Uso de la Nube en la Administración Pública

Fecha de creación

07/09/2022

Tipo de publicación

Reglamentos

Resumen

Este documento establece los requisitos, regulaciones y uso de servicios de Nube en el Estado.

Por consultas sobre el documento comunicarse con Agesic al correo soporte@agesic.gub.uy o con URCDP a través de infourcdp@datospersonales.gub.uy.

Si se trata de una entidad de la Administración Central que desea plantear una excepción a lo previsto en el Decreto N° 92/014, comunicarse a contacto@agesic.gub.uy.

¿Qué es la Nube?

La computación en la nube, también llamada Cloud Computing, es un modelo virtual de prestación de servicios de negocio y tecnología a través de Internet. Mediante ella, se pone a disposición un catálogo de servicios estandarizados y variados que permiten cumplir con las necesidades de diversos tipos de negocio de manera flexible.

¿Pueden las entidades públicas usar servicios de Nube?

La respuesta es sí. No existen prohibiciones para el uso de servicios de nube por parte de las entidades públicas; la diferencia se encuentra en los requisitos que deben cumplir según se trate de entidades de la Administración Central (entendiendo como tal al inciso de Presidencia de la República, Ministerios y sus entidades dependientes); o no, cuando esos servicios de nube se prestan fuera del territorio nacional. Siempre que se gestionen datos personales, se deberá respetar la normativa específica existente.

Requisitos de uso de la Nube para las entidades públicas

Existen dos análisis previos: uno obligatorio y de riesgos de seguridad de la información para las entidades de la Administración Central que pretendan usar servicios de nube; y otro en materia de protección de datos personales y para todo tipo de entidades públicas, que depende exclusivamente del destino de los datos personales que se transmitan a través de esos servicios.

Análisis de riesgos

Para las entidades de la Administración Central, el artículo 3° del Decreto N° 92/014, de 7 de abril de 2014, establece que: “Los sistemas informáticos … de la Administración Central deberán estar alojados en centros de datos seguros situados en territorio nacional, exceptuándose aquéllos que no constituyan un riesgo para el organismo, de acuerdo con los "Lineamientos para la implementación y uso de centros de datos seguros (…)”

Por ende, para estas entidades es necesario “realizar un análisis de riesgos de la información” en forma previa a la utilización de los servicios prestados.

La normativa establece que aún en los casos en que se determine la existencia de un riesgo para el organismo, puede solicitarse una excepción ante Agesic, de acuerdo con el artículo 5° del Decreto N° 92/014.

En el caso de entidades que estén fuera de la Administración Central, salvo que tengan normas especiales que impongan otros requisitos, el uso de los servicios de nube no requerirá el análisis de riesgos indicado, aunque es importante su realización.

Se recomienda el empleo del Marco de Ciberseguridad para la detección y análisis de riesgos. Resulta una herramienta de gran relevancia para el análisis de distintos riesgos inherentes a la ciberseguridad.

Protección de datos personales

Cuando el uso de servicios de nube involucre datos personales, debe tenerse en cuenta el Dictamen Nº 8/014, del 23 de julio de 2014 de la Unidad Reguladora y de Control de Datos Personales (URCDP), que señala que ese uso puede implicar una transferencia internacional de datos si el servicio o los respaldos se encuentran ubicados fuera del territorio nacional.

En este punto es importante distinguir la ubicación de los países, es decir, si se trata de países adecuados o no adecuados.

Territorio adecuado

En este caso no se requieren autorizaciones especiales por parte de la URCDP, aunque sí el cumplimiento de algunos requisitos formales como la inscripción de la base de datos, entre otros.

Territorio no adecuado

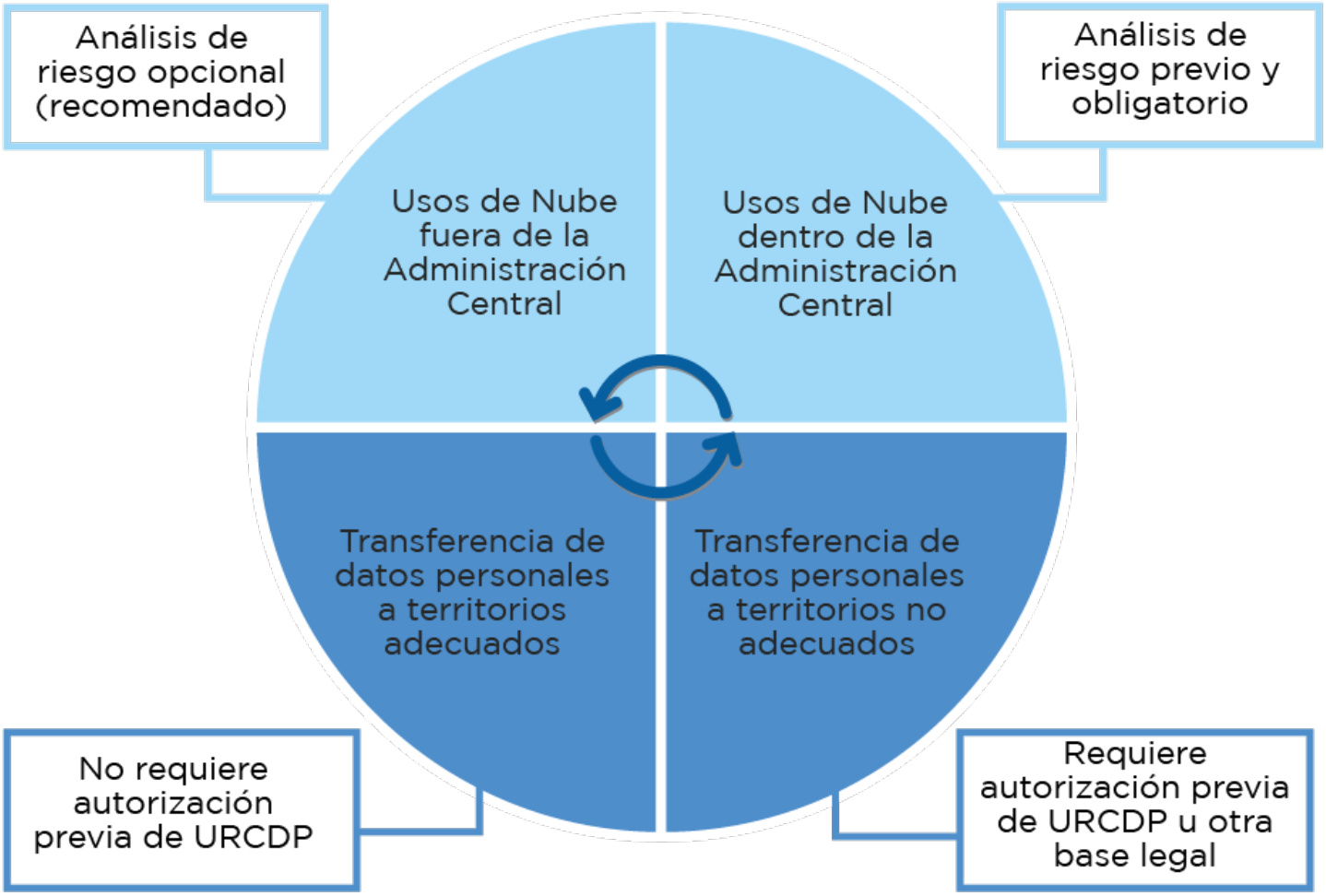
En caso de que la transferencia se realice a un territorio no adecuado, se deberá acreditar ante la URCDP que se cuenta con consentimiento de los titulares de los datos, o con cláusulas contractuales que aseguren la protección de los datos, u otras hipótesis previstas en el artículo 23 de la Ley N° 18.331, del 11 de agosto de 2008.

Adicionalmente, deberá realizarse una evaluación de impacto en la protección de datos, conforme el artículo 6° literal f del Decreto N° 64/020, del 17 de febrero de 2020, para lo que puede emplearse la Guía puesta a disposición por la URCDP. Esta consideración aplica a todas las entidades públicas.

El listado de los países adecuados puede consultarse en la resolución de la URCDP N° 23/021, del 8 de junio de 2021.

Adicionalmente, en cuanto a los datos personales que se almacenan en un servicio de nube, la URCDP recomienda como buena práctica la utilización de la Norma técnica ISO/IEC 27.018, que establece para los proveedores de servicios de nube un conjunto de “requerimientos mínimos a fin de facilitar el cumplimiento de la normativa de protección de datos por los responsables que se constituyen en sus clientes”, sin embargo, esta última es más exigente que la norma técnica referida.

Para determinar si los proveedores de servicios de nube que se contraten cumplen con los requisitos exigidos en materia de seguridad y protección de datos, es necesario hacer un análisis de los términos contractuales propuestos.



Compras públicas

En materia de contratación de servicios de nube, es importante recalcar que la misma deberá realizarse por parte de las entidades públicas, de conformidad con los procesos definidos en el TOCAF y normas concordantes. En el sitio web de la Agencia Reguladora de Compras Estatales (ARCE) se detallan los procedimientos aplicables según la normativa vigente.

¿Quiénes deben realizar los análisis indicados?

Los análisis de riesgos, tanto en materia de ciberseguridad como de protección de datos personales, corresponde que sean realizados a la interna de la organización, por los equipos de TI, Seguridad, Legal, y en caso de existir, por quien desempeña el rol de delegado de protección de datos, regulado por la Resolución N°32/020. Existen múltiples herramientas y marcos disponibles para la realización de éstos análisis, algunos de los cuales pueden encontrarse en el sitio web de Agesic y de URCDP.

En lo que respecta a las consideraciones en materia de compras, es necesario que la evaluación del procedimiento más acorde al objeto de la compra sea realizada por el área de Administración y Finanzas de la entidad.

¿A qué entidades consultar sobre el uso de los servicios de Nube?

El Decreto N° 184/015, del 14 de julio de 2015, indica que Agesic debe crear las condiciones para definir una política nacional concertada para el desarrollo del gobierno electrónico. Asimismo, hay distintas leyes y decretos que le asignan competencias en materia de desarrollo de políticas y buenas prácticas en materia de seguridad de la información, gestión de trámites y servicios en línea, y en particular, la intervención en planes de gobierno electrónico. Posee además potestades en materia de fiscalización en seguridad de la información, pudiendo apercibir a las entidades que incumplan con los estándares definidos en el área de su competencia.

En particular, en lo que refiere al uso de la nube por parte de entidades de la Administración Central, conforme el Decreto N° 92/014, Agesic tiene participación en los planes de acción diseñados por estas para el cumplimiento de las disposiciones del decreto, así como el cometido de fiscalizar el cumplimiento de sus normas y contemplar excepciones debidamente fundadas.

En lo que respecta a datos personales, la entidad rectora es la URCDP, quien tiene competencias para definir los territorios adecuados para las transferencias internacionales de datos, establecer los mecanismos para dar seguridad a dichas transferencias, y autorizar aquellas que se realicen a territorios no adecuados según la normativa vigente (Ley N° 18.331, de 11 de agosto de 2008).

En lo que hace relación con asesoramiento en compras y contrataciones a entidades estatales dependientes del Poder Ejecutivo, la competencia se encuentra asignada a la ARCE (artículo 331 de la Ley N° 19.889, del 9 de julio de 2020).