UNIDAD DE PLANIFICACIÓN RURAL AGROPECUARIA
UPRA

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

BOGOTA D.C., ENERO 2022

1 RESUMEN EJECUTIVO.

La UPRA, a través del proceso de servicios tecnológicos de la Oficina TIC, define el Plan de Tratamiento de Riesgos, con el fin de mitigar la pérdida de confidencialidad, integridad o disponibilidad de los activos de información, buscando evitar situaciones que impidan el logro de los objetivos misionales de la Entidad. El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos. Estas acciones comprenden la destinación de recursos físicos, técnicos y económicos, la definición de medidas, objetivos, justificación, responsable del tratamiento de la medida, su prioridad. Al definir estas acciones se logra identificar las herramientas necesarias y los procedimientos a seguir para la ejecución del Plan de Tratamiento de Riesgos.

2 INTRODUCCIÓN.

El plan de tratamiento de riesgos de seguridad de la información permite reducir la pérdida de confidencialidad, integridad y disponibilidad de los activos de información, mediante el descubrimiento de debilidades y el mejoramiento de los procesos y procedimientos, que buscan asegurar y resguardar información, enfrentando los riesgos identificados. Los riesgos más relevantes, como desastres naturales, procesos no adecuados en el tratamiento de la información, desconocimiento de normas y políticas de seguridad por parte de los funcionarios y el no cumplimiento de estas, suelen ser las razones más frecuentes y de mayor impacto en la seguridad de la información. A través de una cultura de carácter preventivo, mediante charlas de sensibilización, material gráfico de apoyo y medidas preventivas difundidas a todos los funcionarios y contratistas de la entidad, se busca dar a conocer el concepto de riesgo de seguridad de la información, así como su contexto, lo finalmente permite reducir la afectación, en caso de que uno o más de los riesgos identificados se materialicen. Adicionalmente se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor efectividad.

Para lograr la implementación exitosa del presente plan, es necesario el compromiso y cumplimiento de las siguientes acciones:

- Comprometer a la alta dirección de la entidad.
- Dar cumplimiento a la implementación del plan.
- Difundir y capacitar a todo el personal de la entidad, en el proceso de plan de gestión del riesgo de la seguridad de la información.

3 DEFINICIONES

- **Amenaza:** es un agente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo a una organización o entidad cuando logra materializarse.

- **Control o Medida:** acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
- **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.
- **Probabilidad:** es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Riesgo:** es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo en la organización o entidad.
- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

4 POLÍTICA DE ADMINISTRACION DE RIESGOS

Como estrategia principal, es necesario que todos los usuarios que hacen uso directo o indirecto de los activos de información de la UPRA, se comprometan a mantener una cultura de la gestión del riesgo asociados a los activos, apropiándose de las políticas, planes, programas y proyectos de la entidad y del sector, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de riesgos relacionados con la seguridad de la información. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, identifica las opciones para tratar y manejar los riesgos, permite tomar decisiones adecuadas y fija los lineamientos para administración de los mismos.

Luego de la detección de riesgos, se deberá trazar un plan de tratamiento que conlleve a su análisis, atención y gestión, para luego mitigarlos. De igual manera, para la adecuada gestión del riesgo se debe asignar un responsable del tratamiento, que debe ser el mismo dueño del proceso o responsable del activo.

5 ALCANCE.

La adecuada gestión y el buen tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, permite involucrar activamente los procesos de la entidad, para que adopten buenas prácticas que contribuyan a la toma de decisiones y prevención de incidentes que puedan afectar el logro de los objetivos misionales de la UPRA.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, 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.

6 OBJETIVO GENERAL.

Trazar una estrategia que permita definir los lineamientos y la metodología a seguir para el Plan de tratamiento de riesgos de Seguridad y privacidad de la información.

7 OBJETIVOS ESPECÍFICOS.

- Dar cumplimiento a las directrices y leyes impartidas en la legislación colombiana para la protección de la información.
- Implementar estrategias que permitan mantener la continuidad de la operación IT de la Entidad.
- Gestionar los riesgos de Seguridad y Privacidad de la Información y Seguridad Digital.
- Actualizar permanentemente los activos de información de la Entidad.
- Implementar y ejecutar un plan para la identificación y tratamiento de vulnerabilidades a los que están expuestos los activos de información.
- Atender y gestionar los incidentes de seguridad de la información con efectividad.
- Fortalecer las estrategias que permiten dar a conocer a funcionarios y contratistas, los temas relacionados a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

8 MARCO LEGAL Y NORMATIVO.

Para el soporte normativo y legal del presente Plan, la UPRA identifica como pilares principales las siguientes normas, leyes, decretos y estándares establecidos por el estado colombiano:

8.1 CONPES 3854 de 2016

Tiene como objetivo general identificar los riesgos a los que están expuestos los ciudadanos, las entidades del Gobierno y los empresarios en el entorno digital y que aprendan cómo protegerse, prevenir y reaccionar ante los delitos y ataques cibernéticos.

8.2 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.

8.3 Decreto 1008 de 14 de junio 2018

Tiene como objetivo oficializar el cambio de la estrategia de la política de gobierno digital.

8.4 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.

8.5 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.

9 DOCUMENTOS RELACIONADOS

Como apoyo al presente Plan, los siguientes documentos son de vital importancia para la identificación y tratamiento de los riesgos asociados a la seguridad de la información:

- Manual de la Política Seguridad y Privacidad de la Información.
- Inventario de activos de información.
- Inventario tecnológico.
- Procedimiento Gestión de Incidentes de Seguridad de la Información.
- Bitácora de Administración de IT.

10 IDENTIFICACIÓN DE VULNERABILIDADES.

Cómo estrategia para la identificación de vulnerabilidades la UPRA se soporta en su documentación disponible, sus planes de mejora y la experiencia del personal IT. Las vulnerabilidades identificadas son:

10.1 A nivel de entidad:

- Control de credenciales de acceso.
- Control de acceso a los activos de la información.
- Acuerdos de Nivel de Servicio ANS.
- Procedimientos para la identificación de vulnerabilidades.
- Procedimientos para el control de cambios.

10.2 A nivel de usuarios:

- Personal insuficiente.
- Conocimiento necesario.
- Falta de conciencia de seguridad.
- Desconocimiento del manual de políticas de seguridad de la información.
- Control del personal para el mantenimiento y limpieza.

10.3 A nivel de espacios físicos:

- Control de acceso a zonas restringidas.
- protección de zonas expuestas a riesgos medio ambientales.
- Red regulada.
- Protección de acceso zonas restringidas.

10.4 A nivel de red:

- Pruebas de seguridad a la infraestructura tecnológica IT.
- Pruebas de seguridad a los sistemas de información.
- Puntos de acceso desatendidos.
- Seguridad aplicada para la transmisión de datos.

10.5 A nivel de hardware:

- Mantenimiento de la infraestructura IT.
- Reemplazo de la IT obsoleta.
- Protección de la infraestructura crítica frente amenazas externas como la temperatura, el polvo y la humedad.
- Equipos de seguridad del tipo frontera.
- Equipos activos de Red
- Prácticas de almacenamiento de IT en condiciones favorables.
- Procedimiento para la disposición final de IT obsoleta.
- Copia de información no controlada.

10.6 A nivel de software:

- Procedimiento para las pruebas de seguridad de nuevas soluciones de software.
- Cuentas de usuario o sesiones desatendidas.
- Registros y logs de auditoría.
- Roles y asignación de permisos.
- Documentación de software.
- Mecanismos para la identificación y autenticación de usuarios.
- Software monitoreo de seguridad.
- Software end point.

11 METODOLOGÍA

Para ejecutar adecuadamente el Plan de Tratamiento de Riesgos, la Entidad establece una serie de fases que permiten identificar de los riesgos a los que están expuestos los activos información.

Fase	Actividad
Identificación de riesgos	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.
Valoración de los riesgos	Generar una lista completa de los riesgos, luego de haber completado la matriz anterior. Estos riesgos; según el DAFP, se pueden clasificar de acuerdo a los riesgos inherentes a la seguridad digital, (Confidencialidad, Integridad y Disponibilidad).
Análisis del riesgo de 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. En esta fase se definen los criterios que se deben utilizar para evaluar la importancia del riesgo, de acuerdo al impacto que pueda tener en caso de que este se materialice (Insignificante – Bajo – Moderado – Mayor – Catastrófico).
Evaluación de los controles establecidos para la mitigación de los riesgos.	Evaluar los controles, luego de haber establecido el 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.
Tratamiento	Adelantar acciones de mejora que permitan mantener la confidencialidad, integridad y disponibilidad de la información, mediante la identificación de los niveles de riesgo, su ponderación, las acciones requeridas y el tratamiento que se le dará (Mitigar - Aceptar). Es importante tener en cuenta que, de acuerdo a lo establecido en la ISO 31000:2018 el tratamiento de riesgos no son excluyentes entre sí, ni resultan eficaces en todas las circunstancias.

Así mismo, el plan de tratamiento incluye una serie de actividades relacionadas con las acciones a ejecutar para la consecución de plan.

Acción	Actividad	Responsable	Fecha de terminación
Actualizar el Manual de Políticas de Seguridad y Privacidad de la Información.	Implementar nuevas medidas que permitan garantizar la seguridad de la información, frente a nuevas amenazas o riesgos emergentes.	Servicios Tecnológicos - Oficial de seguridad	Junio 30 de 2022
Socialización y sensibilización.	Manual de Políticas de Seguridad y Privacidad de la Información.	Servicios Tecnológicos - Oficial de seguridad	Julio 30 de 2022
Identificar los de riesgos de seguridad y privacidad de la información.	Identificar los riesgos asociados a la seguridad y privacidad de la información, seguridad digital y plan de continuidad.	Servicios Tecnológicos - Oficial de seguridad	Septiembre 30 de 2022
Aceptación de riesgos identificados.	Aceptación, aprobación y planes de tratamiento de riesgos.	Oficina TIC – Servicios Tecnológicos	Octubre 31 de 2022
Publicación de riesgos identificados.	Publicación de la matriz de riesgos.	Servicios Tecnológicos - Oficina de Comunicaciones	Noviembre 10 de 2022
Tratamiento y seguimiento de riesgos identificados.	Realizar el seguimiento al tratamiento de riesgos identificados y verificación de evidencias.	Servicios Tecnológicos – Oficina asesora de Planeación.	Noviembre 30 de 2022
Evaluación de riesgos residuales.	Evaluar aquellos riesgos que se mantienen luego de los controles implementados en su mitigación, con el fin de alcanzar un nivel de aceptación.	Oficina TIC – Servicios Tecnológicos	Diciembre 10 de 2022
Mejoramiento.	Identificación de oportunidades de mejora, acorde a los resultados obtenidos durante la evaluación de riesgos residuales.	Oficina TIC – Servicios Tecnológicos – Oficial de Seguridad	Diciembre 17 de 2022
Monitoreo y revisión	Reporte de indicadores sobre la gestión del plan de riesgo.	Servicios Tecnológicos –	Diciembre 17 de 2022

12 RECURSOS NECESARIOS

Para lograr la ejecución del Plan Tratamiento de riesgos de seguridad y Privacidad de la información, la UPRA dispone de los siguientes recursos.

Humanos: es necesario contar con el personal técnico y profesional necesario para implementar, actualizar y realizar seguimiento a las políticas, procesos y procedimientos establecidos para la protección y seguridad de los activos de información y la mejora continua.

Técnicos: contar con los recursos tecnológicos necesarios para mantener en óptimas condiciones de trabajo la infraestructura tecnológica de la UPRA que soportan los activos de información de la Entidad.

Logísticos: contar con los recursos y herramientas necesarias para adelantar jornadas de socialización, trasferencia de conocimiento y realizar seguimiento constante a la gestión de riesgos.

Financieros: contar con los recursos necesarios para la adquisición de conocimiento, apoyo técnico y profesional y desarrollo de auditorías.

13 PRESUPUESTO

La UPRA ha destinado el presupuesto necesario para la ejecución del Plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad digital y Plan de continuidad IT, mediante la adquisición de nuevos equipos de seguridad perimetral, equipos de procesamiento, renovación de servicios de soporte técnico especializado con los fabricantes, migración de servicios a nube publica y nube privada y servicios de almacenamiento para copias de respaldo en nube privada. A además se cuenta con el personal técnico y profesional necesario para apoyar las tareas necesarias para la implementación de plan.