AGENCIA DE RENOVACIÓN DEL TERRITORIO

RESOLUCIÓN NÚMERO _000709_ DE 2021

(23 NOVIEMBRE 2021)

"Por la cual se adoptan los lineamientos y estándares para la estrategia de seguridad digital, se acoge el Modelo de Seguridad y Privacidad de la Información (MSPI) y se crea el Equipo Técnico de Seguridad Digital y de la Información de la Agencia"

EL DIRECTOR GENERAL DE LA AGENCIA DE RENOVACIÓN DEL TERRITORIO

En ejercicio de sus facultades constitucionales y legales, en especial las conferidas por el parágrafo del artículo 16 del Decreto 2106 de 2019, por los numerales 1, 16 y 18 del artículo 6 del Decreto 1223 de 2020, y

CONSIDERANDO

Que el artículo 209 de la Constitución Política de Colombia dispone que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad, mediante la descentralización, la delegación y la desconcentración de funciones.

Que de acuerdo con lo previsto en los artículos 3 y 5 de la Ley 489 de 1998 y el artículo 3 de la Ley 1437 de 2011, las actuaciones administrativas se desarrollarán con arreglo, ente otros, a los principios de eficacia, economía, celeridad, así como de coordinación, concurrencia y subsidiaridad consagrados por el artículo 288 de la Constitución Política; los cuales deben ser observados en el señalamiento de las competencias propias de los organismos y entidades de la Rama Ejecutiva y en el ejercicio de las funciones de los servidores públicos.

Que el Decreto 2366 de 2015 creó la Agencia de Renovación del Territorio (ART) con el objeto de coordinar la intervención de las entidades nacionales y territoriales en las zonas rurales afectadas por el conflicto priorizadas por el Gobierno Nacional, a través de la ejecución de planes y proyectos para la renovación territorial de estas zonas, que permitan su reactivación económica, social y su fortalecimiento institucional, para que se integren de manera sostenible al desarrollo del país.

Que el artículo 10 del Decreto 1223 del 2020 establece como funciones de la Oficina de Tecnologías de la Información de la Agencia (en adelante la OTI), entre otras las siguientes: *"1. Impartir los lineamientos en materia tecnológica para definir políticas, estrategias y prácticas que soporten la gestión de la Agencia. (...) 3. Garantizar la aplicación de los estándares, buenas prácticas y principios para la gestión de la información a cargo de la Agencia. (...) 7. Impartir lineamientos para el cumplimiento de*

estándares de seguridad, privacidad, calidad y oportunidad de la información que administra la Agencia, así como el intercambio permanente de información con todos los actores en el marco las funciones de la Agencia".

Que conforme a las funciones transcritas anteriormente, la OTI tiene dentro de sus competencias funcionales el dictar los lineamientos así como coordinar la implementación de las estrategias y políticas para la seguridad de la información de todos los activos de información de la entidad.

Que el Director General de la ART, mediante la Resolución No. 00585 del 23 de octubre de 2020, modificó la Resolución No. 000142 del 20 de abril de 2018 que creó el Comité Institucional de Gestión y Desempeño, definió los responsables de las Políticas Institucionales de Gestión y Desempeño Institucional del Modelo Integrado de Planeación y Gestión (MIPG) y designó como dependencia responsable de liderar la Política de Seguridad Digital a la Oficina de Tecnologías de la Información (OTI).

Que el Decreto 1078 de 2015 Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, subrogado por el Decreto 1008 de 2018, estableció los lineamientos generales de la Política de Gobierno Digital; señalando en el artículo 2.2.9.1.1.3 los principios que rigen la Política, entre los que se encuentra el principio de Seguridad de la Información el cual *"busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano".*

Que el artículo 2.2.17.1.6 del Decreto 1078 de 2015, subrogado por el Decreto 620 de 2020, que estableció los lineamientos generales en el uso y operación de los servicios ciudadanos digitales, determinó los principios que orientan la prestación de los servicios ciudadanos digitales, señalando que por el principio de Seguridad, Privacidad y Circulación Restringida de la Información *"Toda la información de los usuarios que se genere, almacene, transmita o trate en el marco de los servicios ciudadanos digitales deberá ser protegida y custodiada bajo los más estrictos esquemas de seguridad digital y privacidad con miras a garantizar la autenticidad, integridad, disponibilidad, confidencialidad, el acceso y circulación restringida de la información, de conformidad con lo estipulado en el habilitador transversal de seguridad de la información de la Política de Gobierno Digital".*

Que el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, subrogado por el Decreto 1008 de 2018, contempla que la Política de Gobierno Digital se desarrolla a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generan valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC. Según el mismo artículo, los Habilitadores Transversales de la Política de Gobierno Digital son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha Política.

Que el artículo 147 (Transformación Digital Pública) de la Ley 1955 de 2019, *"Por la cual se expide el Plan Nacional de Desarrollo 2018-2022, Pacto por Colombia, Pacto por la Equidad"*, dispone que las entidades estatales del orden nacional deberán incorporar en sus respectivos planes de acción el componente de transformación digital siguiendo los estándares que para este propósito defina el Ministerio de Tecnologías de la Información y las Comunicaciones.

Que el parágrafo del artículo 16 del Decreto 2106 de 2019, *"Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública"*, establece que *"Las autoridades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones"*.

Que mediante la Resolución No. 00500 del 10 de marzo de 2021, el Ministerio de Tecnologías de la Información y las Comunicaciones estableció los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital; y estableció los lineamientos y estándares para la estrategia de seguridad digital.

Que mediante la Directiva Presidencial No. 03 del 15 de marzo de 2021, se dictan lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos; con el fin de disminuir los costos de funcionamiento, acelerar la innovación, brindar entornos confiables digitales para las entidades públicas y mejorar sus procedimientos y servicios.

Que el documento CONPES 3701 de 2011 (Lineamientos de Política para Ciberseguridad y Ciberdefensa), busca generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Tiene como objetivo central: *"Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio"*.

Que el documento CONPES 3854 de 2016 (Política Nacional de Seguridad Digital), indica que la Política incluye la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital, a través de principios y dimensiones estratégicas, involucrando activamente a todas las partes interesadas, y asegurando una responsabilidad compartida entre las mismas. Tiene como objetivo principal: *"Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país"*.

Que el documento CONPES 3995 de 2020 (Política Nacional de Confianza y Seguridad Digital), formula una política nacional que tiene como objetivo general: *"Establecer medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías"*.

Que de otra parte, el artículo 4 de la Ley 1581 de 2012, *"Por la cual se dictan disposiciones generales para la protección de datos personales"*, consagra los principios para el tratamiento de datos personales y específicamente en el literal g) sobre el principio de Seguridad señala: *"La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean*

necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento".

Que la 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"*, regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información. Así mismo, normaliza los Registros de Activos de Información, el Programa de Gestión Documental y, entre otras disposiciones, determina la clasificación de la información.

Que por disposición del artículo 21 del Decreto 1223 de 2020, a la Subdirección de Gestión de la Información de la Dirección de Información y Prospectiva (DIPRO), le corresponde, entre otras funciones, la de: *"Implementar en coordinación con la Oficina de Tecnologías de la Información las políticas orientadas a la captura, administración, tratamiento, procesamiento, integridad, calidad e intercambio de la información requerida por la entidad en el marco de la implementación de los PDET".*

Que el artículo 11 de la Resolución No. 000687 del 1° de diciembre de 2020, *"Por la cual se adoptan disposiciones transitorias en relación con la gestión y registro de la información para la implementación y seguimiento de los PDET, a través de los mecanismos tecnológicos y/o sistemas de información dispuestos por la Agencia de Renovación del Territorio"*, prescribe que los mecanismos tecnológicos y/o sistemas de información de la Agencia, como son el Banco de Proyectos de Inversión de la ART, el Sistema de Gestión de Oferta y el Sistema de Información Geográfico, serán administrados funcionalmente y técnicamente por la DIPRO. La Dirección de Información y Prospectiva realizará la creación de usuarios y administrará sus accesos, en concordancia con las políticas de seguridad y privacidad definidas por la Oficina de Tecnologías de la Información.

Que el artículo 14 de la Resolución No. 000687 de 2020 señala que en los procesos de planeación para la posterior suscripción de convenios, acuerdos, memorandos de entendimientos y/o documentos similares, relacionados con el intercambio e interoperabilidad de la información con entidades públicas o privadas, nacionales o extranjeras, corresponderá a la DIPRO a través de la Subdirección de Gestión de la Información, validar técnicamente su procedencia, siguiendo los lineamientos y las políticas en materia de intercambio e interoperabilidad de la información que para el efecto establezca la Oficina de Tecnologías de la Información (OTI).

Que conforme a lo dispuesto por el artículo 5 de la Resolución No. 000530 del 7 de septiembre de 2021, *"Por la cual se conforma la Mesa de Trabajo para el Modelo de Gobierno de Información Misional PDET y se determinan su funcionamiento y conformación"*; la Mesa de Trabajo tiene entre sus funciones la de *"Impulsar el uso de las políticas y lineamientos de seguridad de la información que desde la Oficina de Tecnologías de la Información se establezcan, dentro del marco del Modelo de Gobierno de Información Misional PDET".*

Que con fundamento en las anteriores consideraciones, se hace necesario adoptar los lineamientos y estándares para la Estrategia de Seguridad Digital, acoger el Modelo de Seguridad y Privacidad de la Información (MSPI) y crear el Equipo Técnico de Seguridad Digital y de la Información de la Agencia de Renovación del Territorio (ART).

Que en cumplimiento del Decreto 1081 de 2015, Único Reglamentario del Sector Administrativo de la Presidencia de la República, modificado por el Decreto 270 de 2017, del artículo 8 de la Ley 1437 de 2011 y de la Resolución No. 000423 del 14 de junio de 2017 expedida por la Dirección General de la ART, el proyecto de Resolución

fue publicado en el sitio web de la Agencia de Renovación del Territorio (ART) para comentarios de la ciudadanía.

Que, en mérito de lo expuesto,

RESUELVE

Capítulo I
Modelo de Seguridad y Privacidad de la Información y Estrategia de Seguridad Digital

Artículo 1. *Objeto.* El presente acto administrativo tiene por objeto adoptar los lineamientos y estándares para la Estrategia de Seguridad Digital, acoger el Modelo de Seguridad y Privacidad de la Información (MSPI) y crear el Equipo Técnico de Seguridad Digital y de la Información de la Agencia de Renovación del Territorio.

Artículo 2. *Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).* La Agencia de Renovación del Territorio (ART) acoge el Modelo de Seguridad y Privacidad de la Información (MSPI) adoptado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), como habilitador de la Política de Gobierno Digital; y para su cumplimiento, lo implementará a través del Sistema de Gestión y Seguridad de la Información (SGSI) y lo alineará con el Plan de Seguridad y Privacidad de la Información y los demás planes estratégicos de la Agencia.

El Plan de Seguridad y Privacidad de la Información deberá ser revisado y aprobado anualmente por el Comité Institucional de Gestión y Desempeño (CIGD).

La Oficina de Tecnologías de la Información (OTI), como responsable de la Estrategia de Seguridad Digital, deberá articular el SGSI con el Programa Integral de Gestión de Datos Personales (PIGDP), para definir los controles y condiciones de protección y privacidad de los datos.

Artículo 3. *Política General de Seguridad y Privacidad de la Información y Manual de Políticas de Seguridad Digital y de la Información.* La Oficina de Tecnologías de la Información (OTI) será la responsable de definir y liderar la Política General de Seguridad y Privacidad de la Información y el Manual de Políticas de Seguridad Digital y de la Información; los cuales serán de obligatorio cumplimiento para todos los funcionarios, contratistas y colaboradores que apoyen las labores de la Agencia, quienes tienen el deber de conocerlos y aplicarlos.

La OTI será la encargada de liderar las capacitaciones y las sensibilizaciones de seguridad de la información, fomentando el uso y apropiación de la seguridad digital y de la información.

Parágrafo. Cuando se advierta una posible violación de la seguridad de la información deberá ser puesta en conocimiento de Control Disciplinario de la ART, para que en el marco de sus competencias adelante las actuaciones a que haya lugar de conformidad con la Ley.

Artículo 4. *Gestión de Activos de Información.* Todos los procesos que hacen parte de la Agencia deberán elaborar y mantener actualizado el Registro de Activos de Información, constituido por el inventario de la información pública que la ART genera, obtiene, adquiere o controla; elaborado con la información, requisitos y procedimientos

establecidos por la entidad para tales efectos y de conformidad con las normas vigentes.

El Registro de Activos de Información será actualizado con una periodicidad anual o por demanda cuando existan cambios representativos; y aprobado por el Comité Institucional de Gestión y Desempeño (CIGD), previa revisión de la Oficina de Tecnologías de la Información y del Equipo Técnico de Seguridad Digital y de la Información.

Los instrumentos generados para el levantamiento del Registro de Activos de Información serán diseñados, publicados y socializados por la OTI, el Grupo Interno de Trabajo de Servicios Administrativos y las demás dependencias que interactúan en el proceso cuando sea requerido.

Artículo 5. ***Gestión de Riesgos de Seguridad Digital y de la Información.*** La ART adopta la metodología de gestión de riesgos de seguridad digital y de la información impartida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) y el Departamento Administrativo de la Función Pública (DAFP), con el fin de mitigar los riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital, y realizar una adecuada gestión de riesgos que permita la identificación, análisis, valoración de riesgos e implementación de los controles técnicos, así como definir un plan de tratamiento de los riesgos de seguridad digital y de la información.

Todos los procesos participarán en la identificación y valoración de los riesgos de seguridad digital y de la información con los lineamientos de la OTI y deberán implementar los controles que se generen en el plan de tratamiento de los riesgos de seguridad digital y de la información. Los instrumentos generados para el levantamiento y gestión de los riesgos de seguridad digital y de la información serán diseñados por la OTI; el seguimiento y socialización corresponderá a la Oficina de Planeación.

Artículo 6. ***Cultura para la seguridad digital y de la información.*** La OTI definirá el Plan de Sensibilización y Capacitación de Seguridad Digital y de la Información, con el fin de promover la cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y colaboradores que la ART considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Este plan debe estar articulado con el Plan Institucional de Capacitaciones (PIC) y se revisará con una periodicidad anual.

Artículo 7. ***Tecnologías emergentes.*** En la Estrategia de Seguridad Digital, además de todas las tecnologías de la información y las comunicaciones que utiliza la ART, se tendrá en cuenta la adopción de nuevas tecnologías o tecnologías emergentes con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información.

Artículo 8. ***Controles e Interoperabilidad.*** Desde la OTI se implementarán controles y procesos que habiliten la integración al servicio ciudadano digital de interoperabilidad de forma segura y cumpliendo las directrices dadas sobre el particular en el marco de la Política de Gobierno Digital. Por esta razón todos los servicios de interoperabilidad o procesos de intercambio de información realizados con otras entidades estarán sujetos al acompañamiento y supervisión de la OTI para preservar la seguridad digital y de la información.

Artículo 9. ***Sistemas de información administrados funcional y técnicamente por otras dependencias.*** Las Dependencias que dentro de sus funciones deban realizar actividades de desarrollo de software, custodia y administración de sistemas de información, deberán diseñar e implementar los controles tecnológicos y de seguridad de la información, así como los planes de tratamiento que eviten la materialización de riesgos para asegurar la confidencialidad, integridad y disponibilidad de la información. Los controles y planes diseñados por las dependencias deberán ser revisados por la OTI, que orientará su implementación como responsable de la Estrategia de Seguridad Digital.

Parágrafo. Respecto de la información asociada a la implementación y seguimiento de los PDET, gestionada y registrada en los mecanismos tecnológicos y/o sistemas de información dispuestos por la Dirección de Información y Prospectiva (DIPRO), la Mesa de Trabajo para el Modelo de Gobierno de Información Misional PDET, conformada mediante la Resolución No. 000530 del 7 de septiembre de 2021, impulsará el uso de las políticas y lineamientos de seguridad de la información que desde la Oficina de Tecnologías de la Información se establezcan, dentro del marco del Modelo de Gobierno de Información Misional PDET, en los términos dispuestos por el artículo 5 de la citada Resolución.

Capítulo II
Incidentes de Seguridad Digital y de la Información

Artículo 10. ***Gestión de Incidentes de Seguridad Digital y de la Información.*** La OTI establecerá un procedimiento de gestión de incidentes de seguridad digital y de la información para realizar el tratamiento, investigación y gestión de los incidentes de seguridad digital de los activos de información, que permita además detectar, analizar y mitigar un riesgo. Todos los colaboradores deberán hacer buen uso de los recursos tecnológicos asignados y reportar a la OTI los incidentes o riesgos que se puedan detectar en los activos de información a su cargo.

Capítulo III
Equipo Técnico de Seguridad Digital y de la Información

Artículo 11. ***Equipo Técnico de Seguridad Digital y de la Información.*** Créase el Equipo Técnico de Seguridad Digital y de la Información de la Agencia de Renovación del Territorio (ART).

Artículo 12. ***Conformación.*** El Equipo Técnico de Seguridad Digital y de la Información estará conformado por:

1. El Jefe de la Oficina de Tecnologías de la Información o su delegado, quien lo presidirá.
2. El Oficial de Protección de Datos Personales o su delegado.
3. Un servidor público representante de la Oficina de Planeación.
4. Un servidor público representante de la Dirección de Sustitución de Cultivos de Uso Ilícito.
5. Un servidor público representante de la Dirección de Información y Prospectiva.
6. Un servidor público con funciones en gestión documental.
7. Un servidor público con funciones en seguridad de la información.

Parágrafo. El Equipo Técnico podrá invitar a cada reunión, con voz y sin voto, a aquellas personas que considere necesarias por la naturaleza de los temas a tratar.

Artículo 13. ***Funciones del Equipo Técnico de Seguridad Digital y de la Información.*** El Equipo Técnico de Seguridad Digital y de la Información de la Agencia de Renovación del Territorio tendrá las siguientes funciones:

1. Apoyar a la OTI en la implementación del Modelo de Seguridad y Privacidad de la Información al interior de la Agencia.
2. Revisar los diagnósticos del estado de la seguridad de la información y proponer al líder de la Estratega de Seguridad Digital, un plan de mejora para mitigar los riesgos y cerrar las brechas identificadas.
3. Acompañar e impulsar el desarrollo de proyectos de seguridad digital y de la información.
4. Recomendar roles y responsabilidades específicos que se relacionen con la seguridad de la información.
5. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
6. Apoyar las estrategias de seguridad de la información que, en el marco de las competencias de la OTI, permitan la implementación de los controles necesarios para contribuir a la protección de los datos personales en la Agencia.
7. Impulsar las políticas, procedimientos y herramientas del Sistema de Gestión de Seguridad Digital y de la Información aprobados por el Comité Institucional de Gestión y Desempeño (CIGD).
8. Recomendar acciones para la gestión de los incidentes de seguridad digital, para proteger la información y asegurar la continuidad de las operaciones y los servicios tecnológicos.
9. Verificar el cumplimiento normativo y las buenas prácticas de seguridad digital y de la información en marco de la estrategia.
10. Apoyar a la Oficina de Tecnologías de la Información en la revisión del Registro de Activos de Información para aprobación de las actualizaciones por parte del Comité Institucional de Gestión y Desempeño, y proponer estrategias para la gestión de los activos de información de la entidad.
11. Hacer recomendaciones frente al plan de tratamiento de los riesgos de seguridad digital y de la información, así como proponer acciones para su cumplimiento.
12. Apoyar a la OTI en la definición del Plan de Sensibilización y Capacitación de Seguridad Digital y de la Información para aprobación del Comité Institucional de Gestión y Desempeño.
13. Apoyar y dar acompañamiento a la OTI en la atención de las auditorías internas y externas que se realicen en el marco de la Estrategia de Seguridad Digital y en las revisiones al Modelo de Seguridad y Privacidad de la Información (MSPI).

Artículo 14. ***Reuniones del Equipo Técnico de Seguridad Digital y de la Información.*** El Equipo Técnico de Seguridad Digital y de la Información se reunirá mínimo una (1) vez cada trimestre o cuando se requieran reuniones extraordinarias, previa convocatoria realizada por el Jefe de la Oficina de Tecnologías de la Información, cuya asistencia es de carácter obligatorio.

Capítulo IV
Roles y Responsabilidades de Seguridad Digital y de la Información

Artículo 15. ***Roles y responsabilidades de seguridad digital y de la información.*** Los roles y responsabilidades de seguridad digital y de la información son determinados por la Agencia de Renovación del Territorio en el Manual de Políticas de Seguridad Digital y de la Información, adoptado por el Comité Institucional de Gestión y Desempeño, en concordancia con el Modelo de Seguridad y Privacidad de la Información (MSPI) que se acoge por el presente acto administrativo.

Capítulo V
Etapas Generales de la Gestión de Incidentes de Seguridad Digital y de la Información

Artículo 16. ***Definición de las etapas.*** Las etapas generales de la gestión de incidentes de seguridad digital y de la información, según el Modelo de Seguridad y Privacidad de la Información (MSPI), se encuentran enfocadas a:

1. **Prevención.** La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de ciberseguridad.
2. **Protección y detección.** La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos.
3. **Respuesta y comunicación.** Aún con las medidas de seguridad adoptadas, la Agencia debe desarrollar e implementar planes de respuesta a incidentes de seguridad digital y de la información.
4. **Recuperación y aprendizaje.** Desarrollar e implementar actividades apropiadas para definir y mantener los planes de recuperación, resiliencia y restauración de las infraestructuras críticas, servicios, sistemas de información, procesos o en general de un activo de información que se haya deteriorado debido a un incidente de seguridad digital y de la información.

Parágrafo. La Estrategia de Seguridad Digital y la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) son transversales y de aplicación a todos los procesos que forman parte de la Agencia de Renovación del Territorio, en consecuencia, los funcionarios, contratistas y colaboradores de la ART participarán activamente en el desarrollo de las actividades que la OTI disponga para la ejecución de cada una de las etapas establecidas en el presente artículo.

Artículo 17. ***Vigencia.*** La presente Resolución rige a partir de la fecha de su publicación.

PUBLÍQUESE y CÚMPLASE

Dada en Bogotá, D.C., a los **23 NOVIEMBRE 2021**

JUAN CARLOS ZAMBRANO ARCINIEGAS
Director General

Proyectó: Yuli Andrea Parra Amaya, Contratista Oficina de Tecnologías de la Información.
Revisó: Freddy Aguas Barbosa, Gestor Oficina de Tecnologías de la información.
María Cristina Ortega Vega, Gestor Oficina Jurídica.
David Jesús Morales Pérez, Jefe Oficina Jurídica. DJMP
Cristina González Pérez, Directora de Información y Prospectiva.
Marcela Castro Macías, Secretaria General.
Aprobó: Sofía Salamanca Barrera, Jefe Oficina de Tecnologías de la información.