República de Colombia

Libertad y Orden

DEPARTAMENTO ADMINISTRATIVO
PRESIDENCIA DE LA REPÚBLICA

CIRCULAR No. 01

PARA: ENTIDADES DE LA RAMA EJECUTIVA DEL ORDEN NACIONAL.

DE: DIRECTOR DEL DEPARTAMENTO ADMINISTRATIVO DE LA PRESIDENCIA DE LA REPÚBLICA Y CONSEJERO PRESIDENCIAL PARA LA TRANSFORMACIÓN DIGITAL Y GESTIÓN Y CUMPLIMIENTO.

ASUNTO: RECOMENDACIONES DE USO DE SERVICIOS EN LA NUBE COMO MEDIDA PARA MITIGAR RIESGOS DE SEGURIDAD DIGITAL.

FECHA: 17 DE FEBRERO DE 2022

Con el propósito de dar cumplimiento al Decreto 1784 de 2019, modificado por el Decreto 1185 de 2021, en especial a lo contenido en el artículo 26 y artículo 33A y teniendo en cuenta que según cifras del Centro Cibernético Policial en lo transcurrido del año 2021 se presentaron un total de 49.457 denuncias por los delitos contemplados en la Ley 1273 de 2009, a continuación se presentan recomendaciones que buscan fortalecer la política de Gobierno Digital, en protección de datos y la seguridad digital de las entidades, a partir del uso de servicios en nube

En atención a lo dispuesto en el 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", así como en la Directiva Presidencial No. 3 del 15 de marzo de 2021, se han emitido disposiciones y lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos, con los cuales el Gobierno Nacional ha promovido la optimización de la gestión de recursos públicos, el uso de tecnologías emergentes tales como los servicios en la nube, así como la aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital, para generar confianza en los procesos de las entidades públicas y garantizar la protección de datos personales.

Conforme a lo aquí señalado el Gobierno Nacional ha priorizado el uso de servicios de nube en las entidades de la Rama Ejecutiva del Orden Nacional, lo cual resulta relevante no solo para optimizar los recursos públicos en proyectos de tecnologías de la información, sino para aprovechar sus beneficios, entre ellos, los de obtener mayor escalabilidad, seguridad de la infraestructura, protección de los datos, actualización de las plataformas, redundancia, flexibilidad, oportunidad y disponibilidad.

Respecto a los incidentes asociados a eventos de ciberseguridad, se ha encontrado que han afectando de manera particular infraestructura en entornos "on-premise", es decir, infraestructura (hardware y software) adquirida y dispuesta en instalaciones físicas de las entidades, lo que implica que aspectos como la configuración y actualizaciones (incluidas las optimizaciones y correcciones de seguridad), sean responsabilidad de sus equipos técnicos, a diferencia de los entornos en nube, en los cuales, el proveedor y la entidad compradora actúan bajo un esquema de responsabilidad compartida sobre la seguridad de los servicios.

Bajo las condiciones vigentes en el acuerdo marco de precio de Nube Pública IV, instrumento de agregación de demanda habilitado para que las entidades puedan habilitar entornos informáticos soportados en la Nube, es el Cloud Service Proveedor - CSP de cada proveedor de nube habilitado, el responsable de la infraestructura global de servicios de nube pública, la infraestructura de red, de procesamiento, de almacenamiento, la capa de virtualización de los servicios y la seguridad física de los centros de datos. Igualmente, es el proveedor, como distribuidor de los servicios del CSP, el que debe garantizar contar con elementos de seguridad

MAP

nativos ante ataques de denegación de servicio (DoS) y ataques de denegación de servicio distribuido (DDoS), así como garantizar la seguridad de los datos en reposo y tránsito, así mismo el proveedor debe garantizar que el CSP disponga de herramientas especializadas, las cuales pueden ser adquiridas por las entidades para reforzar sus esquemas de seguridad y de igual manera, es su responsabilidad garantizar la seguridad ante vulnerabilidades al hardware sobre su infraestructura, garantizar la segmentación de clientes y la instalación de parches de seguridad, aspectos de suma importancia para reducir riesgos para los servicios informáticos prestados por las entidades.

Por todo lo expuesto, se reitera a las entidades destinatarias de esta Circular, la necesidad de evaluar y priorizar el aprovisionamiento de capacidades informáticas haciendo uso de entornos en la nube, atendiendo las recomendaciones y guías que para el efecto disponga el Ministerio de Tecnologías de la Información y las Comunicaciones, en particular, las que conforman el Modelo de Seguridad y Privacidad de la Información, buscando proteger la infraestructura, la continuidad de los servicios, la protección de los datos de la entidad y de las personas.

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, a que acojan la recomendación objeto de la presente Circular y dispongan las actividades pertinentes con sus mecanismos de planeación y ejecución, en el marco de sus competencias.

VÍCTOR MANUEL MUÑOZ RODRÍGUEZ
Director
Presidencia de la República

MARÍA LUCÍA VILLALBA GÓMEZ
Consejera Presidencial para la
Transformación Digital, Gestión y
Cumplimiento