UNIDAD DE PLANIFICACIÓN RURAL AGROPECUARIA UPRA

PLAN DE TRATAMIENTO DE RIESGOS

BOGOTA D.C., SEPTIEMBRE DE 2019

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de la UPRA, hace parte del Plan de Seguridad y Privacidad de la Información de la UPRA a través del cual se realiza la implementación del Sistema de Gestión de Seguridad de la Información, que a su vez aterriza el Modelo de Seguridad y Privacidad de la Información (MSPI), alineado con el Marco de Referencia de Arquitectura de 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 por medio del Plan de Tratamiento de Riesgos 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 datos.

2. PLAN DE TRATAMIENTO DE RIESGOS.

El Plan de Tratamiento de Riesgos de la UPRA, identifica las acciones, responsables, recursos y prioridades en la gestión de los riesgos de seguridad de la información ya identificados, lo cual es aterrizado en una serie de políticas y procedimientos aplicados en la entidad.

2.1. Políticas de Seguridad de la Información.

Aportan en la implementación de los controles de Seguridad identificados en el Análisis de Riesgos realizado, y de acuerdo a la familia del control 5 de norma ISO 27002, “Política de Seguridad, la organización debe establecer las políticas de seguridad asociadas a diferentes dominios específicos de la seguridad de la información, abordando aspectos de la seguridad organizativa, lógica, física y legal, que permitan realizar una eficiente gestión de los activos de información identificados y valorados por los propietarios de los procesos, de tal forma que se vele por el adecuado aseguramiento de la información.”, en este sentido la UPRA ha definido el Manual de de Políticas de Seguridad de la Información, las cuales se encuentran alineadas con el alcance del SGSI, es decir son aplicables a los procesos y procedimientos de alcance del SGSI.

Entre las políticas de seguridad de la información de la UPRA, se encuentran:

- Política de Contraseñas
- Política de uso aceptable de activos
- Política de control de acceso
- Política de Backups
- Política de Retiro de Activos
- Política de entornos de desarrollo, pruebas y producción
- Política de borrado seguro
- Política de centro de datos
- Política de seguridad física y del entorno
- Política de control de cambios
- Política de gestión de medios removibles
- Política de continuidad y gestión de continuidad del negocio

2.2. Procedimientos

Si bien las políticas definidas en la UPRA establecen el qué, mediante procesos y procedimientos se establecen actividades del cómo ponerlas en funcionamiento, para lo cual la UPRA cuenta con procedimientos para:

- Soporte y Asistencia Técnica.
- Copias de Respaldo
- Gestión de servicios tecnológicos
- Actualización o modificación de componentes de TI.
- Gestión de situaciones de seguridad de la información
- Mantenimiento preventivo y/o correctivos de bienes e IT.

2.3. Formación.

La UPRA desarrolla jornadas de sensibilización y comunicación que permiten involucrar a todos los actores que forman parte de la implementación del SGSI, a través de la creación de conciencia y entendimiento de los mismos, enmarcadas en diferentes temáticas de seguridad de la información, dando cumplimiento al control 7.2.2 de la Norma ISO 27002 “Concientización, educación y capacitación de la seguridad de la información”.

El diseño y desarrollo de la estrategia de sensibilización, tiene como objetivo aportar en el desarrollo de las actividades que giran alrededor de la formación de competencias en los colaboradores de la unidad, que les sirva de base en la toma de decisiones acertadas y bien informadas sobre los temas de seguridad de la información, sus actuaciones y responsabilidades que se generen.

2.4. Clasificación de la Información.

Durante la implementación del SGSI de la UPRA, se definió la guía de clasificación de la información, que permite dar cumplimiento de los controles A.8.2.1, A.8.2.2 y A.8.2.3 del Anexo A de la norma ISO27001:2013. La guía comprende los niveles de clasificación de la información de la entidad, los roles identificados en el manejo de la información y el tratamiento indicado para cada nivel de clasificación.

2.5. Sistema de Métricas.

La UPRA cuenta con indicadores que permiten obtener resultados para medir la eficacia de los controles implantados, alineados con el SGI de la unidad y aplicados a la implementación del Modelo de Seguridad y Privacidad de la Información, que permite asegurar un proceso de mejoramiento continuo en la aplicación de los controles requeridos para la gestión de los riesgos de seguridad de la información identificados en los activos de información.