“Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a la Resolución No. 500 de 2021”

**LA MINISTRA DE TECNOLOGÍAS DE LA INFORMACIÓN Y
LAS COMUNICACIONES**

En ejercicio de sus facultades legales, en especial las que le confiere el parágrafo del artículo 16 del Decreto 2106 de 2019, y

**CONSIDERANDO QUE**

Conforme al principio de "masificación del gobierno en línea" hoy Gobierno Digital, consagrado en el numeral 8 del artículo 2 de la Ley 1341 de 2009, las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones (TIC) en el desarrollo de sus funciones.

De acuerdo con el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015 (DUR-TIC), "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", la Política de Gobierno Digital será definida por MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Según el numeral 2, los habilitadores transversales de la Política de Gobierno Digital, son los elementos fundamentales de Seguridad y Privacidad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de dicha Política.

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” señala que las autoridades deberán disponer de una estrategia de seguridad digital, para la gestión documental electrónica y preservación de la información, siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Mediante la Resolución N°. 500 de 2021 de MinTIC, “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” se adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI).

El numeral 4 del artículo 147 de la Ley 1955, «Por el cual se expide el Plan Nacional de Desarrollo 2018-2022 "Pacto por Colombia, Pacto por la Equidad”», como parte integral de las estrategias integrales de transformación digital para crear valor público dispuso que las entidades estatales deben optimizar la gestión de recursos públicos en proyectos de tecnologías dando prioridad a los servicios de nube.

La pandemia global de COVID-19 aceleró la transformación digital de la administración pública, ya que una parte significativa de las entidades y colaboradores han adoptado mecanismos de teletrabajo y trabajo en casa y que a su vez esta dinámica implica la necesidad de fortalecer capacidades que soportan los servicios tecnológicos, con características como flexibilidad, oportunidad y disponibilidad, como las ofrecidas en entornos de computación en la nube.

Algunos de los sistemas de información en la nube procesan datos personales y su tratamiento en este tipo de entornos informáticos viene en aumento, así mismo, el número de oportunidades en las que una entidad necesita cooperar con otras entidades o proveedores en relación con el tratamiento de datos personales también se ha incrementado. Por lo tanto, la gestión de la seguridad de la información en estos entornos requiere que se incorporen lineamientos adicionales a los establecidos actualmente en el MSPI.

De acuerdo con el principio de seguridad contenido en el régimen de protección de datos, en el tratamiento de la información contenida en los bancos de datos, así como aquella que resulte de las consultas que realicen los usuarios, se deben adoptar las medidas técnicas necesarias para garantizar la seguridad de los registros, con el fin de evitar su adulteración, pérdida, consulta o uso no autorizado.

Las entidades públicas dan cumplimiento a las obligaciones previstas en el MSPI a través de la adquisición de productos y servicios de múltiples proveedores, y que estos pueden tener acceso directo o indirecto a la información y los sistemas de información de las entidades adquirientes, o proporcionarán elementos (software, hardware, procesos o recursos humanos) que están involucrados en el procesamiento de la información.

Por lo tanto, las entidades públicas, como partes adquirientes de productos y servicios y los proveedores pueden causar riesgos de seguridad de la información entre sí, lo que deriva en la necesidad de evaluar y tratar los riesgos mediante una gestión adecuada de la seguridad de la información y la implementación de los controles pertinentes.

Por otra parte, durante el 2021 se atendieron 5.834 incidentes de ciberseguridad ciudadana, acorde con lo reportado por El Centro Cibernético Policial-CCP, asimismo, el Equipo de Respuesta a Incidentes Cibernéticos de Gobierno - CSIRT Gobierno, registró durante el mismo periodo 323 incidentes a los sistemas de la administración pública.

En febrero de 2022, el Equipo de Respuesta a Incidentes Cibernéticos de los Estados Unidos USCERT emitió un documento de Asesoramiento en Ciberseguridad donde alerta que las autoridades de seguridad digital de los Estados Unidos, Australia y el Reino Unido observaron un aumento en los incidentes de ransomware sofisticados y de alto impacto contra organizaciones de infraestructura crítica en todo el mundo. Dichas autoridades alertaron que las tácticas y técnicas de ransomware continuaron evolucionando en 2021, y se evidencia una creciente sofisticación tecnológica de los actores criminales y una mayor amenaza de ransomware para las organizaciones a nivel mundial.

Que el 16 de febrero de 2022 este Ministerio público para conocimiento de las múltiples partes interesadas la propuesta para fortalecer el MSPI y adicionar lineamientos a la Resolución 500 de 2021. Para tal efecto, se dispuso un término comprendido entre la mencionada fecha de publicación y el XX de febrero de 2022, con el fin de garantizar así la participación de todos los agentes interesados.

Teniendo en cuenta la coyuntura expuesta se hace necesario fortalecer el MSPI y definir lineamientos adicionales para mitigar los riesgos de seguridad de la información en los ámbitos anteriormente señalados.

En mérito de lo expuesto,

**RESUELVE:**

**ARTÍCULO 1.** Adiciónese el numeral 7 al artículo 5 a la Resolución MinTIC No. 500 de 2021, en los siguientes términos:

“7. Contener los servicios, controles y condiciones para la protección de los datos personales de los titulares de información de modo que se asegure el cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios o aquella que la modifique o sustituya.”

**ARTÍCULO 2.** Adiciónese los numerales 12 y 13 al artículo 6 a la Resolución MinTIC No. 500 de 2021, en los siguientes términos:

 “12. Determinar e implementar controles de protección de la privacidad en aquellos sistemas relacionados con el tratamiento de datos personales.

13. Adoptar medidas, al momento de adquirir productos y servicios de Seguridad Digital operados en entornos de nube, que garanticen el cumplimiento de lo dispuesto en la Ley Estatuaria 1581 de 2012 y sus normas reglamentarias, en particular las relativas a la transferencia internacional de datos personales.”

**ARTÍCULO 3**. Adiciónese el artículo 6.1 a la Resolución MinTIC No. 500 de 2021, en los siguientes términos.

“**ARTÍCULO 6.1 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** **PARA LAS RELACIONES CON LOS PROVEEDORES.** Los sujetos obligados deben determinar e implementar los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital señalados en el Anexo 2 de la presente resolución, así como cumplir con los siguientes requerimientos y características.

1. Definir claramente los roles y responsabilidades de seguridad de la información con respecto a la relación con el proveedor.
2. Al adquirir productos o servicios de Seguridad Digital se deberá propender por mantener una arquitectura de seguridad.
3. Analizar los riesgos de Seguridad Digital propios de la integración de soluciones e implementar controles para su mitigación.
4. Implementar controles que permitan minimizar los riesgos asociados a la transferencia de datos generada por cambios de fabricante o proveedor.
5. Identificar la vida útil de los productos y servicios adquiridos con el fin de planificar cualquier migración o transferencia y respaldar los datos para garantizar la continuidad de la operación.
6. Optimizar la gestión de los riesgos de Seguridad Digital estableciendo estrategias soportadas en servicios de nube.

**Parágrafo.** Los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital señalados en el Anexo 2, serán actualizados por el MinTIC a través de las sucesivas versiones de cada uno de los documentos que lo componen y previo informe del equipo técnico. La actualización se publicará en la sede electrónica de MinTIC.”

**ARTÍCULO 4. *Vigencia.*** La presente resolución rige a partir de la fecha de su publicación en el Diario Oficial.

**PUBLÍQUESE Y CÚMPLASE**

Dada en Bogotá D.C. a los

**CARMEN LIGIA VALDERRAMA**

Ministra de Tecnologías de la Información y las Comunicaciones

Elaboró: Felipe Sarmiento- Asesor de la Dirección del Viceministerio de Transformación Digital

 Danny Alejandro Garzón Aristizábal- Asesor de la Dirección de Gobierno Digital

Revisó: Angela Janeth Cortés Hernández-Profesional Especializado del Viceministerio de Transformación Digital

 Ivan Marrugo -Coordinador Equipo de política de la Dirección de Gobierno Digital

 Marco Sánchez- Abogado Equipo de política de la Dirección de Gobierno Digital

 Ingrid Tatiana Montealegre – Directora de Gobierno Digital

 Aprobó: Ivan Duran – Viceministro de Transformación Digital