



## PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**AGENCIA DE RENOVACIÓN DEL TERRITORIO**

16/12/2019  
BOGOTA D.C.

## **1. INTRODUCCIÓN.**

La Agencia de Renovación del Territorio - ART buscando implementar un Modelo de seguridad y privacidad de la información – MPSI, que le permita asegurar el desarrollo de las políticas de gestión y directrices en materia de seguridad digital, así como realizar el seguimiento a la estrategia de Gobierno Digital y de seguridad de la información de la Agencia, establece el plan de seguridad y privacidad de la información, además El Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes seguridad digital y de la información de la Agencia y el logro de los propósitos de la Política de Gobierno Digital.

Teniendo en cuenta lo anterior se establece el siguiente plan para dar el cumplimiento respectivo.

## **2. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.**

Establecer las actividades que contemplen la implementación del Modelo de Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio de la Agencia.

## **3. ALCANCE**

Aplica a la agencia de Renovación del territorio a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la Agencia compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por el Ministerio TIC, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

## **4. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN**

Las funciones del Comité de Seguridad de la Información, serán asumidas por el Comité de Gestión y Desempeño de la ART.

## 5. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA ART

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma:

Gestión	Actividades	Responsables	Fechas Programación Tareas	
			Fecha de inicio	Fecha final
1.Publicación y Socialización de políticas	Socializar la Política General de seguridad de la información de la ART.	Asesor TI	01/02/2020	01/03/2020
	Socializar el Manual de políticas de seguridad de la información de la ART.	Asesor TI	01/02/2020	01/03/2020
	Plan de socialización, sensibilización y capacitación para la cultura organizacional y el uso y apropiación de TI	Asesor TI	01/03/2020	30/03/2020
	Implementar los Acuerdos de Confidencialidad	Asesor TI	01/03/2020	30/03/2020
	Actualizar y modificar el Manual de Políticas de seguridad de la información de la ART cuando sea necesario.	Grupo soporte informático	01/07/2020	30/07/2020
	Seguimiento y Evaluación de cumplimiento del Manual de políticas de Seguridad de la información de la ART.	Grupo soporte informático - Oficina Control interno - Oficina Planeación	01/11/2020	30/11/2020
2. Organización de la Seguridad de la información	Definir el Comité de Seguridad de la Información	Comité de Gestión y Desempeño		
	Definir las funciones del comité	Comité de Gestión y Desempeño		
	Definir un equipo de trabajo y de responsables que defina los lineamientos para la Gestión de los activos de información de la ART.	Comité de Gestión y Desempeño		
	Establecer funciones del Oficial de seguridad.	Asesor TI		
3.Gestión de Activos	Realizar una guía con su respectivo procedimiento para efectuar el levantamiento e inventario de activos de información de la ART.	Asesor TI - Grupo Soporte informático	01/03/2020	30/03/2020

	Socializar la política y la guía de Gestión de Activos de la ART.	Grupo Soporte informático	01/04/2020	30/04/2020
	Realizar el informe de levantamiento y Actualización de los activos de información de la ART entregados por las coordinaciones o grupos de trabajo involucrados.	Asesor TI - Grupo Soporte informático	01/05/2020	07/05/2020
	Validar y Aceptar los activos de información entregados al comité de activos.	Comité designado por Comité de Gestión y Desempeño	01/07/2020	30/07/2020
	Enviar al área jurídica el informe de registro de activos para su aprobación. Ley 1712 del 2014 Artículo 13.	soporte informático - Gestión Documental - Oficina jurídica	01/08/2020	30/08/2020
	Publicar los activos de información actualizados. Página Web de la entidad.	Oficina Comunicaciones	01/09/2020	30/09/2020
	Realizar Seguimiento y Evaluación a los Activos con reportes anuales sobre la actualización de los activos de información.	Oficina Planeación - Oficina Control interno	01/03/2021	02/03/2021
	4. Gestión de Riesgos	Adoptar una metodología que permita realizar la Gestión de Riesgos.	Asesor TI	01/04/2020
Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación de la ART.		Asesor TI	01/05/2020	01/06/2020
Verificación del Mapa de Calor.		Oficinas involucradas		
Realizar la Identificación, el Análisis y la Evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de la ART.		Asesor TI - Grupo Soporte informático- Gestión Documental	01/06/2020	01/08/2020
Retroalimentar los Riesgos Identificados en la ART.		Asesor TI - Grupo Soporte informático- Gestión Documental	01/08/2020	30/08/2020
Implementar la Matriz de Riesgos de la información de la ART.		Control Interno - Asesor TI	01/08/2020	30/08/2020

	Verificar la Matriz de Riesgos alimentada por las Áreas involucradas.	Control Interno	30/08/2020	01/09/2020
	Establecer Controles de Seguridad	soporte informático	01/09/2020	30/10/2020
	Realizar el Plan de Tratamiento de Riesgos y la verificación de controles de la ART.	Asesor TI - soporte informático - Gestión documental	01/09/2020	30/10/2020
	Evaluación de los Riesgos Residuales.	soporte informático - Gestión documental	30/10/2020	15/12/2020
	Seguimiento y evaluación de la Gestión de Riesgos.	Oficina Control interno - Oficina Planeación	01/06/2021	01/07/2021
5. Gestión de Incidentes de Seguridad de la información.	Revisión de la política de Gestión de incidentes de seguridad de la información en el Manual de políticas de la ART.	Asesor TI - soporte informático	01/02/2020	01/06/2020
	Actualización de la política de Gestión de incidentes de Seguridad y publicación.	Asesor TI - soporte informático	01/07/2020	30/07/2020
	Implementación del Procedimiento de Gestión de incidentes de seguridad.	soporte informático	01/08/2020	30/08/2020
	Atención, verificación y manejo de los incidentes de seguridad, según procedimiento definido.	soporte informático	01/09/2020	30/09/2020
	Integrar Incidentes de seguridad con el CSIRT - PONAL: "Equipo de Respuesta ante Incidentes de Seguridad de la Policía Nacional".	soporte informático	01/09/2020	30/10/2020
	Seguimiento a los Incidentes de seguridad y vulnerabilidades del MSPI.	soporte informático	01/06/2021	30/07/2021
	Participar en el Análisis de impacto del negocio.	soporte informático	01/10/2020	15/12/2020
6. Plan de Continuidad del Negocio	Realizar Colaborar en la construcción de un plan de continuidad del negocio	soporte informático	30/10/2020	15/12/2020
	Aprobar el plan de continuidad del negocio para que pase al comité de seguridad de la información de la ART.	soporte informático	01/03/2021	06/03/2021

7.Gobierno Digital	Actualizar el plan de la seguridad de la información de la ART	Asesor TI	01/02/2020	28/02/2020
	Hacer seguimiento a la política de gobierno digital en el Anexo de seguridad.	Asesor TI	01/03/2020	12/15/2020
	Realizar seguimiento al plan de seguridad y privacidad.	Oficina Planeacion	01/06/2020	15/12/2020
8.Auditorias y Mejora Continua	Realizar Auditorías Internas y Externas	Oficina Control Interno		
9.Vulnerabilidades	Definir lineamientos y alcance para ejecutar las pruebas de vulnerabilidades y pentest	soporte informático	01/06/2020	15/06/2020
	Contratar Análisis de Vulnerabilidades y Pentest, estudios previos, plan de contratación	soporte informático	16/06/2020	30/09/2020
	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis de vulnerabilidades y pentest	soporte informático	15/10/2020	30/11/2020
10.protección de datos personales	Recolectar bases de datos, Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo a los estándares emitidos por la SIC		01/04/2020	01/05/2020
	Revisión de bases de datos		01/06/2020	01/07/2020
	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información		01/08/2020	01/09/2020

## 6. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.
- Ley 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, en especial la

financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- 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 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.