DIRECTIVA PRESIDENCIAL 3 DE 2021

(marzo 15)

Diario Oficial No. 51.617 de 15 de marzo de 2021

PRESIDENCIA DE LA REPÚBLICA

PARA	ENTIDADES PÚBLICAS DE LA RAMA EJECUTIVA DEL ORDEN NACIONAL.
DE	PRESIDENTE DE LA REPÚBLICA.
ASUNTO	LINEAMIENTOS PARA EL USO DE SERVICIOS EN LA NUBE, INTELIGENCIA ARTIFICIAL, SEGURIDAD DIGITAL Y GESTIÓN DE DATOS.

Con el fin de dar cumplimiento al artículo 147 de la Ley 1955 de 2019, “por el cual se expide el Plan Nacional de Desarrollo 2018-2022 “Pacto por Colombia, Pacto por la Equidad”, disminuir los costos de funcionamiento, acelerar la innovación, brindar entornos confiables digitales para las entidades públicas y mejorar sus procedimientos y servicios, se imparten las siguientes directrices:

1. USO DE SERVICIOS DE NUBE

1.1. Dar cumplimiento a las directrices en materia de computación en la nube proferida por el Ministerio de Tecnologías de la Información y las Comunicaciones.

1.2. Evaluar y optimizar la gestión de recursos públicos en proyectos de Tecnologías de la Información a través del uso de los instrumentos de agregación de demanda y priorización de los servicios de nube, para atender las necesidades de los grupos de interés y con base en los costos y beneficios de esta posibilidad.

1.3. Garantizar que los recursos proporcionados por los servicios de nube crezcan o decrezcan en cualquier momento, en algunos casos automáticamente, con el fin de ajustar rápidamente el aprovisionamiento requerido y responder adecuadamente a la demanda de los usuarios, de acuerdo con la necesidad técnica para el uso o aplicación respectivo.

1.4. En la medida de lo posible, usar tecnologías agnósticas y tecnológicamente neutrales que permitan el despliegue en distintos proveedores con el fin de evitar la dependencia de un proveedor en particular.

1.5. Contratar los servicios de nube que se encuentren contemplados en los acuerdos marco de precios vigentes, u otros mecanismos que para el efecto hayan sido establecidos por Colombia Compra Eficiente o la modalidad de contratación contenida en el Estatuto de Contratación Pública.

1.6. Los servicios de nube deberán permitir la interoperabilidad con otras nubes o centros de cómputo locales (en la entidad).

1.7. Dar cumplimiento al conjunto de normas que integran la política de gobierno digital, proferida por el Ministerio de Tecnologías de la Información y las Comunicaciones, y particularmente en lo que respecta a seguridad digital, cumplir con los lineamientos y estándares señalados en el habilitador de seguridad y privacidad.

1.8. Las entidades destinatarias de la presente Directiva, dentro de los seis (6) meses siguientes a su expedición, deberán elaborar un plan de implementación para el uso de servicios de nube que contemple los criterios referidos, el cual deberá estar articulado al Diagnóstico del Modelo de Seguridad y Privacidad de la información y realizando las actualizaciones pertinentes en el Plan Estratégico de Tecnologías de la información - PETI.

2. INTELIGENCIA ARTIFICIAL (IA)

2.1. El uso de sistemas de IA deberá propender por el crecimiento inclusivo, el desarrollo sostenible y el bienestar de los ciudadanos. La IA debe mejorar la calidad de vida de los colombianos.

2.2. En caso de implementar proyectos de IA, deberán informar sobre sus avances, dentro de los respectivos informes anuales de rendición de cuentas.

2.3. Fomentar la participación de los funcionarios públicos en cursos, capacitaciones o programas de talento dirigidos a generar mayor conocimiento y capacidades sobre IA, su implementación, características y funcionalidades, dando cumplimiento a las directrices de austeridad en el gasto.

2.4. Facilitar la realización de sandboxes regulatorios en IA en el marco de la coordinación y articulación interinstitucional.

2.5. Efectuar el desarrollo de los Proyectos de IA en el marco de la coordinación interinstitucional y en apoyo a la cooperación internacional que surja en la materia, permitiendo el intercambio de información y el seguimiento a las recomendaciones, con sujeción a las funciones asignadas y a la normativa aplicable.

2.6. En el marco de 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”, informar a la ciudadanía cuando estén implementando un proyecto que incorpore sistemas de IA y el propósito de su uso, brindando información clara y actualizada, con el fin de asegurar el conocimiento de esta tecnología y las características de los proyectos.

2.7. Formular y desarrollar proyectos de IA, dando cumplimiento a las recomendaciones y principios éticos en la materia.

2.8. Desplegar los sistemas de IA sobre la base de sus funciones, el contexto y en consonancia con el estado de la técnica. Para este fin implementarán medidas que permitan demostrar de forma activa su diligencia y cuidado en la implementación de estos sistemas.

2.9. Según sus roles, el contexto y su capacidad para actuar, aplicar un enfoque sistemático de gestión de riesgos en cada fase del ciclo de vida del sistema de IA para abordar los riesgos relacionados con los sistemas de IA y su implementación, reduciendo cualquier riesgo de discriminación, entre otras posibles afectaciones.

2.10. Documentar los procesos y las decisiones adoptadas durante el ciclo de vida del sistema de IA, para permitir el análisis de sus resultados, teniendo en cuenta el contexto y siendo coherente con el estado de la técnica.

3. SEGURIDAD DIGITAL

Con el fin de fortalecer las capacidades y la funcionalidad de las entidades en términos de ciberseguridad y resiliencia corporativa se imparten las siguientes directrices:

3.1. Dar cumplimiento a las directrices en materia de seguridad digital y de la información que expida el MinTIC y las que se expidan en el marco de la política nacional de confianza y seguridad digital del Gobierno nacional.

3.2. Además de las directrices indicadas en el numeral anterior, fortalecer las medidas en materia de seguridad digital considerando las dinámicas que ha incorporado el uso de medios digitales, tales como:

3.2.1. Definir políticas fuertes frente a la infraestructura usada por los colaboradores y funcionarios, en las cuales se determine que el desarrollo de las actividades laborales debe realizarse desde equipos corporativos o equipos que cumplan con los controles de seguridad mínimos. Estos equipos o cualquier dispositivo que se utilice en actividades laborales, deben surtir un proceso de alistamiento y aseguramiento estricto realizado por las áreas de Tecnologías de Información y las Comunicaciones, Seguridad de la Información y/o oficiales de seguridad.

3.2.2. Evitar la instalación de programas o extensiones de navegadores de fuentes desconocidas ya que estas pueden traer malware (software malintencionado) que puede afectar la integridad de los dispositivos y exponer la información sensible no solo propia, sino de las redes a las que se conecta n.

3.2.3. No exponer información personal o sujeta a reserva en enlaces de internet públicos cuyo acceso se genera sin autenticación. En caso de que el enlace (link) sea generado por un código de respuesta rápida (QR), este no debe tener identificadores que permitan fácilmente acceder a otros registros. Para tal fin se deben usar funciones de cálculo hash y otras formas de anonimización de datos.

3.2.4. Cuando se usen aplicaciones de mensajería instantánea estas deben garantizar el uso de encriptación extremo a extremo (end-to-end) y que tenga una política de privacidad y tratamiento de datos aceptable.

3.2.5. Todos los sitios web que procesen información deben contar con capa de conexión segura (Secure Sockets Layer - SSL). Así mismo, ninguna contraseña debe ser almacenada en texto plano y se debe implementar un proceso de cambio de contraseñas periódico.

3.3. Garantizar la preparación y continuidad de sus funciones al momento de evaluar los riesgos de seguridad digital, con el fin de reducir los efectos adversos de los incidentes de seguridad.

3.4. Si la entidad debe habilitar un servicio en línea, primero deberá construir la matriz de riesgos que permita identificar las brechas de seguridad que se generan a nivel de ciberseguridad, seguridad de la información e imagen institucional, antes de realizar la actividad, y procurando que las acciones de contingencia no afecten la seguridad de los datos.

3.5. Las entidades destinatarias de la presente Directiva, dentro de los seis (6) meses siguientes a su expedición, deberán adoptar un plan de implementación articulado a los lineamientos del Modelo de Seguridad y Privacidad de la Información, en el que se contemple la actualización de los controles de seguridad de la información definidos por la entidad, así mismo, se deben realizar las actualizaciones pertinentes en el Plan Estratégico de Tecnologías de la Información - PETI.

4. GESTIÓN DE DATOS

4.1. Cuando las Entidades requieran la adquisición de imágenes del territorio, ya sea de plataformas satelitales o aerotransportadas, deberán establecer los canales de coordinación necesarios con las diferentes entidades que puedan verse involucradas, con el propósito de optimizar los recursos y aportar a la transferencia de conocimiento en el marco de la Infraestructura Colombiana de Datos Espaciales - ICDE.

4.2. La publicación e intercambio de los nuevos conjuntos de datos para uso abierto, deberán estar acompañados de los metadatos técnicos y metadatos de gestión. El primero se refiere a la estructura y formato del conjunto, tales como modelo de datos, procedencia, temática y permisos de acceso. El segundo contiene los términos para uso e interpretación de áreas funcionales, tales como definiciones de variables, reglas de calidad de datos y reglas para compartir. Para dar cumplimiento a la presente directriz, el Ministerio de Tecnologías de la información y las Comunicaciones actualizará la Guía Nacional de Datos Abiertos.

4.3 Los conjuntos de datos deben estar acompañados de documentos de apoyo para su adecuada interpretación, uso y aprovechamiento, tales como diccionarios de datos, manuales de metadata o catálogos de campos.

4.4 Para los formularios y aplicaciones de captura de datos se deberán implementar reglas de validación que permitan verificaciones automáticas al ingresar la información.

4.5. Incluir, dentro de la información esencial o básica de los proyectos, los datos geográficos, cuando aplique, cumpliendo con los lineamientos de la Infraestructura Colombiana de Datos Espaciales - ICDE.

4.6. Implementar la adecuada gestión de riesgos y la calidad de los datos, priorizando la disponibilidad de la información de forma estructurada, de manera que se puedan identificar los atributos, características, registros, conceptos y dominios de datos. Igualmente, se debe evaluar la necesidad de adelantar proyectos de depuración y actualización de datos, así como el fortalecimiento de controles y mecanismos de aseguramiento de su calidad en los sistemas de información.

5. ENTIDADES DEL ORDEN TERRITORIAL Y DE LAS RAMAS LEGISLATIVA Y JUDICIAL

De acuerdo con las disposiciones del parágrafo del artículo 2.2.9.1.1.2 del Decreto 1078 de 2015, “por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” se establece que “(...) La implementación de la Política de Gobierno Digital en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política (...)”, por lo cual, se invita a todas las entidades territoriales, así como a aquellas que pertenecen a las ramas Legislativa y Judicial, a que acojan las directrices objeto de la presente Directiva y dispongan las actividades pertinentes con sus mecanismos de planeación y ejecución, en el marco de sus competencias.

15 marzo de 2021.

IVÁN DUQUE MÁRQUEZ.

Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.
Normograma del Ministerio de Relaciones Exteriores
ISSN 2256-1633
Última actualización: 15 de enero de 2024 - (Diario Oficial No. 52.621 - 27 de diciembre de 2023)