UNIDAD DE PLANIFICACIÓN RURAL AGROPECUARIA UPRA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

BOGOTA D.C., ENERO 2024

INTRODUCCIÓN.

El plan de tratamiento de riesgos de seguridad de la información de la UPRA, se encuentra alineado con el Plan de Seguridad y Privacidad de la Información, con la GUIA POLÍTICA DE ADMINISTRACIÓN DE RIESGOS, que hace parte del Sistema de Gestión institucional, y tiene como fin la definición de actividades técnicas y organizacionales a tener en cuenta e implementar en la entidad, para atender las vulnerabilidades propias de los activos de información institucionales, en procura de reducir la pérdida de confidencialidad, integridad y disponibilidad de estos.

Adicionalmente, permite el fortalecimiento de los procesos y procedimientos que hacen parte de las medidas técnicas adoptadas como parte de la gestión de riesgos.

DEFINICIONES

- 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 i 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).

3. OBJETIVOS

3.1 GENERAL

Establecer las acciones a desarrollar durante la vigencia 2024, en el marco de la implementación de controles requeridos para mitigar los riesgos de seguridad de la información asociados a los diferentes activos de información institucionales.

3.2. ESPECÍFICOS

- Implementar acciones de tipo técnico que permitan gestionar los riesgos de seguridad de la información.
- Implementar acciones de tipo organizacional que permitan gestionar los riesgos de seguridad de la información.

4. ALCANCE.

El Plan de Tratamiento de Riesgos comprende el desarrollo de actividades enmarcadas en la declaratoria de aplicabilidad del SGSI. Debe ser de estricto cumplimiento por parte de los funcionarios, contratistas y terceros que presten sus servicios, o tengan algún tipo de relación con la UPRA, por lo cual, todos los procesos de la Entidad, en especial aquellos que impactan directamente la consecución de los objetivos misionales, deben involucrarse activamente en su ejecución.

5. NORMAS DE CALIDAD:

- Modelo de Seguridad y Privacidad de la Información de MINTIC: Tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.
- NORMA ISO 27001:2013: Estándar internación que tiene como objetivo sugerir lineamientos y buenas prácticas a cualquier tipo de organización o entidad para el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.
- ISO 31000:2018: Tiene como objetivo sugerir lineamientos y buenas prácticas a cualquier tipo de organización o entidad, para incorporar estándares y procesos de alto nivel para evaluar y mitigar riesgos en todas sus operaciones.
- 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 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

7. METODOLOGÍA DEL PLAN DE TRATAMIENTO DE RIESGOS

Identificación y valoración de Activos de Información,

Identificación de los responsables de los activos de información quienes son los responsables de realizar la identificación y categorización de estos. La identificación y valoración de activos de información se realiza conforme a lo establecido en el Modelo de Gestión de Riesgos de Seguridad Digital del Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, Imagen 1.

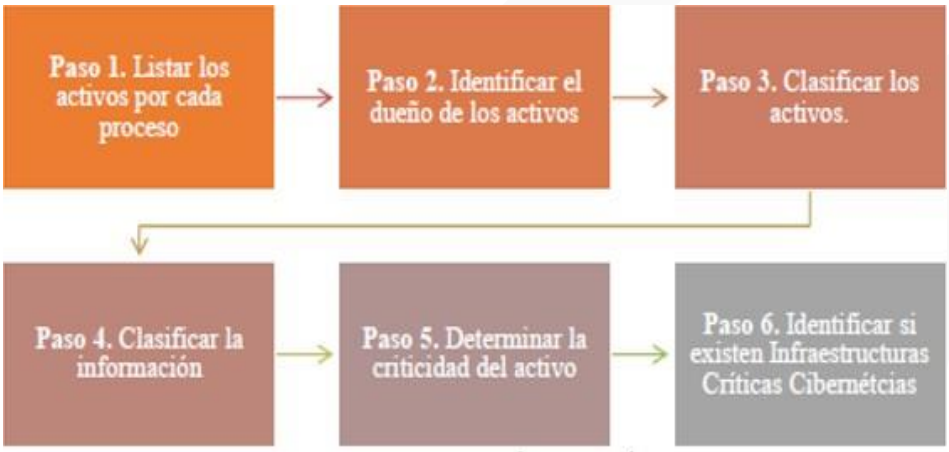

Imagen 1. Pasos para la identificación y valoración de activos.
Fuente: Ministerio de Tecnologías de la Información y Comunicaciones

Paso 1. Listar los activos por cada proceso:

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

Paso 2. Identificar el dueño de los activos:

Cada uno de los activos identificados deberá tener un dueño designado, Si un activo no posee un dueño, nadie se hará responsable ni lo protegerá debidamente.
Paso 3. Clasificar los activos:

Cada activo debe tener una clasificación o pertenecer a un determinado grupo de activos según su naturaleza cómo, por ejemplo: Información, Software, Hardware, Componentes de Red entre otros.

Paso 4. Clasificar la información:

Realizar la clasificación de la información conforme lo indican las leyes 1712 de 2014, 1581 de 2012, el Modelo de Seguridad y Privacidad en su Guía de Gestión de Activos, el dominio 8 del Anexo A de la norma ISO27001:2013 y demás normatividad aplicable.
Paso 5. Determinar la criticidad del activo (Valoración del Activo):

Ahora la entidad pública debe evaluar la criticidad de los activos, a través de preguntas que le permitan determinar el grado de importancia de cada uno, para posteriormente, durante el análisis de riesgos tener presente esta criticidad para hacer una valoración adecuada de cada caso.

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas -ICC-

Se invita a que las entidades públicas identifiquen y reporten a las instancias y autoridades respectivas en el Gobierno nacional si poseen ICC. Un activo es considerado infraestructura crítica si su impacto o afectación podría superar alguno de los siguientes 3 criterios:

- IMPACTO SOCIAL
- IMPACTO ECONÓMICO PIB de un Día o 0,123%
- IMPACTO AMBIENTAL

Identificación de Riesgos.

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

Valoración de amenazas y vulnerabilidades.

Identificación de amenazas y vulnerabilidades asociadas a los activos de información institucionales según el riesgo valorado, de acuerdo con la Norma ISO 27005 y el Modelo de Gestión de Riesgos de Seguridad Digital del Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

Determinación del Nivel de Riesgo de Seguridad de la Información.

La determinación del nivel de riesgo de seguridad de la información es la combinación de la valoración de los activos de información, el nivel de amenaza y la valoración de la probabilidad de la vulnerabilidad; para tal fin se definirá la metodología de valoración de riesgos que permita ubicar los riesgos identificados en un mapa de calor de clasificación de riesgos según la criticidad de los activos, de esta ubicación se determina el nivel de riesgo aceptable.

Gestión del Riesgo.

De acuerdo con la determinación del Nivel de Riesgo de Seguridad de la Información, se establece para la gestión de riesgos, los siguientes cuatro métodos:

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

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 riesgode seguridad de la información	Identificar y valorar los riesgos a los cuales están expuestos los activos de información con el fin de establecer controles apropiados de seguridad. Enesta fase se definen los criterios que se deben utilizar para evaluar la importancia del riesgo, de acuerdo con el impacto que pueda tener en caso de que este se materialice (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 los controles, luego de haber establecidoel riesgo inherente a cada activo de información, el impacto y probabilidad de ocurrencia. La evaluación de controles se realiza identificando los criterios relacionados a cada uno de los riesgos establecidos.	Oficial de seguridad de la información – Grupo de apoyo de seguridad de la información, grupo de serviciostecnológicos, de Sistemas de información y de gestión y análisis de información, servicios administrativos y almacén.
Tratamiento	Adelantar acciones de implementación decontroles 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 serviciostecnológicos, 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 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.

9.2 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:
- Implementación de soluciones tecnológicas innovadoras de manejo de información, con atributos de calidad e interoperabilidad (escalabilidad, seguridad, confiabilidad y articulación de sistemas información) y
- 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.

9.3 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, tales como biométricos que faciliten la seguridad, equipos de seguridad perimetral de red y herramientas de escaneo de archivos.