DIRECTIVA PRESIDENCIAL 2 DE 2022

(febrero 24)

Diario Oficial No. 51.958 de 24 de febrero de 2022

PRESIDENCIA DE LA REPÚBLICA

Para:	Entidades Públicas de la Rama Ejecutiva del Orden Nacional.
De:	Presidente de la República.
Asunto:	Reiteración de la política pública en materia de seguridad digital.
Fecha:	24 febrero 2022

Las entidades que conforman la administración pública no han sido ajenas a la dinámica propia del incremento de los incidentes en el ámbito cibernético, con el riesgo de producir impactos negativos a partir de la materialización de incidentes de seguridad en el entorno digital. Por ello, la Seguridad Digital es, sin duda alguna, uno de los retos más importantes que enfrentan todo tipo de organizaciones.

De conformidad con lo establecido en los artículos 147 y 148 de la Ley 1955 de 2019, el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones y en especial, para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic), se imparten las siguientes directrices:

1. Contratar los servicios de nube que se encuentren contemplados en los acuerdo marco de precios vigentes, u otros mecanismos que para el efecto hayan sido establecidos por Colombia Compra Eficiente y en ausencia de estos, aplicando la modalidad de contratación contenida en el Estatuto de Contratación Pública, con el propósito de optimizar el uso de recursos públicos y obtener beneficios en términos de estandarización de alcances técnicos mínimos exigibles, escalabilidad, seguridad de la infraestructura, protección de los datos, actualización de las plataformas, redundancia, flexibilidad, oportunidad y disponibilidad, que le brinden a las entidades la capacidad de resiliencia corporativa oportuna ante un fenómeno de afectación.

2. Mantener actualizados los catálogos de sistemas de información, servicios, bases de datos, activos de información, infraestructura, flujos de información y artefactos (matrices, vistas, entre otros) que indiquen la relación de los Sistemas de Información con procesos y macroprocesos, servicios, información, entre otros; con el propósito de facilitar la identificación de activos críticos en la operación de las entidades.

3. Implementar una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital, de conformidad con el Modelo de Seguridad y Privacidad de la Información (MSPI) dispuesto por el Ministerio de Tecnologías de la información y las Comunicaciones (Mintic), haciendo énfasis en la identificación y gestión adecuada y efectiva de riesgos de seguridad digital. De la misma forma, se debe tener en cuenta la articulación con el Marco de Arquitectura Empresarial, en particular del dominio de arquitectura de seguridad donde se establecen lineamientos para aspectos de seguridad por defecto y desde el diseño de los nuevos sistemas de información.

4. Exigir y verificar que los proveedores de servicios en la nube contratados, cumplan de manera efectiva con los requerimientos mínimos en materia de ciberseguridad y se articulen a la estrategia de seguridad digital de la entidad.

5. Adoptar la seguridad digital con un enfoque preventivo y proactivo basado en la gestión efectiva de riesgos en el entorno digital, priorizando la protección de datos personales e información sensible de la entidad o que goza de reserva legal, al igual que de los servicios y sistemas de información e infraestructuras críticas.

6. Las entidades de acuerdo a, su tamaño, despliegue de infraestructura tecnológica, superficie de exposición en internet y los servicios y sistemas esenciales críticos que gestionen, deben conformar un Equipo o Grupo de Seguridad Digital, encargado de verificar la correcta aplicación de las políticas y estrategias vigentes en su organización, manteniendo una postura de seguridad enfocada al cumplimiento de la misionalidad y funciones asignadas.

7. Disponer de un procedimiento de gestión de incidentes de seguridad digital, para realizar su tratamiento, investigación y gestión, priorizando el reporte ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad) de Gobierno, de aquellos que son identificados y catalogados por la entidad como “Muy Grave” y “Grave”, con el propósito de contar con el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno y los protocolos requeridos para la recolección de evidencia digital.

8. Las entidades deberán realizar una evaluación del nivel de madurez en Seguridad de la Información a través del instrumento de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información. Para este fin, las entidades deberán atender de manera prioritaria los requerimientos que para el efecto expida el Mintic.

9. Disponer de un punto de contacto y un buzón de correo electrónico para facilitar el intercambio de información y la gestión de incidentes de seguridad digital, con el CSIRT Gobierno.

10. Ante incidentes de seguridad digital, que generen conductas punibles, tipificadas como tal por la legislación penal, se deberá priorizar la realización de la respectiva denuncia ante las autoridades competentes de realizar su investigación y en el marco de los procedimientos que para el efecto dispongan los órganos de policía judicial.

11. Garantizar la coordinación y el intercambio de información con las autoridades competentes para facilitar los procesos de investigación, así como los que se requieran para soportar la contención, erradicación y recuperación ante incidentes de seguridad digital.

12. Contar con planes de continuidad del negocio, orientados a generar el diagnóstico inicial, la contención, la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información. Igualmente, se deben realizar ejercicios que permitan probar la efectividad del plan de continuidad del negocio frente al escenario de materialización de riesgos de seguridad de la información.

13. Generar y probar políticas y procedimientos de copias de seguridad de la información (backup) que mitiguen el riesgo de pérdidas de información, haciendo énfasis en sistemas de información que soporten los procesos misionales y críticos, teniendo en cuenta que las copias de seguridad se realicen tanto de los datos como de las configuraciones y se mantengan fuera de línea y soporten adecuadamente los planes de continuidad asociados a la operación de la entidad.

14. Realizar un monitoreo permanente a la infraestructura de los servicios utilizados, incluyendo a los que usen los teletrabajadores o trabajadores en casa, con el fin de analizar posibles acciones no autorizadas.

15. Evaluar y actualizar de manera periódica los riesgos y controles necesarios en la relación con proveedores de tecnologías de la información.

16. Las redes inalámbricas (WiFi) de servicio en las entidades, deben ser redes para acceso y consulta de internet y no para que por medio de estas se administren infraestructuras internas o se acceda a servicios misionales internos desde dispositivos no corporativos.

17. Mantener actualizados los sistemas operativos, navegadores, manejador de contenidos, librerías y, en general, todo el software, con las respectivas actualizaciones de seguridad liberadas por los fabricantes.

18. Implementar protocolos y políticas de acceso remoto que eviten a los usuarios escalar privilegios y mitigue el riesgo de acceso no autorizado a recursos o información.

19. Adelantar campañas de sensibilización y capacitación a todos los funcionarios de la entidad, en seguridad digital y sus implicaciones, y desarrollar procesos de formación especializada para las áreas a cargo de la seguridad digital.

Se reitera que en desarrollo de la Política de Gobierno Digital y su Manual de Implementación, es responsabilidad de los representantes legales de las entidades públicas del orden nacional, coordinar, hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital, así como garantizar el desarrollo integral de la política al interior de sus entidades, entendiendo que esta es un eje transversal y apalancador de su gestión interna, que apoya el desarrollo de las políticas de gestión y desempeño institucional.

Adicional a lo anterior, se reiteran las directrices emitidas en la Directiva Presidencial número 03 del 15 de marzo de 2021, respecto a lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

Por otra parte, y conforme a las disposiciones de los artículos 113 y 209 de la Constitución Política, se invita a todas las entidades territoriales, así como a aquellas que pertenecen a las Ramas Legislativa y Judicial, y a los órganos autónomos, a que acojan las directrices de la presente Directiva y dispongan las actividades pertinentes con sus mecanismos de planeación y ejecución, en el marco de sus competencias.

24 de febrero de 2022.

IVÁN DUQUE MÁRQUEZ

Disposiciones analizadas por Avance Jurídico Casa Editorial Ltda.
Compilación Juridica MINTIC
n.d.
Última actualización: 30 de abril de 2024 - (Diario Oficial No. 52.728 - 15 de abril de 2024)

MINTIC