ANEXO 11. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOGOTA D.C., ENERO 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

INTRODUCCIÓN

El plan de tratamiento de riesgos de seguridad de la información de la Unidad de Planificación Rural Agropecuaria – UPRA, se encuentra alineado con el Plan de Seguridad y Privacidad de la Información, con la Guía Política De Administración De Riesgos y los lineamientos del Sistema de Gestión Institucional.

Su propósito es definir y priorizar las acciones técnicas, organizacionales y administrativas necesarias para mitigar los riesgos que puedan afectar los activos de información institucionales, con el fin de preservar su confidencialidad, integridad y disponibilidad, así como garantizar la protección de los datos personales tratados por la entidad.

Este plan contribuye al fortalecimiento de los procesos y procedimientos relacionados con la gestión de riesgos de seguridad y privacidad de la información, y se constituye en una herramienta clave para la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), promoviendo la implementación de controles efectivos y la articulación entre las áreas técnicas y misionales de la UPRA.

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

DEFINICIONES

•Activo de Información: Elemento, recurso o componente, ya sea 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, de operación o misionales.

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

•Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo, determinar su nivel y tomar decisiones sobre su tratamiento, en consonancia con los objetivos de seguridad de la información. (ISO/IEC 27000).

•Confidencialidad: Propiedad de la información por la cual se garantiza que solo personas, procesos o sistemas autorizados pueden acceder o divulgar la información. (ISO/IEC 27000 / MSPI MinTIC).

•Control: Políticas, procedimiento, práctica o estructura organizativas concebidas para gestionar un riesgo, reduciendo la probabilidad de que una amenaza explote una vulnerabilidad y/o mitigando su impacto.

•Disponibilidad: Propiedad de la información que asegura que los usuarios autorizados puedan acceder a los activos de información cuando lo requieran. (ISO/IEC 27000 / MSPI MinTIC).

•Infraestructura Crítica Cibernética (ICC): Conjunto de sistemas, activos de información, redes o servicios esenciales para la prestación de funciones o servicios públicos, cuyo daño, interrupción o destrucción podría tener 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, económica o social. (Decreto 338 de 2022).

•Integridad: Propiedad de la información que asegura que la misma sea exacta, completa y no haya sido modificada o destruida de manera no autorizada. (ISO/IEC 27000 / MSPI MinTIC).

•Incidente de Seguridad de la Información: Suceso o serie de sucesos no planificados que pueden comprometer la confidencialidad, integridad o disponibilidad de los activos de información, o violar las políticas de seguridad institucionales. (ISO/IEC 27035 / MSPI MinTIC).

•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 el tratamiento. (Guía DAFP).

•Método de Tratamiento del Riesgo: Enfoque adoptado por la organización para gestionar un riesgo particular, que puede consistir en aceptarlo, reducirlo, transferirlo o evitarlo. (ISO 31000 / MSPI MinTIC).

•Nivel de Riesgo: Valor o calificación asignada a un riesgo, resultado de combinar la probabilidad de ocurrencia del evento con la magnitud del impacto que este puede generar. (ISO 31000 / Guía DAFP).

•Privacidad de la Información: Derecho que tienen las personas a que sus datos personales y la información que las identifica sean tratados de manera adecuada, respetando su intimidad y conforme a la normativa aplicable. (Ley 1581 de 2012 y Decreto 1377 de 2013).

•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

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

o disponibilidad de la información institucional. Definición adaptada de la norma ISO/IEC 27000. (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 todos los soportes. (ISO/IEC 27000).

•Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos Interrelacionados o interactuantes (incluyendo políticas, procesos, recursos, estructura organizativa) que permite 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 identificado, mediante uno o varios métodos de gestión: aceptar, reducir, transferir o evitar el riesgo. (ISO 31000 / MSPI MinTIC).

•Vulnerabilidad: Debilidad de un activo o 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. OBJETIVOS

3.1 GENERAL

Establecer las acciones necesarias para la implementación y seguimiento de controles técnicos, administrativos y organizacionales durante la vigencia 2026, orientadas a prevenir, mitigar y gestionar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información institucionales, en concordancia con el Plan de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información (SGSI) de la UPRA.

3.2 ESPECÍFICOS

•Implementar controles y medidas de carácter técnico que fortalezcan la protección de los activos de información y la infraestructura tecnológica.

•Desarrollar e implementar acciones de tipo organizacional que promuevan la gestión efectiva de los riesgos de seguridad y privacidad de la información.

•Fomentar la articulación con las demás áreas de la entidad para garantizar un enfoque integral y transversal en la gestión de riesgos.

•Promover la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), de acuerdo con los lineamientos del MinTIC, el DAFP y las normas ISO 27001 e ISO 31000.

4. ALCANCE

El Plan de Tratamiento de Riesgos comprende el desarrollo y seguimiento de actividades orientadas a la gestión y mitigación de los riesgos identificados en los activos de información institucionales, de acuerdo con la declaratoria de aplicabilidad del Sistema de Gestión de Seguridad de la Información (SGSI).

Este plan es de cumplimiento obligatorio para todos los funcionarios, contratistas y terceros que presten sus servicios, o mantengan relación con la Entidad. Su aplicación abarca todos los procesos institucionales, en especial aquellos que impactan directamente la consecución de los objetivos misionales y estratégicos.

Durante la vigencia 2026, las acciones definidas deberán contribuir al fortalecimiento de la cultura de seguridad y privacidad de la información, y al cumplimiento de los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, el DAFP y las normas ISO 27001 e ISO 31000.

5. NORMAS DE CALIDAD

•Modelo de Seguridad y Privacidad de la Información de MINTIC: Instrumento institucional que tiene como objetivo preservar la confidencialidad, integridad, disponibilidad y privacidad de los activos de información, garantizando su buen uso y el cumplimiento de la normativa aplicable.

•NORMA ISO 27001: 2022: Estándar internación que ofrece lineamientos y buenas prácticas para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

•ISO 31000:2018: Norma internacional que proporciona principios y directrices para la gestión del riesgo en cualquier tipo de organización, incluyendo la identificación, evaluación y tratamiento de riesgos.

•Guía para la administración del riesgo y el diseño de controles en entidades públicas Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP

6. 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 1341 de 2009	Ley de Tecnologías de la Información y las Comunicaciones – TIC.
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 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
Lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC	Preservar confidencialidad, integridad y disponibilidad de los activos de información y garantizar la privacidad de los datos.

Guía DAFP sobre riesgos de gestión, corrupción y seguridad digital – versión 4:	Para administración del riesgo y diseño de controles en entidades públicas.
ISO/IEC 27001:2022	Estándar internacional que define requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).
ISO 31000:2018	Directrices para la gestión del riesgo a nivel organizacional.

7. METODOLOGÍA DEL PLAN DE TRATAMIENTO DE RIESGOS

Identificación y valoración de Activos de Información:

El proceso comienza con la identificación de los responsables de los activos de información, quienes deberán realizar la identificación y categorización de estos. La identificación y valoración se realiza conforme al Modelo de Gestión de Riesgos de Seguridad Digital del Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas:

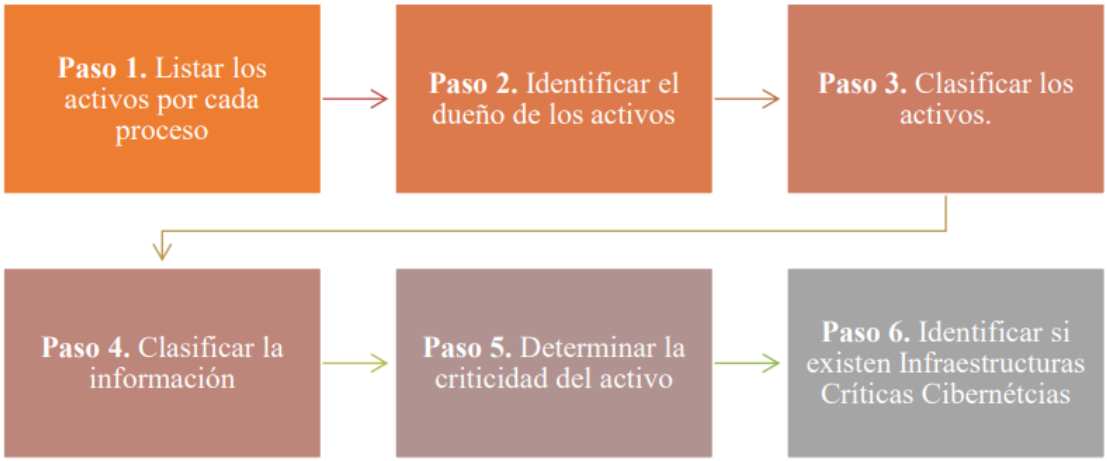

Imagen 2. Pasos para la identificación y valoración de activos.
Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

Paso 1. Listar los activos por cada proceso:

En cada proceso, se deberán listar los activos, indicando algún consecutivo, nombre y Descripción breve de cada uno.

Paso 2. Identificar el dueño de los activos:

Cada activo debe tener un dueño designado, Si un activo no posee un dueño, no habrá responsable de su protección, lo que aumenta su riesgo.

Paso 3. Clasificar los activos:

Cada activo debe asignarse a un grupo según su naturaleza, por ejemplo: Información, Software, Hardware, Componentes de Red, entre otros.

Paso 4. Clasificar la información:

La clasificación de la información se realizará conforme a la Ley 1712 de 2014, Ley 1581 de 2012, el Modelo de Seguridad y Privacidad de MinTic, guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2022 y demás normatividad aplicable.

Paso 5. Determinar la criticidad del activo (Valoración del Activo):

Se evaluará la criticidad de los activos, mediante cuestionarios que determinen su importancia para la entidad. Esta valoración permitirá priorizar los riesgos en fases posteriores.

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas (ICC)

Las entidades públicas deberán aplicar la metodología y los criterios vigentes publicado por el centro cibernético de incidencias (ColCERT) para la identificación de Infraestructuras Críticas Cibernéticas. Un activo o sistema se considera ICC, si su afectación pudiera generar un impacto significativo en el bienestar social, la continuidad de los servicios esenciales, la economía o la estabilidad institucional.

Una vez identificadas las ICC, la entidad deberá:

•Identificar los componentes tecnológicos, procesos, sistemas y servicios que la conforman.

•Registrar dichas ICC en el inventario institucional de activos.

•Coordinar con las instancias nacionales la notificación o reporte cuando aplique. Este paso está alineado con lo establecido en el Decreto 338 de 2022 y los lineamientos de ColCERT para la protección de la infraestructura crítica cibernética.

Identificación de Riesgos.

Los riesgos asociados a los activos de información se clasifican según: pérdida de la confidencialidad, pérdida de la integridad o pérdida de la disponibilidad.

Valoración de amenazas y vulnerabilidades.

Se Identificarán amenazas y vulnerabilidades según la criticidad de los activos de información conforme con la Norma ISO 27005 y el Modelo de Gestión de Riesgos de Seguridad Digital del Anexo 4.

Determinación del Nivel de Riesgo de Seguridad de la Información.

El nivel de riesgo se determina combinando la valoración de los activos de información, el nivel de amenaza y la probabilidad de que una vulnerabilidad sea explotada. Esta metodología permitirá ubicar los riesgos en un mapa de calor, lo que facilita definir el nivel de riesgo aceptable.

Gestión del Riesgo.

Se podrán aplicar cuatro métodos para tratar los riesgos identificados:

- Aceptar el riesgo
- Tratar el riesgo
- Transferir el riesgo
- Evitar el riesgo

Sensibilizaciones y cultura organizacional

Para la vigencia 2026 se realizarán mínimo dos sensibilizaciones dirigidas a todos los funcionarios y contratistas, apoyados en el área Tic con uso y apropiación de la oficina TIC y el área de Comunicaciones. Se desarrollarán campañas continuas para fortalecer la cultura de seguridad y privacidad de la información, destacando la importancia de proteger los activos y datos críticos de la entidad.

8. DESARROLLO DE LA METODOLOGIA.

FASE	ACTIVIDAD	RESPONSABLE
Identificación de riesgos asociados a los activos de información	Identificar aquellos riesgos críticos a los que se encuentran expuestos los activos de información, mediante encuestas realizadas a los procesos o dueños de los activos de información. Luego de identificar los riesgos estos serán registrados en una matriz que permita su clasificación.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información – Líderes de procesos
Análisis del riesgo de seguridad de la información	Identificar y valorar los riesgos identificados considerando la probabilidad de ocurrencia y el impacto que podrían tener en caso de materializarse. Se utilizarán criterios de impacto: (Insignificante – Bajo – Moderado – Mayor – Catastrófico).	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información – Líderes de procesos
Evaluación de los controles establecidos para la mitigación de los riesgos.	Evaluar la efectividad de los controles implementados frente a los riesgos identificados Se analizará la adecuación de cada control según el riesgo, impacto y probabilidad de ocurrencia.	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.
Tratamiento	Adelantar acciones de implementación de controles y mejoras que permitan atender los riesgos identificados y valorados.	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.
Documentar	Documentar la implementación de controles	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información

9. RECURSOS

9.1 HUMANOS

Las actividades definidas en el Plan de Seguridad y Privacidad de la Información serán ejecutadas por los integrantes 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.

9.2 ECONÓMICOS

El desarrollo del Plan de Seguridad y Privacidad de la Información de la Unidad de Planificación Rural Agropecuaria (UPRA), está respaldado por los proyectos de inversión gestionados por la Oficina de Tecnologías de la Información y las Comunicaciones TIC de la Entidad, que incluyen:

•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:

- Implementación de soluciones tecnológicas innovadoras de manejo de información, con atributos de calidad e interoperabilidad (escalabilidad, seguridad, confiabilidad y articulación de sistemas información).
- 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.

9.3 FÍSICOS

Se consideran 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, tales como sistemas biométricos que faciliten la seguridad de acceso, equipos de seguridad perimetral de red y herramientas de escaneo y análisis de archivos.