad.

Los objetivos de realizar este monitoreo son los siguientes:

- Incrementar la capacidad de vigilancia y detección de amenazas en las actividades diarias de los sistemas de información y comunicaciones de la entidad.
- Analizar los ataques o posibles amenazas.
- Recuperar información perdida o dañada que la entidad haya podido tener por consecuencia de un ataque.
- Mejorar la capacidad de respuesta ante cualquier ataque o incidente de seguridad.