PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno Digital

Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano

Documento preparado por la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros - **SeGDi – PCM**.

Fecha: 4 de enero de 2018.

Lima - Perú

CONTENIDO

1. Prólogo

El empleo de las Tecnologías de la Información y la Comunicación (TIC), en todos los ámbitos de la sociedad, ha supuesto la posibilidad de habilitar más y mejores servicios a todas las personas en general; en particular, desde la perspectiva de los Estados representa la posibilidad de mejorar la eficiencia de las entidades de la Administración Pública y la eficacia en los servicios públicos que prestan a los integrantes de la sociedad, todo ello logrando un uso eficiente de los recursos públicos.

En el Perú la Ley Nº 27658 - Ley Marco de Modernización de la Gestión del Estado, declaró al Estado Peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y contribuir en el fortalecimiento de un Estado moderno, descentralizado y con mayor participación del ciudadano; por lo que deviene en necesario mejorar la gestión pública a través del uso de dichas tecnologías que permitan brindar mejores servicios a los ciudadanos.

Conviene señalar que el Decreto Legislativo N° 604 crea el Sistema Nacional de Informática que tiene por finalidad asegurar que las actividades en torno al empleo de las TIC, en el ámbito de la Administración Pública, se desarrollen en forma integrada, coordinada, racionalizada y bajo una normatividad técnica común, contando con autonomía técnica y de gestión. Además, tiene como ámbito de competencia *"La instrumentalización jurídica y de mecanismos técnicos para el ordenamiento de los recursos de cómputo y de la actividad informática del estado, así como toda la documentación asociada; la operación y explotación de los bancos de datos y archivos magnéticos de información al servicio de la gestión pública. Corresponde a este desarrollo la planeación sistemática de procesos, métodos y técnicas apoyadas en ciencia y técnica aplicada, que se establecen con el fin de usar, procesar y transportar información"*[1].

Actualmente, mediante el Decreto Supremo Nº 022-2017-PCM se aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros – PCM, el cual a través del Capítulo VI Subcapítulo I establece las funciones de la Secretaría de Gobierno Digital – SeGDi, disponiendo a través de su artículo 47 que dicha Secretaría es "[…] *el órgano de línea, con autoridad técnico normativa a nivel nacional, responsable de formular y proponer políticas nacionales y sectoriales, planes nacionales, normas, lineamientos y estrategias en materia de informática y de Gobierno Electrónico. Asimismo, es el órgano rector del Sistema Nacional de Informática* […]".

En tal contexto, se considera que las entidades de la Administración Pública integrantes del indicado Sistema Nacional de Informática encuentran diferentes desafíos, en gran parte debido al desarrollo y evolución constante de las TIC, entre otros, el empleo de servicios en la nube.

En efecto, el uso de servicios en la nube ofrece una gran cantidad de beneficios potenciales a las entidades públicas, como la escalabilidad, elasticidad, alto rendimiento, resistencia y la seguridad, además de la rentabilidad de costes.

[1] Artículo 3 del Decreto Legislativo N° 604.

Comprender y gestionar los riesgos relacionados con la adopción e integración de los servicios en la nube en las entidades de la Administración Pública supone un reto clave. La gestión eficaz de los aspectos antes mencionados en relación con la provisión de dicho tipo de servicios en la nube está llevando a muchas entidades de la Administración Pública a innovar y, en ciertos casos, a replantearse sus procesos de evaluación del riesgo y de toma de decisiones fundadas respecto a este nuevo modelo de provisión de servicios.

Conviene mencionar que las amenazas a la seguridad no deben ser excusa para no innovar o migrar a los servicios en la nube, por el contrario con ello se incrementa las prácticas de control de seguridad bajo las nuevas tecnologías, por lo tanto mejorarán y actualizarán las políticas de regulación.

La Secretaría de Gobierno Digital considera que para impulsar la transformación digital en el Estado peruano las entidades de la Administración Pública cumplen un rol importante en el desarrollo de sus proyectos, para lo cual ya están en condiciones de definir su estrategia para el uso de servicios en la nube, por lo que estimamos que el presente "*Lineamiento para el Uso de Servicios en la Nube para Entidades de la Administración Pública del Estado Peruano*" propiciará no sólo acelerar su transformación y, por ende, la digitalización de los servicios públicos que son prestados por parte de dichas entidades de la Administración Pública, sino que facilitará que puedan innovar en la prestación de los mismos, permitiéndoles influir en la mejora de la calidad de vida de nuestros ciudadanos y personas en general, lo cual es reconocido por los gobiernos de la *Organización para la Cooperación y el Desarrollo Económico* (**OCDE**)[2]; en tal sentido, estimamos que el presente lineamiento es una acción que coadyuvará, a su vez, en el objetivo que tiene nuestro país de ser parte de dicha organización.

Finalmente, ésta Secretaría de Gobierno Digital quiere manifestar su agradecimiento a las entidades de la Administración Pública que han emitido su opinión sobre el presente documento, como el Ministerio de Justicia y Derechos Humanos MINJUS, a través de la Dirección General de Protección de Datos Personales y el Organismo Supervisor de las Contrataciones del Estado – OSCE, a través de su Dirección Técnica Normativa y, del mismo modo, a los representantes del Consejo Consultivo Nacional de Informática – CCONI, y a los integrantes del Comité de Coordinación Interinstitucional de Informática – CCOII, así como a todos aquellos que nos hicieron llegar sus comentarios, sugerencias y aportes.

Lima, 4 de enero de 2018.

FIRMA DIGITAL PCM PRESIDENCIA DEL CONSEJO DE MINISTROS

Firmado digitalmente por SCHOL CALLE Lieneke Maria (FAU20168999926)
Motivo: Soy el autor del documento
Fecha: 04.01.2018 12:47:29 -05:00

Secretaría de Gobierno Digital – SeGDi.
Presidencia del Consejo de Ministros – PCM.
Perú.

[2] ***Declaración de Daejeon de 2015 sobre ciencia, tecnología y políticas de innovación para la era global y digital***, la cual puede ser consultada en: https://goo.gl/Q4Nw2Y.

2. Principios generales para el uso de servicios en la nube para entidades de la Administración Pública en el Estado Peruano.

Los presentes lineamientos se interpretan según los siguientes principios:

- **Impulsar la transformación digital del país**. Para que el Perú pueda aprovechar los beneficios que trae la transformación digital debe estar en la posibilidad de acceder a las mejores tecnologías y herramientas para el procesamiento de información que se ofrece a nivel mundial, pues de lo contrario quedará rezagado. En efecto, si las entidades de la Administración Pública no pueden acceder a recursos tecnológicos que permitan que los servicios que prestan a los ciudadanos y a las empresas en nuestro país sean más eficientes, nuestro país pierde la oportunidad de ser más competitivo. Igualmente, esto puede significar una limitación para el acceso a servicios a los ciudadanos peruanos.
- **Facilitar un mejor acceso de servicios a las personas**. En el Perú las personas deben poder acceder a recursos tecnológicos de primer nivel que permitan facilitar el acceso a servicios que pueden ser provistos haciendo uso para ello de una amplia infraestructura. Por lo tanto, las provisiones que no permitan el libre flujo de datos impiden que nuestro país mejore la prestación de dicho servicios, así como los beneficios que ello conllevaría, como el análisis de grandes volúmenes de información a altas velocidades o la automatización de los procesos.
- **Respetar las jurisdicciones de otros países**. Muchos proveedores de servicios en la nube se encuentran en el extranjero, por lo tanto, debido a razones de libertad de contratación y aplicación territorial de las normas, estos no pueden estar obligados a cumplir con normas específicas de determinados países. En dicho sentido, existen tratados de libre comercio (como el TLC entre Estados Unidos y el Perú) donde se ha estipulado que el Perú no puede establecer tratamientos discriminatorios a la inversión extranjera sobre las condiciones de operación de su negocio.
- **El presente lineamiento contiene recomendaciones generales y sugerencias**. La contratación de servicios en la nube por parte de las entidades de la Administración Pública del Estado Peruano es una opción, por lo que el presente documento es orientador y, por ende, no impone obligaciones, dejando a salvo lo previsto por los respectivos marcos regulatorios nacionales que resulten aplicables en cada caso.

3. Introducción.

3.1. Conceptos previos.

En la actualidad el acceso a servicios a través de Internet se viene incrementado en la medida que las personas disponen de más dispositivos a su alcance, de los que pueden hacer uso. Este hecho, es decir, la variedad de los dispositivos que dan acceso a estos servicios, supone el auge en el uso de las tecnologías web como estándar. Así, la migración a entornos web es un catalizador para la externalización de los sistemas de información de un amplio número de organizaciones.

Como consecuencia de esta situación surge el modelo de servicios en la nube, como una propuesta tecnológica capaz de ofrecer servicios en red de forma ágil y flexible, donde dichos servicios consisten en la disposición de software, plataformas o infraestructuras por parte de un proveedor de servicios en la nube (PSN[3]), o por parte de la propia entidad, accesibles en red, con independencia de donde se encuentren alojados los sistemas de información y de forma transparente para el usuario final.

Ilustración 1: *Servicios en la Nube.*

Una de las definiciones de servicios en la nube con mayor aceptación es la propuesta por el Instituto Nacional de Normas y Tecnología del Departamento de Comercio de los Estados Unidos de América[4] [NIST SP-800-145]: "*La provisión de servicios en la nube es un modelo para permitir el acceso por red, de forma práctica y bajo demanda, a un conjunto de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio*"[5].

[3] Conocido en idioma inglés como *Cloud Service Provider* o por su respectivo acrónimo de CSP.
[4] Conocido en idioma inglés como *National Institute of Standards and Technology* o por su respectivo acrónimo de NIST.
[5] SP 800-145, The NIST Definition of Cloud Computing (September 2011), Disponible en: https://goo.gl/uWJhJU.

El modelo de servicios en la nube ofrece a las organizaciones grandes beneficios como pueden ser la alta disponibilidad, el acceso a información desde cualquier lugar, la flexibilidad en asignación de recursos y un posible ahorro económico significativo.

Existen diversas modalidades de servicios en la nube, tanto en lo referente al modelo de despliegue (privada, pública, híbrida o comunitaria) como en las categorías de servicio que se ofrecen **Infraestructura como servicio** (*Infrastructure-as-a-Service* - IaaS), **Plataforma como servicio** (*Platform-as-a-Service* (PaaS), **Software como servicio** (*Software-as-a-Service* - SaaS).

El presente lineamiento ha tenido en consideración los marcos legislativos aplicables y recoge los aspectos técnicos mínimos necesarios que las entidad de la Administración Pública del Estado Peruano tendrán en consideración para la adopción de servicios en la nube; asimismo, se han identificado las medidas de seguridad y los requisitos que deben cumplir los proveedores de servicios en la nube para dar cumplimiento a los indicados preceptos legislativos aplicables, así como para proveer dicho servicio con las garantías de seguridad pertinentes en base a buenas prácticas o estándares reconocidos internacionalmente.

Protocolo de Internet versión 6 (IPv6)

En agosto de 2017, la Presidencia del Consejo de Ministros, a través de la SeGDi, dispuso la formulación de un Plan de Transición al Protocolo IPV6[6], a implementarse de manera progresiva en toda la infraestructura tecnológica, software, hardware, servicios, entre otros, en las entidades de la Administración Pública. En consecuencia, las entidades de la Administración Pública deberán observarlo en sus procesos e incluirlo en los contratos con los proveedores de servicios en la nube, cuando corresponda.

3.2. Características de los servicios en la nube

La característica principal de los servicios en la nube es la accesibilidad de la información. Este modelo de servicio facilita el acceso, con independencia del lugar o el tipo de dispositivo que se emplee: basta tener acceso a la red, aunque el uso de estos servicios implica habitualmente la necesidad de disponer de conexiones con una capacidad significativa.

Otra de las características que hacen que el servicio de la nube se venga expandiendo de forma significativa es el ahorro económico. Generalmente el modelo de servicios en la nube permite reducir costes a las entidades y organizaciones con respecto al modelo de servicio y alojamiento tradicional. Esto debido al ahorro de recursos dedicados internamente a hardware, mantenimiento, personal dedicado, suministros, espacio e instalaciones, entre otros. Además, con el servicio en la nube, se permite a los usuarios del servicio pagar solo por los recursos que utiliza, ya sea facturando en función de parámetros como los ciclos de procesador consumidos, el ancho de banda o las máquinas virtuales dedicadas, permitiendo además añadir o eliminar recursos de forma sencilla y en tiempo real.

[6] Aprobado mediante el Decreto Supremo N° 081-2017-PCM, el cual puede ser consultado en: https://goo.gl/ZZVQ9j.

Por otro lado, los servicios en la nube se caracterizan por la deslocalización de datos, entendida ésta como una principal ventaja y donde el usuario o clientes de los proveedores de servicios en la nube puede llevar los datos y los procesos al lugar más conveniente para la entidad u organización, empero manteniendo el control de acceso independientemente de donde se encuentren los datos. De esta forma se pueden mantener copias del servidor repartidas en distintos puntos del planeta tanto para mejorar los tiempos de acceso como para evitar pérdidas de datos o servicios por la caída de un centro de procesamiento de datos; sin embargo, dicha deslocalización tiene implicancias de seguridad que las entidades u organizaciones deben evaluar convenientemente antes de optar por contratar servicios en la nube.

Por su parte, la guía [NIST SP-800-145][7] identifica cinco características esenciales:

- **Autoservicio a demanda**. El cliente puede ajustar la capacidad necesaria de forma unilateral, sin necesidad de involucrar al personal del proveedor.
- **Amplio acceso a través de redes**. Acceso estándar a través de redes, habilitando todo tipo de dispositivos de acceso: teléfonos inteligentes, tabletas, portátiles, equipos personales, servidores, entre otros.
- **Agregación y compartición de recursos**. Los recursos del proveedor se agregan y se ponen a disposición de múltiples clientes para su compartición. La agregación incluye equipos físicos y equipos virtuales que se asignan dinámicamente bajo demanda. El cliente se independiza de la ubicación física de los recursos, aunque puede delimitar ubicaciones a un cierto nivel de abstracción (país, estado, etc.).
- **Adaptación inmediata**. La capacidad requerida puede provisionarse rápida y elásticamente para seguir las variaciones de la demanda. Desde el punto de vista del consumidor, los recursos parecen ilimitados, pudiendo disponer de cualquier volumen en cualquier momento.
- **Servicio consumido**. El proveedor puede controlar el servicio prestado efectivo en cada momento, al nivel de abstracción que se especifique por contrato; por ejemplo, capacidad de almacenamiento, capacidad de procesamiento, ancho de banda, cuentas de usuario, etc. El uso de recursos puede ser monitorizado, controlado y reportado, proporcionando una gran transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

Adicionalmente, se puede considerar otras características como:

- **La innovación se acelera.** Al aprovechar los servicios y capacidades más recientes de los servicios en la nube, reduce las barreras para que las entidades de la Administración Pública innoven para la transformación digital y les permitan centrarse más en la innovación empresarial que en las tecnologías, lo que acelera el tiempo de valoración.

[7] SP 800-145, The NIST Definition of Cloud Computing, Op Cit., p6.

- **Ayuda para migrar a los servicios en la nube.** Comenzar a utilizar servicios en la nube a menudo implica traducir datos y sistemas informáticos a la tecnología que soporta la provisión de dichos servicios. Por lo tanto, es recomendable considerar los servicios de migración que pudieran ofrecer los PSN para llevar a cabo dicha migración a los servicios en la nube.
- **Aprovecha las grandes economías de escala.** Debido al uso de cientos de miles de clientes de servicios en la nube, los proveedores pueden conseguir grandes economías de escala que se traducen en precios de pago por uso inferiores y pueden ayudar a reducir costos de mano de obra de tecnologías de la información – TI y darle acceso a una plataforma altamente distribuida y muy compleja.
- **Aumentar la velocidad y agilidad.** El entorno del servicio informático en los servicios en la nube acelera el desarrollo y la implementación de las aplicaciones y permite a su equipo probar diferentes opciones más rápido; el resultado es un aumento de la agilidad de la organización.

Por último, cabe destacar la posible dependencia de terceros en la provisión de servicios en la nube. La tendencia mayoritaria apunta hacia externalizar los servicios en la nube a terceros delegando en ellos todas las tareas de mantenimiento, adquisición de sistemas, gestión de la capacidad, entre otros. Si bien esto es considerado generalmente como una ventaja, debe tenerse en cuenta que esta característica nunca debe conllevar una pérdida del control de la información, o una despreocupación por la seguridad, debido a que la responsabilidad final siempre recae en la entidad de la Administración Pública u organismo contratante. A la hora de contratar estos servicios es fundamental estudiar adecuadamente las condiciones del servicio y las medidas de seguridad aplicadas para confirmar que son adecuadas para los requisitos exigidos a la entidad o la organización cliente.

3.3. Modelos de despliegue

Ante las posibilidades para crear un entorno de servicios en la nube se han clasificado las infraestructuras en públicas, privadas, comunitarias o híbridas; las cuales explicamos a continuación:

- **Nube pública**: La infraestructura de esta nube está disponible para el público en general o para un gran grupo de industria y dicha infraestructura la controla un proveedor de servicios en la nube.
- **Nube privada**: La infraestructura de esta nube es operada únicamente por y para una organización.
- **Nube híbrida**: Es la composición de dos o más modelos, por ejemplo, privada y pública, que permanecen como entidades únicas pero que coexisten por tener tecnología que permite compartir datos o aplicaciones entre las mismas, o la combinación de servicios de nube y "*on premises*"[8] o servidores locales, en constante interacción entre ambas plataformas.

[8] La expresión en idioma inglés "*on premise*" puede traducirse como "aplicaciones locales".

- **Nube comunitaria**: La infraestructura de esta nube es compartida por varias organizaciones relacionadas entre ellas y que comparten requisitos de servicio. Uno de los miembros del colectivo controla los recursos.

3.4. Categorías de servicio

Se ofrecen una serie de categorías de servicio que se detallan a continuación:

- **Infraestructura como servicio** *(Infrastructure as a Service - IaaS)*. Se encarga de entregar una infraestructura al usuario, normalmente mediante una plataforma de virtualización. El proveedor de este servicio en la nube se encarga de la administración de la infraestructura y el cliente tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red virtualizados.
- **Plataforma como servicio** *(Platform as a Service - PaaS)*. El proveedor de este servicio en la nube se encarga de entregar una plataforma a la organización cliente. El cliente no administra ni controla la infraestructura, pero tiene el control sobre las aplicaciones instaladas y su configuración, y puede incluso instalar nuevas aplicaciones.
- **Software como servicio** *(Software as a Service - SaaS).* El proveedor de este servicio en la nube es el encargado de ofrecer al cliente el software como un servicio. Las aplicaciones son accesibles desde varios dispositivos cliente a través de una interfaz de cliente ligero, como por ejemplo un navegador web; el cliente no administra ni controla la infraestructura en que se basa el servicio que utiliza. Las suites ofimáticas a las que se puede acceder online son un buen ejemplo de este modelo.

Es recomendable que las entidades de la Administración Pública tengan en cuenta los requisitos basados en el rendimiento, el precio, la seguridad y garantía/auditoría de se brinda, así como los términos y condiciones necesarias, en su estrategia de adquisición de las indicadas categorías de servicios en la nube (*IaaS*, *PaaS* o *SaaS*).

4. Requisitos en materia de seguridad de la información

La contratación y adopción de servicios en la nube como estrategia para soportar los procesos y servicios públicos de las entidades de la Administración Pública introduce un amplio número de beneficios para que estas puedan innovar, reducir costos en sus procesos y brindar soluciones ágiles; sin embargo, y, aun con los beneficios indicados, emergen riesgos que requieren ser controlados y gestionados adecuadamente. Más aun, es condición necesaria que la contratación y adopción de servicios en la nube se enmarque dentro de los requisitos exigibles por los marcos legales existentes y en la adopción de guías de buenas prácticas de dichos marcos, como los relativos a seguridad de la información[9] y, en su caso, como veremos en el numeral correspondiente del presente lineamiento, los vinculados con la protección de datos personales[10].

[9] El Estado Peruano tiene en este ámbito tres instrumentos normativos importantes:
- R.M. N° 004-2016-PCM, de fecha 08ENE2016, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos. 2° Edición", en todas las entidades del Sistema Nacional de Informática. https://goo.gl/8X5w8w.
- R.M. N° 166-2017-PCM, de fecha 21JUN2017, que aprueba modificaciones al artículo 5 de la R.M. N° 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información. https://goo.gl/HGqJ25.
- Directiva de Seguridad, aprobada por la Autoridad Nacional de Protección de Datos Personales – APDP. https://goo.gl/e3pX2q

[10] https://goo.gl/e3pX2q.

Asimismo, en lo relacionado con el cumplimiento de requisitos de seguridad, el modo de afrontar dicho cumplimiento normativo difiere en función de que la infraestructura en la nube sea propiedad y esté administrada por un tercero o lo esté por la propia entidad pública. En el supuesto de que sea la entidad pública la propietaria y administrador de la infraestructura sobre la que se despliegan los servicios en la nube, la completa adecuación efectiva a la normativa vigente recae en dicho organismo, mientras que, en el caso de estar la infraestructura operada por un tercero, éste observará los requisitos establecidos en la normativa de seguridad que sea de aplicación. En cualquier caso, la responsabilidad del cumplimiento de dicho marco normativo o de cualesquiera otras normas de aplicación, así como del correcto tratamiento de los datos en términos generales desde el punto de vista de su seguridad, recaerá siempre sobre la entidad pública propietaria de la información, con independencia de la existencia de acuerdos, seguros u otras medidas compensatorias.

El presente lineamiento centra su contenido en identificar los requisitos mínimos a tener en consideración cuando las entidades de la Administración Pública del Estado Peruano opten por la contratación de un proveedor de servicios en la nube, ello para que la contratación de tales servicios esté alineada con el cumplimiento de la normatividad sobre la materia, así como la relacionada con la de seguridad de la información y, cuando corresponda, con la de protección de datos personales, de modo que se resguarde tanto la información como la prestación de los servicios públicos brindados por los diferentes entes y niveles del ámbito público.

Es importante recordar que la gestión de la seguridad de los servicios en la nube que se contraten en las entidades de la Administración Pública son una responsabilidad compartida entre la entidad contratante y el proveedor de servicios en la nube, donde la primera define los controles de seguridad, mientras que el proveedor de servicios en la nube es responsable de la seguridad de la nube.

El nivel de responsabilidad de ambas partes depende del tipo de modelo de despliegue en la nube, y las entidades de la Administración Pública deben ser claras en cuanto a sus responsabilidades en cada modelo.

Ilustración 2: *Responsabilidad compartida entre la entidad pública y el proveedor de servicios en la nube en el ámbito de Seguridad de la Información.*

Adicionalmente, vale la pena resaltar que, si no se garantiza la seguridad de los servicios, datos e información soportada por servicios en la nube, en última instancia, podría resultar en mayores costos, afectación de la imagen y pérdida de los beneficios esperados.

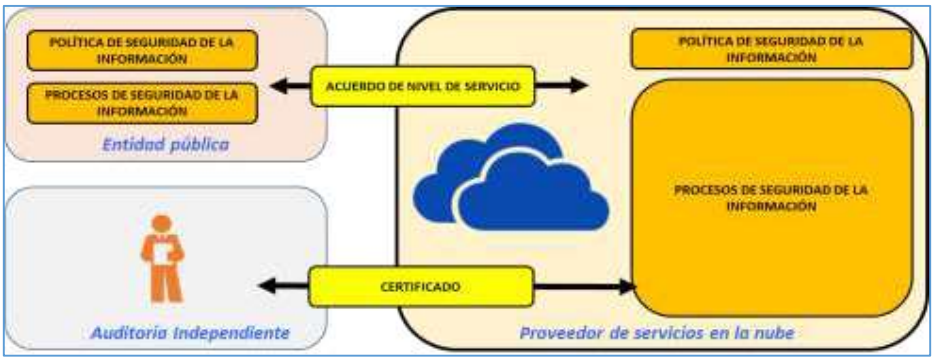

Ilustración 3: *Esquema marco de Seguridad de la Información de Proveedores en la Nube*

En línea con lo anterior, la entidad de la Administración Pública que contrate servicios en la nube habrá de considerar lo siguiente:

- Disponer de una política de seguridad de la información, controles de seguridad de la información, proceso de gestión de riesgos, en base a base lo indicado en la **R.M. N° 004-2016-PCM y sus modificatorias.**
- Observar la guía de buenas prácticas señaladas en la **Directiva de Seguridad en el ámbito de la protección de datos personales.**
- Disponer de un **Acuerdo de Nivel de Servicio - ANS** con el proveedor de servicios en la nube, en la que quede claramente definida las responsabilidades de la entidad pública y el proveedor de servicios en la nube.
- Requerir mínimamente al proveedor de servicios en la nube un certificado de seguridad de la información ampliamente reconocido y basado en estándares internacionales, el mismo que tiene que ser emitido **por una organización de auditoría independiente, como: *Federal Risk and Authorization Management Program* (FedRAMP), entre otros.**

ISO/IEC 27001	Seguridad de la información.
ISO/IEC 27017	Controles de seguridad de la información basada en ISO/IEC 27002 específicamente para los servicios en nube
ISO/IEC 27018	Requisitos para la protección de la información de identificación personal (PII) en sistemas cloud.

- Requerir al proveedor de servicios en la nube mínimamente, el manejo de los siguientes **protocolos de cifrado**, los cuales se basan en estándares y algoritmos aceptados y probados por la industria:

AES	(128 bits o superior)

TDES	(Teclas de doble longitud)
RSA	(1024 bits o superior)
ECC	(160 bits o superior)

- Para el caso del manejo de tarjetas de pago requerir al proveedor de servicios en la nube como mínimo el Estándar de Seguridad de los Datos de la Industria de las Tarjetas de Pago **(también conocido como PCI DSS).**

4.1. Roles y funciones

La responsabilidad sobre la seguridad de la información es propia de cada uno de los entes públicos y debe ser ejercida por los mismos, en cuanto establecen los controles de seguridad de acuerdo con la legislación y normativa vigente. A tal efecto, el área o responsable de la seguridad de cada entidad pública tendrá como interlocutor al área responsable de la seguridad del proveedor de servicios en la nube – PSN.

El área o responsable de la seguridad de la entidad pública deberá cerciorarse que puede garantizar la capacidad efectiva del PSN de resolver incidentes, en particular cuando dicho PSN recurre a equipos o servicios en diferentes jurisdicciones.

Nótese que la naturaleza de los activos que son responsabilidad del PSN puede variar fuertemente dependiendo del modelo de servicio, siendo mínima en el modelo IaaS y máxima en el modelo SaaS. Típicamente, un PSN tendrá personal, instalaciones e infraestructura. En IaaS su responsabilidad termina en la infraestructura virtualizada. En PaaS su responsabilidad se extiende a la plataforma provisionada. En SaaS su responsabilidad se extiende a la gestión de los servicios.

A menudo aparecen en el despliegue proveedores de comunicaciones (por ejemplo, proveedores de servicios de internet[11]). A estos se les considerará proveedores con igual responsabilidad sobre los medios que le son propios.

Puede que la infraestructura sea propia o esté subcontratada. Por ejemplo, proveedor SaaS usando IaaS de un tercero.

4.2. Clasificación

Las entidades públicas clasificarán sus sistemas según la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información". Esta labor la coordina el área o responsable de la seguridad conjuntamente con los responsables internos que defina cada entidad pública en relación con la Información que gestionan y los servicios que prestan.

Los requisitos o niveles de seguridad en términos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad se trasladarán a los elementos que los soporten, sean propios de la entidad pública, sean de un PSN contratado, o sean de una cadena de subcontratación entre PSNs.

[11] Conocido en idioma inglés como *Internet Service Providers* o por su respectivo acrónimo de ISP.

El traslado de los valores antes indicados pueden verse truncados si se emplean técnicas apropiadas tales como:

- Si la información se cifra, sólo se propaga el nivel de disponibilidad.
- Si el servicio es redundante (proveedor alternativo), no se traslada el nivel de disponibilidad.

Un escenario habitual es el de servicios de almacenamiento en la nube, sin tratamiento de datos en la nube. En este caso es recomendable que todos los datos se cifren antes de salir de la entidad pública, de forma que los requisitos de seguridad sobre los proveedores de servicios en la nube se reducen a la dimensión de disponibilidad. La entidad pública será la única en poder de las claves de cifra, a las que aplicará lo previsto en el control respectivo de la señalada NTP ISO/IEC 27001:2014 Tecnología de la Información.

4.3. Recomendaciones

De modo general se puede recomendar los siguientes puntos:

- Las claves de cifrado no se almacenen en texto claro en la nube, ni se utilizarán en aplicaciones que se ejecuten en la nube, dependiendo el servicio que se contrate.
- El proceso de autorización de usuarios (altas, bajas y gestión de derechos de acceso) no se realice en la nube.
- Las aplicaciones de firma electrónica y de sellos de tiempo no se ejecuten en PSNs, sino con los medios propios o de las terceras partes de confianza de conformidad con la legislación aplicable sobre la materia.

4.4. Los registros de la actividad de los usuarios se tratan de forma específica, preferentemente reteniéndolos en la propia entidad; es decir, que no estén hospedados en el PSN. **Medidas de protección**

A efectos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, el PSN queda obligado a cumplir y demostrar que, como mínimo, cumple con todas las medidas de seguridad de la NTP ISO/IEC 27001:2014 Tecnología de la Información, pertinentes para el nivel de disponibilidad requerido por las entidades de la Administración Pública. Esto incluye instalaciones y personal. Las citadas medidas de seguridad podrán ser reemplazadas por otras siempre y cuando se acredite con las certificaciones respectivas que protegen igual o mejor el riesgo sobre los activos y se satisfacen los principios básicos en materia de seguridad de la información.

4.5. Restricciones adicionales

Los elementos virtualizados y los elementos de virtualización se tratarán igual que los elementos físicos correspondientes a efectos de configuración, mantenimiento, reglas de seguridad y aspectos regulatorios.

Las imágenes de los elementos virtuales se tratarán como datos con los mismos requisitos de seguridad que la información y los servicios manejados por dichos elementos virtuales.

Son aspectos básicos importantes sobre la propiedad y gestión de datos en un modelo de responsabilidad compartida de la nube, que:

i) Las entidades de la Administración Pública sean propietarias de los datos,
ii) Las entidades de la Administración Pública puedan, de estimarlo pertinente, elegir la localización geográfica para almacenar sus datos, y no se mueven a menos que las propias entidades decidan moverlos.
iii) Las entidades de la Administración Pública puedan descargar o eliminar sus datos cuando lo deseen; y,
iv) Las entidades de la Administración Pública deben considerar la sensibilidad de sus datos y decidir si lo hacen y cómo cifrarán los datos mientras están en tránsito o en reposo.

5. Requisitos en materia de protección de datos de carácter personal.

En la medida que en la prestación de servicio en la nube se alberguen datos personales se seguirá lo establecido por la legislación nacional sobre dicha materia: la Ley N° 29733 – Ley de Protección de Datos Personales, su Reglamento aprobado mediante el Decreto Supremo Nº 003-2013-JUS, , así como el Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, y modifica la indicada Ley N° 29733; pudiendo adoptarse además buenas prácticas como las contenidas en la Directiva de Seguridad elaborada por la Autoridad Nacional de Protección de Datos Personales.

Las entidades de la Administración Pública[12] como los prestadores de servicios en la nube tienen responsabilidades por diferentes aspectos de la provisión de dichos servicios; por lo tanto, ambas partes evalúan el conjunto de prácticas que resulten necesarias para asegurar suficientemente sus respectivos entornos.

La Ley N° 29733 – Ley de Protección de Datos Personales, no hace referencia directa a la contratación de servicios en la nube. Sin embargo, acorde con su artículo 9.- Principio de seguridad, en dicha norma se considera que para fines del tratamiento de datos personales, el titular del banco de datos personales y el encargado de su tratamiento establecen las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales y, por consiguiente, evitar su alteración, pérdida, tratamiento o acceso no autorizado; para ello, las medidas de seguridad a establecerse serán las apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate. Los requisitos y condiciones de los bancos de datos personales en materia de seguridad son establecidos por la Autoridad Nacional de Protección de Datos Personales, salvo la existencia de disposiciones especiales contenidas en otras leyes.

En tal sentido, al considerar la implementación de servicios en la nube, uno de los criterios más importantes es el relacionado al tipo de información o al contenido de los datos personales que el proveedor de los servicios de la nube almacenará o procesará, para lo cual dichos proveedores proporcionarán información detallada de cómo las entidades de las administración pública

[12] Entidad comprendida en el artículo I del Título Preliminar de la Ley N° 27444, Ley del Procedimiento Administrativo General, o la que haga sus veces, de conformidad con lo indicado por el artículo 2, numeral 9), de la Ley N° 29733 – Ley de Protección de Datos Personales.

pueden satisfacer los requisitos específicos de conformidad con la regulación de la materia antes citada en caso opten por utilizar los servicios de computación en la nube .

Es necesario que las entidades de la Administración Pública mantengan el control total y la propiedad sobre sus datos, y tengan la posibilidad de elegir, de acuerdo con sus evaluaciones de riegos e impactos, la ubicación geográfica en la que se puedan almacenar los mismos. Por otro lado, los prestadores de servicios en la nube deberán proporcionar controles de identidad y acceso para restringir el acceso a la infraestructura y los datos del cliente, cumpliendo para tal efecto los estándares de cumplimiento, y observar las políticas de seguridad y cumplimiento de la nube, como: visibilidad, control y auditabilidad.

Las entidades de la Administración Pública que opten por servicios en la nube estudiaran con detalle qué tipo de datos personales son susceptibles de ser transferidos a dichos servicios de conformidad con la legislación sobre la materia; a tal efecto, es adecuado que conozcan detalladamente que tipo de datos trata.

Los tipos de datos a considerar son:

- **Datos personales**. - Es toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.
- **Datos sensibles**. - Son datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

Asimismo, considerando que la responsabilidad sobre la protección de datos personales es propia de cada uno de los entes públicos y debe ser ejercida por los mismos, en cuanto establecen los controles de seguridad adecuados según los tipos de datos personales que almacenan y gestionan de acuerdo a la legislación y normativa vigente, es recomendable que el área o el responsable de la protección de datos personales que cada entidad de la Administración Pública hubiera designado tenga como interlocutor al área responsable que corresponda del proveedor de servicios en la nube – PSN.

5.1. De la legislación nacional sobre protección de datos personales y el uso de servicios en la nube

La Ley N° 29733 – Ley de Protección de Datos Personales, en su artículo 30, establece que "[c]uando, por cuenta de terceros, se presten servicios de tratamiento de datos personales, estos no pueden aplicarse o utilizarse con un fin distinto al que figura en el contrato o convenio celebrado ni ser transferidos a otras personas, ni aun para su conservación".

En base a ello, el artículo 33 del Decreto Supremo N° 0003-2013-JUS - Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales, establece que "[e]l tratamiento de datos personales por medios tecnológicos tercerizados, sea completo o parcial, podrá ser contratado por el responsable del tratamiento de datos personales siempre y cuando para la ejecución de aquel se garantice el cumplimiento de lo establecido en la Ley y el […] reglamento".

En ese sentido, las entidades deben decidir qué datos mantendrá en sus propios sistemas de información. Luego de lo cual, atendiendo al artículo 8.- Principio de finalidad de la reseñada Ley de Protección de Datos Personales, el proveedor de servicios en la nube debe garantizar que no utilizará los datos para otra finalidad que no tenga relación con los servicios contratados.

5.2. Del responsable y al encargado del tratamiento de datos personales

Previamente al proceso de contratación de algún servicio en la nube, se identificarán al responsable del tratamiento, al encargado del tratamiento y sus interacciones con el fin de determinar cuál es la responsable de cumplir con las normas de protección de datos, y así definir cómo pueden ejercer los administrados sus derechos, cuál es la legislación nacional aplicable y cuál es la eficacia con la que la Autoridad Nacional de Protección de Datos puede operar.

Así, el responsable del tratamiento de datos personales seguirá siendo la entidad de la Administración Pública que contrata servicios en la nube, no pudiendo incorporarse como una cláusula contractual algún cambio o sustitución de la responsabilidad; por otro lado, el encargado del tratamiento de datos personales será el proveedor de servicios en la nube. Sin embargo, los roles del responsable como del encargado del tratamiento de datos se determinarán de acuerdo a cada caso en que se usa prestación de servicios en la nube.

En el caso que una entidad de la Administración Pública contrate servicios de almacenamiento en la nube sin tratamiento de datos personales (Por ejemplo: se utilice un procedimiento de disociación o anonimización), es recomendable que dichos datos se cifren antes de salir de la entidad, de forma que los requisitos de seguridad sobre los proveedores se reduzcan a la dimensión de disponibilidad.

5.3. Del control previo a la contratación de servicios en la nube

Las entidades de la Administración Pública que contraten servicios en la nube deben tener claro que el control previo puede ser necesario para el tratamiento de datos, dependiendo del tipo de servicios en la nube y de los tipos de datos que se procesen.

La transferencia de datos requiere necesariamente una verificación previa a la relación contractual, del tipo de servicio que prestan los proveedores, a fin de verificar el adecuado cumplimiento de la normatividad; toda vez que algunos de los usos de servicios en la nube implicarán tener sistemas de estado críticos y operaciones complejas y proyectos de migración, por lo que los contratos de los servicios en la nube se adecuan a la legislación y jurisdicción peruana.

Así, las entidades de la Administración Pública podrán contrastar que las condiciones ofrecidas con el proveedor de servicios en la nube incluyan elementos relacionados a la información, ubicación del tratamiento de datos, existencia de sub encargados, políticas de seguridad, derecho del usuario y obligaciones legales del proveedor, de forma tal que permitan la portabilidad de los datos en caso se requiere un cambio de proveedor.

5.4. De la localización del proceso y de los datos personales

Los proveedores de servicios en la nube deberán respetar los derechos de los ciudadanos e identificar las responsabilidades compartidas con las entidades que contratan dichos servicios, para ello, los proveedores garantizarán que la localización de cada uno de los recursos físicos que emplea para implementar el servicio de computación en la nube, de forma directa o subcontratada, se encuentren en países cuya legislación permita la aplicación de medidas de seguridad apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate[13], así como que permita el cumplimiento de las obligaciones adquiridas contractualmente con las entidades públicas peruanas; toda vez que si bien los datos pueden estar en distintos lugares y momentos, los derechos de los ciudadanos y las obligaciones de protección de los datos personales, deben estar permanentes cautelados en función a las responsabilidad del encargado o responsable del tratamiento de los datos.

Sin embargo, en caso se realice flujo transfronterizo de datos personales, se habrá garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por la Ley o por los estándares internacionales en la materia[14].

Las entidades de la Administración Pública que almacenen y procesen cantidades masivas de datos personales de alta confidencialidad con características críticas para la seguridad de este país, pueden evaluar que la localización de los datos se restringa al ámbito territorial para este tipo de datos; para lo cual inclusive pueden optan por contratar servicios en nube que almacenen y procesen estos tipos de datos en dispositivos dedicados en un entorno de nube dedicado para mayor seguridad.

5.5. De las medidas técnicas y organizativas apropiadas y acordes: Integridad de los datos, gestión de identidades y control de acceso

La integridad y la disponibilidad de los datos son elementos esenciales en la prestación de los servicios de computación en la nube.

Actualmente, el responsable del tratamiento y sus encargados implementarán las medidas técnicas y organizativas para proteger los datos personales contra su destrucción accidental o ilícita o su pérdida accidental, alteración, divulgación o acceso no autorizado; teniendo en cuenta el estado de la técnica y el coste de su implementación, dichas medidas deben garantizar un nivel de seguridad apropiados y acordes en relación con los riesgos representados por el tratamiento y la naturaleza de los datos a proteger.

Si bien se puede utilizar normas técnicas (Por ejemplo: NTP-ISO/IEC 27001 o ISO/IEC 27001) para asegurar los datos de los clientes, éstas pueden no ajustarse a los requisitos nacionales con respecto a las medidas que es adecuado adoptar. Es necesaria una mayor coherencia y armonización, y por tanto será válido que los proveedores de servicios en la nube proporcionen un elevado nivel de seguridad de los datos personales, con especial atención a la gestión de identidades y el control de acceso.

[13] De conformidad con el artículo 9 de la Ley Nº 29733, Ley de Protección de Datos Personales, concordante con el artículo 10 de su Reglamento aprobado mediante D.S. Nº 003-2013-JUS.
[14] De conformidad con el artículo 9 de la Ley Nº 29733, Ley de Protección de Datos Personales.

5.6. De la filtración de datos personales y notificaciones de incidentes de seguridad

Las entidades de la Administración Pública que contratan servicios en la nube, podrán requerir a los proveedores de dicho servicio, la existencia de mecanismos para compartir oportunamente con dichas entidades los hallazgos que le sean pertinentes sobre violaciones de la seguridad que hubieran tenido relación con los datos personales al encargado o responsable del tratamiento.

De acuerdo a los estándares internacionales sobre protección de datos, será opcional que las entidades que contraten servicios en la nube, previamente identifiquen claramente el grado de violación de la seguridad de los datos que se debe comunicar, a quién se debe comunicar (cliente del proveedor de servicios en la nube, con conocimiento de la autoridad competente en cuanto a protección de datos, y a los interesados), así como las modalidades pertinentes. Una obligación indeterminada de comunicar cualquier violación (incluso las menores o insignificantes) de la seguridad de los datos personales puede perjudicar gravemente a los proveedores de servicios en la nube y generar una alarma innecesaria de las entidades de la Administración Pública y de los ciudadanos en general.

5.7. Del derecho de acceso de los ciudadanos a los datos personales

El responsable o el encargado del tratamiento de datos personales, según sea el caso (por ejemplo, si se hubiera estipulado en el contrato), tiene la obligación de garantizar a los ciudadanos, los derechos establecidos en la legislación nacional; por ejemplo, a obtener la confirmación de si se están procesando o no datos relativos al interesado, a obtener información sobre los propósitos del tratamiento, las categorías de los datos en cuestión, el receptor o las categorías de los destinatarios a quienes se comunicarán los datos, a corregir, borrar o bloquear los datos procesados de un modo que no sea compatible con las disposiciones de la normatividad existente.

Es muy importante, especialmente cuando el proveedor de servicios en la nube se engloba en la definición de encargado del tratamiento, que dicho proveedor establezca una cooperación muy estrecha con las entidades de la Administración Pública que los contratan, para asegurar que estos últimos, en su calidad de responsables del tratamiento, estén en condiciones de cumplir sus obligaciones respecto a la protección de datos frente a los interesados.

Es conveniente precisar los términos de esa cooperación entre las partes en el contrato correspondiente, pues ya que se realiza el tratamiento de datos personales, es necesario observar los estándares y las normas sobre la materia.

En esta situación, la naturaleza de los datos puede oscilar desde información personal aparentemente poco importante, hasta información altamente confidencial, como expedientes penales y registros relativos a la suspensión del derecho al voto y de licencias. Esto implica, que las entidades de la Administración Pública deben considerar la confidencialidad de los datos para los servicios que se ejecutan en la nube, y también para la infraestructura de la nube en sí.

Las entidades de la Administración Pública pueden considerar necesario llevar a cabo comprobaciones antes del procesamiento, según el tipo de servicio y de los tipos de datos que se van a procesar.

5.8. De las obligaciones adicionales de las entidades que contratan servicios en la nube

La provisión de servicios en la nube requiere que las entidades de la Administración Pública que lo contratan soliciten información sobre la intervención de subcontratistas en la prestación; pues en ese sentido, dará su conformidad a la participación de los subcontratistas, previo informe de la tipología de servicios que subcontrata el prestador de servicios.

En el acto contractual, es recomendable incorporar las cláusulas que correspondan para la protección de datos personales por parte del encargado y del responsable del tratamiento.

6. Normativa interna

Es responsabilidad de las entidades de la Administración Pública, documentar, publicar y comunicar internamente a los usuarios del servicio en la nube, los criterios de uso aceptable del servicio, incluyendo:

- Finalidades de uso permitidas
- Tipo de información que puede usarse en el servicio
- Acciones prohibidas
- Responsabilidades y obligaciones del usuario (por ejemplo, custodia de credenciales de acceso, etc.)
- Acceso y uso del servicio desde dispositivos personales (por ejemplo, smartphones, tabletas, portátiles, etc.)
- Herramientas y medidas de seguridad que se deben utilizar (por ejemplo, cifrado de información, copias de seguridad (backup), etc).

7. Contratación

En cuanto a la contratación de servicios en la nube por parte de las entidades de la Administración Pública y un tercero, una de las primeras medidas a contemplar son los Acuerdos de Nivel de Servicio (ANS); en efecto, ello responde a la necesidad de establecer una serie de requisitos contractuales en la prestación del servicio, debiendo contemplar las características del servicio a ser provisto, las responsabilidades de ambas partes, los modelos de nube, los términos y condiciones, precios y seguridad, entre otros. A su vez se establecerán acuerdos de nivel de servicio para definir la calidad del servicio contratado.

Cabe tener en cuenta que la Ley N° 30225 – Ley de Contrataciones del Estado y su modificación efectuada mediante Decreto Legislativo N° 1341, así como su Reglamento, aprobado mediante Decreto Supremo N° 350-2015-EF, modificado por Decreto Supremo N° 056-2017-EF, regula los procedimientos de contratación de las entidades de la Administración Pública. La provisión de servicios en la nube se encuentra inmerso en lo relacionado a la contratación. La flexibilidad para realizar cambios sobre las características del servicio, así como el pago por uso, requieren la adaptación de los modelos contractuales por parte de las entidades la Administración Pública. Estos contratos deberán contener, al menos, los siguientes aspectos:

- Definiciones.
- Acuerdo de Nivel de Servicio.
    - Descripción del servicio.
    - Tipo de servicio.
    - Disponibilidad (cantidad de tiempo de inactividad máxima (diario, mensual) o porcentaje de tiempo (diario, mensual) que el servicio estará disponible para su uso.
    - Capacidad del servicio.
    - Mantenimiento (planificado o no planificado, horarios, formas de comunicación).
    - Tiempos de respuesta.
- Tipo de infraestructura.
- Protección de la información.
- Penalizaciones, etc.
- Seguridad.
    - Política de Seguridad o Privacidad (enlaces o correos de contacto)
    - Seguridad en la transferencia
    - Seguridad en el almacenamiento
    - Seguridad física
    - Mecanismos de acceso al servicio.
- Responsabilidades y obligaciones.
- Requisitos legales.
- Gestión de cambios.
- Registro de actividad.
- Gestión de incidentes.
- Eliminación de información.
- Respaldo y recuperación de datos.
- Continuidad del servicio.
- Finalización del servicio.
- Requisitos para la protección de datos personales.
- Modificaciones al contrato.

7.1. Ley de Contrataciones del Estado modificada por Decreto Legislativo N° 1341.

Asimismo, se deberán considerar los principios a que se refiere el artículo 2 del Decreto Legislativo N° 1341:

- Libertad y concurrencia.
- Igualdad de trato.
- Transparencia.
- Publicidad.
- Competencia.
- Eficacia y eficiencia.
- Vigencia tecnológica.
- Sostenibilidad ambiental y social.
- Equidad.
- Integridad.

En cuanto a los supuestos excluidos del ámbito de aplicación deberá aplicarse lo establecido en el Decreto Legislativo N° 1341, o la norma vigente. Asimismo, la organización de los procesos de contratación se realizará de acuerdo a lo dispuesto en esta normativa.

Responsabilidades de las entidades de la Administración Pública:

Para el requerimiento de servicio de contratación en la nube, se observará las disposiciones legales vigentes sobre contratación pública, por lo cual el área usuaria requiere los bienes y servicios a contratar, siendo responsable de los términos de referencia o expediente técnico, además de justificar la finalidad pública de la contratación, Los bienes, servicios u obras que se requieran deben estar orientados al cumplimiento de las funciones de la entidad.

El Contrato debe celebrarse por escrito, lo cual incluye la posibilidad de realizarlo por medios electrónicos, ópticos u otros análogos[15], y ajustarse a la proforma incluida en los documentos del procedimiento de selección con las modificaciones aprobadas por la entidad, de acuerdo a lo establecido en los procedimientos de contratación pública; y su modificación podrá realizarse de acuerdo a ley.

Los contratos incluyen necesariamente:

a) Garantías.
b) Anticorrupción.
c) Solución de Controversias.
d) Resolución del Contrato por incumplimiento.

Responsabilidad del contratista (proveedor de Nube):

El contratista es responsable de ejecutar la totalidad de las obligaciones a su cargo, de acuerdo a lo establecido en el contrato. El plazo de responsabilidad lo determina la ley de la materia.

En contratos de bienes y servicios el contratista es responsable por la calidad ofrecida y por los vicios ocultos por un plazo no menor de un año contado a partir de la conformidad otorgada por la entidad.

Obligatoriedad de utilizar el Sistema Electrónico de Contrataciones del Estado (SEACE), en las contrataciones que se realicen.

Contratación:

Determinar un adecuado Acuerdo de Nivel de Servicio (ANS), es esencial al momento de contratar servicios en la nube.

Las entidades de la Administración Pública al contratar servicios de nube tendrán en consideración los aspectos siguientes:

[15] De conformidad con lo establecido por el ***artículo 1374.- Conocimiento y contratación entre ausentes***, regulado por el Código Civil cuya aplicación es supletoria a las relaciones jurídicas reguladas por otras leyes, siempre que no sean incompatible con su naturaleza, conforme al artículo IX del Título Preliminar de dicho cuerpo normativo.

a) Realizar el análisis de mercado, determinando y comparando de forma previa, de acuerdo a lo establecido en la Ley de Contrataciones del Estado, las condiciones en la que los proveedores de nube prestan dicho servicio, con el fin de verificar si se realiza un nivel adecuado de cumplimiento, para lo cual se solicitará al proveedor la lista de controles establecidas por su empresa, la que deberá ser evaluada y contrastada con otros proveedores de nube, por la entidad pública que considera contratar el servicio.
b) Determinar si el tipo de servicio a contratarse será: Nube Pública, Nube Privada, Nube Híbrida u otra modalidad previamente acordada.
c) Establecer responsabilidad solidaria del proveedor con el sub contratante, quien deberá cumplir con los mismos requisitos que el proveedor de servicios en la nube.
d) Confirmar que el proveedor de nube cumpla con las políticas, normas de seguridad de la Información, las NTP e ISO aprobadas por el Estado Peruano, así como con los convenios y acuerdos internacionales que sobre seguridad de la información el Perú hubiere suscrito o sea parte.
e) Establecer la disponibilidad de la portabilidad de la información por parte del proveedor de nube, estableciendo los accesos y limitaciones respecto de la transferencia de datos y aplicaciones desde el proveedor de nube a los sistemas del usuario; debiendo a su vez garantizar el proveedor, la disponibilidad de los datos y la continuidad del servicio, señalando los niveles de oscilación (eventual) máxima.
f) Disponer que el servicio de nube sea auditable y transparente al usuario.
g) Establecer que la información de carácter general como aquella de carácter personal almacenada es de propiedad exclusiva de la entidad de la Administración Pública, y que en caso de resolverse el contrato de prestación de servicios, la información no permanecerá almacenada, ni será replicada o copiada por el proveedor de servicios de computación en la nube.
h) Realizar un análisis de costos y riesgos respecto a los procedimientos y barreras de ingreso y de salida en caso de cambio de proveedor del servicio de nube, así como los procesos de retorno de datos que habrán de realizarse sin merma de la integridad de los mismos, bajo el control pleno del responsable sobre su destino ulterior.
i) Establecer con claridad el marco regulatorio que rige a ambas partes, entre las que se encuentran: jurisdicción (ley que regirá en caso de controversias), políticas, entre otros.

Obligaciones de las entidades de la Administración Pública:

Análisis y gestión de riesgos sobre la migración de servicios y aplicaciones a entornos de nube. Entre los que se encuentran: sensibilidad de los datos, amenazas, conveniencia de la solución, controles, salvaguardas, para mitigar riesgos, así como:

- Análisis normativo: Que el contrato cumpla con la ley de Contrataciones, la Ley de Protección de Datos, la Ley de Delitos Informáticos, la Política Nacional de Gobierno Electrónico, el Plan de Desarrollo de la Sociedad de la Información – La Agenda Digital Peruana 2.0, entre otros.

- Protección de la información: Considerar cifrado, tanto de los datos en tránsito como a los datos almacenados, garantizando de esta forma la confidencialidad, así como la creación de copias de respaldo que garanticen su plena disponibilidad e integridad.
- Análisis de seguridad y continuidad del servicio: Adecuada gestión de las incidencias de seguridad y mecanismos que garanticen la continuidad del servicio en caso de catástrofes o incidentes.
- Auditoría de seguridad: Garantizar la realización de auditorías de seguridad ordinaria y extraordinaria. Incluyendo destinatarios de las auditorias y conclusiones.

El contrato debe garantizar la portabilidad de los datos entre el prestador de servicios y el ejercicio del derecho de acceso por los ciudadanos, mediante el uso de forma estándares e interoperables de acuerdo a la legislación vigente, esto es el Decreto Supremo N° 083-2011-PCM, Decreto Legislativo N° 1246, Decreto Legislativo N° 1310, normas sobre Datos Abiertos, la Ley de Neutralidad Tecnología, entre otros.

Las entidades de la Administración Pública deben garantizar medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad respecto de la recuperación y conservación de los datos, documentos electrónicos a lo largo de su ciclo de vida.

Obligaciones de los proveedores de servicios en la nube:

Contar con medidas de seguridad equiparable a lo previsto por nuestra legislación o por los estándares internacionales en la materia. Certificación ISO, Brindar información fidedigna y comprobable sobre las medidas de seguridad implementadas.
Facultad que un tercero independiente audite la seguridad de la empresa proveedora del servicio de nube.
Informar a las entidades de la Administración Pública sobre incidentes de seguridad que pudieran afectar los datos o servicios brindados, así como las medidas adoptadas para resolver los incidentes.
Suscribir un acuerdo de confidencialidad entre el encargado del tratamiento de datos de la empresa y el representante autorizado por las entidades de la Administración Pública, que incluye el compromiso de dar instrucciones al personal que tratará los datos para que mantengan la misma confidencialidad.
Brindar el servicio de nube de forma eficiente, transparente, segura, de acuerdo a lo establecido en el NSA.

La resolución del contrato podrá darse por:

- Finalización del plazo.
- Por imposibilidad de continuar brindándose el servicio.
- De forma unilateral por incumplimiento de una de las partes.
- De forma consensuada por acuerdo de ambas partes.

No obstante, lo antes señalado, siendo los contratos de servicio de nube, regularmente contratos de adhesión, las entidades de la Administración Pública y los proveedores de servicios en la nube deberán para contratar con el Estado Peruano considerar en sus contratos los requisitos antes señalados, bajo sanción de nulidad.

7.2. Descripción del servicio

Uno de los requisitos principales que debe reflejarse contractualmente es la descripción detallada del servicio que el proveedor va a prestar. Esta descripción debe incluir los acuerdos de nivel de servicio y todas las especificaciones del mismo.

El contrato recogerá los niveles de seguridad de la información y de los servicios afectados, de forma que el proveedor de servicios en la nube aplique las medidas de seguridad correspondientes en cada caso.

7.3. Subcontratación

Cuando el proveedor contrata a un tercero como soporte de sus servicios. Ejemplos:

- Contratación de personal.
- Contratación de instalaciones.
- Contratación de servicios de comunicaciones.
- Contratación de servicios de copias de respaldo.

Las subcontrataciones deben ser informadas y aceptadas por la parte contratante.

Las obligaciones del proveedor en materia de seguridad se transmiten de forma transitiva a las partes subcontratadas. En particular los niveles de seguridad de la información a la que tenga acceso el proveedor, y de los servicios que de este último dependan. La parte subcontratada deberá atender a los requisitos de seguridad derivados del el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información"según se recoge en el numeral 3 de este lineamiento.

En cuanto a contrataciones realizadas con proveedores no domiciliados se aplicará lo establecido en el artículo 5.1, literal f) del Decreto Legislativo N° 1341.

Subcontrataciones:

El contratista puede subcontratar previa autorización de la entidad de la Administración Pública la ejecución de determinadas prestaciones del contrato hasta el porcentaje que establezca el Reglamento de la Ley de Contrataciones y Adquisiciones del Estado, salvo prohibición expresa contenida en los documentos del procedimiento de selección.
NOTA: No se pueden subcontratar las prestaciones esenciales del contrato vinculadas a los aspectos que determinaron la selección del contratista. Por ejemplo, que cumpla con la legislación vinculada a la Protección de Datos Personales.

7.4. Protección de la información

El contrato debe determinar la propiedad de la información a la que va a tener acceso el proveedor, sea de la parte contratante o de terceras partes. El proveedor debe comprometerse en el contrato a mantener la confidencialidad en el tratamiento de la información del cliente, comprometerse por contrato a no divulgar o acceder indebidamente a la información sin la autorización expresa de su propietario. El proveedor queda obligado a no acceder ni utilizar la información a la que tenga acceso para fin alguno que no esté explicitado en el contrato o se autorice expresamente por escrito con posterioridad a la firma del contrato.

Por lo que respecta a la legislación que afecta a la contratación de servicios en la nube, es de aplicación al menos la legislación que forma parte de los Anexos – "REFERENCIAS" y "MARCO LEGAL" y que hacen parte del presente lineamiento.

7.5. Acuerdos de nivel de servicios

Deben acordarse unos Acuerdos Niveles de Servicio (ANS). Estos acuerdos deben ser aceptables para las entidades de la Administración Pública contratantes y el proveedor que los prestará y deberán reflejar aspectos referentes a capacidad, disponibilidad, continuidad o gestión de incidentes, así como peticiones de cambio, entre otros, con al menos los siguientes criterios:

- Capacidad: se definirán desviaciones de carga que el proveedor deberá asumir. Del mismo modo se definirán tiempos de notificación cuando se detecte insuficiencia de recursos.

- Disponibilidad: se establecerán porcentajes de disponibilidad del servicio en función de la criticidad del mismo, identificándose si hubiera periodos críticos en los que se requieren mayores niveles de disponibilidad. O también se podría indicar la cantidad de tiempo de inactividad máxima (diario o mensual) del Servicio

- Tiempos de recuperación: se definirán tiempos de recuperación para los sistemas de información en línea con los criterios de valoración de disponibilidad de los servicios según la Norma Técnica Peruana "NTP ISO/IEC 27001:2014".

- Peticiones de cambio e incidentes: se definirán los tiempos de respuesta y resolución dependiendo de la naturaleza y complejidad del incidente, así como el horario de atención a peticiones de cambio realizadas por la organización cliente o incidentes reportados automática o manualmente.

De cada ANS, se requerirá la definición de los siguientes aspectos:

- Parámetro: identificador del ANS.
- Responsabilidades: quién recoge y facilita los datos necesarios para realizar los cálculos.

- Fórmula: descripción del cálculo para la obtención del ANS.
- Periodicidad de la captura de datos, del cálculo de las métricas derivadas y de la verificación de umbrales de aviso y de alarma.
- Umbrales: valores mínimos en la prestación del servicio que disparan situaciones de aviso (hay que monitorizar) y de alarma (hay que corregir)
- Penalización: procedimiento para determinar y cuantificar las consecuencias derivadas del incumplimiento de ANS.
- Periodicidad: Se determinará la periodicidad de los informes de cumplimiento de los ANS.

Asimismo, teniendo en cuenta que los niveles de servicio están asociados con diferentes costos, las entidades públicas contratantes podrán evaluar e identificar los servicios de nivel adecuado de acuerdo con las aplicaciones específicas o los datos procesados, asegurando que los requisitos mínimos cumplan con un costo adecuado.

7.6. Acceso al servicio

Se determinarán:

- Los mecanismos de identificación y autenticación para el acceso de los usuarios al servicio.
- Los mecanismos de identificación y autenticación para el acceso de los administradores.
- Los mecanismos de protección de la autenticidad del servidor.
- Los mecanismos de protección de la confidencialidad y la integridad de la información que se trasiegue a través de redes fuera del absoluto control de las partes.

7.7. Responsabilidades y obligaciones

El contrato definirá los roles de las áreas y el personal involucrado en la prestación del servicio, tanto en la parte de la entidad de la Administración Pública contratante como del proveedor de servicios.
A continuación, se describen las responsabilidades mínimas que deberán estar cubiertas en cada caso.

Por parte del proveedor de servicios y de la entidad de la Administración Pública contratante, se deben considerar las siguientes responsabilidades mínimas. Al tratarse de procedimientos de coordinación, ambas partes deben definir a sus interlocutores:

- Área responsable de la seguridad.
- Área o personal de contacto para incidentes de seguridad.
- Área o personal de contacto para cambios y mantenimiento de sistemas.
- Área o personal de contacto para incidencias relativas a los indicadores de servicio (ANS).
- Área o personal de contacto para aspectos contractuales.
- Área o personal de contacto para temas jurídicos y regulatorios, en particular en lo relativo a datos de carácter personal.

7.8. Registro de actividad

Uno de los aspectos que persigue la Norma Técnica Peruana “NTP ISO/IEC 27001:2014” es disponer de trazabilidad de las acciones realizadas sobre los sistemas de información. De esta manera, los sistemas proporcionados por los proveedores de servicios en la nube deberán disponer de registros de acceso que permitan monitorizar, analizar, investigar y documentar acciones indebidas o no autorizadas, tanto a nivel operativo como de administración.

El contrato debe determinar las obligaciones del indicado proveedor en cuanto a registro de la actividad sobre los servicios contratados. Esta actividad comprende tanto a los usuarios de la parte contratante como a los administradores de una y otra parte.

Se detallarán las condiciones en cuanto a control de acceso a los registros de actividad. Quién tiene derecho a acceder a qué información y qué autorizaciones se requieren.

Se detallarán las obligaciones en cuanto a consolidación periódica de datos y la retención de los registros, teniendo en cuenta la naturaleza de la información, de los servicios y la política de la parte contratante.

Puede contemplarse la posibilidad de que el registro de actividad sea hospedado y administrado por la parte contratante, en cuyo caso la parte contratada limita sus obligaciones a proporcionar la información con un determinado tiempo máximo entre que se produce el hecho a registrar y su traslado al servicio de registro.

Los puntos anteriores pueden cubrirse de diferente manera según el registro afecte a incidencias técnicas o a una parte sustancial de la información tratada o de los servicios prestados. Por ejemplo, los registros de acceso a la información esencial pueden considerarse especialmente sensibles y ser hospedados y custodiados en los sistemas del cliente, mientras que el registro rutinario de operación de los sistemas puede quedar como responsabilidad del proveedor de servicios en la nube.

7.9. Finalización del servicio

El contrato que suscriban las entidades de la Administración Pública especificará las condiciones, procedimientos y plazos para una terminación pactada y una terminación abrupta por incumplimiento de los supuestos contractuales.

La finalización del servicio deberá estar recogida en la descripción del propio servicio, identificando la necesidad que pueda existir de que el proveedor devuelva la información a la finalización de la relación contractual y debiendo constar esto en una cláusula junto al tiempo que tardará el proveedor en realizar la migración de los datos. A este respecto se buscará la “neutralidad tecnológica” del servicio que facilite todo tipo de retorno o migración. Las entidades de la Administración Pública deberán analizar la neutralidad tecnológica y el nivel de interoperabilidad de cada proveedor de servicios en la nube, lo cual incluye, pero no se limita a la adopción de la arquitectura

abierta de la nube, el formato estándar de la industria para el almacenamiento de datos, las API compatibles para servicios comunes, entre otros.

Finalmente, deberá estar recogida la necesidad de que el proveedor elimine la información a la finalización de la relación contractual y debiendo constar esto en una cláusula junto a los mecanismos y el tiempo que tardará el proveedor en realizar la destrucción de los datos. Estas cláusulas deben recoger las obligaciones de retención de datos que pudieran ser obligatorias por política o por imperativo legal, indicando los periodos correspondientes y las obligaciones del proveedor en lo que respecta a confidencialidad y control de acceso. Por último, deben recogerse las obligaciones del proveedor para garantizar que la destrucción es efectiva; por ejemplo auditorías.

8. Operación

8.1. Seguimiento del servicio

Al realizar la medición del cumplimiento del servicio, la entidad de la Administración Pública debe considerar evaluar lo siguiente:

a) Cumplimiento de medidas de seguridad.
b) Controles de seguridad.
c) Políticas que garanticen la integridad, confidencialidad y disponibilidad de los datos.
d) Nivel de prestación del servicio según lo acordado en el Acuerdo de Nivel de Servicio (ANS).

En esta línea, señalar que las actividades para verificar el cumplimiento del servicio pueden ser a través de controles técnicos o revisión de los informes de servicio remitidos por el proveedor de servicios en la nube. Durante la verificación la entidad debe considerar al menos los siguientes controles:

- Niveles de calidad, disponibilidad, fiabilidad y capacidad del servicio ofrecido, incluyendo el cumplimiento de las obligaciones de servicio acordadas y la respuesta ofrecida por el proveedor ante desviaciones significativas acordadas en el contrato.
- Niveles de integridad, confidencialidad y disponibilidad de los datos de acuerdo a los requisitos especificados.
- Cumplimiento normativo y legislativo entre el prestador y el cliente de los servicios, incluyendo los aspectos de cumplimiento de aplicación sobre el prestador que correspondan en cada caso, como por ejemplo las disposiciones de la Ley de Protección de Datos Personales y su Reglamento, normatividad obligatoria en materia de Seguridad de la Información, legislación en contratación con el Estado u otros.
- Gestión de incidentes de seguridad, incluyendo toda la información necesaria para determinar orígenes, objetivos, riesgos u otros asociados a cualquier incidente relevante.
- Control de acceso a los servicios, incluyendo listado actualizado de usuarios autorizados para utilizar los servicios disponibles, y los privilegios asociados en cada caso.

- Situación actual de las medidas de protección de la información establecidas por el proveedor, que incluyan aspectos de seguridad física, protección contra software malicioso, seguridad del personal, copias de seguridad u otros.
- Mecanismos definidos para la comprobación de los controles de seguridad por parte del proveedor y los resultados de dichas comprobaciones.

Asimismo, la entidad de la Administración Pública debe solicitar al proveedor los informes de auditoría y no conformidades de aplicación para verificar las medidas de seguridad empleadas por este.

8.2. Prestación del Servicio

Durante la prestación del servicio la entidad de la Administración Pública debe evaluar los requisitos necesarios para que los servicios contratados (infraestructura, plataforma, servicios u otros) mantengan un nivel aceptable frente a imprevistos, fallos aleatorios, degradaciones del desempeño o ataques premeditados. En esta línea, debe considerar los siguientes ámbitos:

a) Disponibilidad y fiabilidad

La disponibilidad de un servicio en la nube dependerá muchas veces de la red que emplee la entidad de la Administración Pública para acceder, es por ello que algunas medidas adoptadas también serán de aplicación a sus proveedores de servicios de Internet.

Para verificar el cumplimiento de la disponibilidad y fiabilidad del servicio, la entidad puede solicitar la siguiente información:

- Tiempo medio hasta que se produce un fallo.
- Tiempo medio entre fallos.
- Disponibilidad total mensual (o diaria).
- Tasa de incidencias.
- Tolerancia a ataques maliciosos.
- Redundancia.
- Replicación.

Además, la entidad de la Administración Pública puede considerar aquellos parámetros vinculados a la calidad de la conexión de red, que podrían afectar el tiempo de respuesta del servicio.

- Rendimiento (ancho de banda).
- Latencia (tiempo medio de ida y vuelta [round trip]).
- Pérdida de paquete.
- Variación de demora paquetes (latencias).

Las entidades de la Administración Pública deben evaluar el rendimiento de la red y la fiabilidad de cada proveedor de servicios en la nube y queda a criterio priorizar a los proveedores de confianza con buenos antecedentes, toda vez que la red es uno de los elementos

fundamentales para la disponibilidad y la fiabilidad a los que hay que prestar más atención.

Debe quedar claro que en el Acuerdo de Nivel de Servicio (ANS) suscrito se haya considerado información sobre:

- Descripción, horario, disponibilidad y fiabilidad del servicio.
- Datos de la mesa de ayuda o punto de contacto (correo, teléfono, web, etc.).
- Reportes de la caída de un servicio, la fecha, la duración, descripción, componente fallado e impacto en el número de usuarios.
- Tiempo de respuesta del servicio, vía de comunicación y cambios.
- Continuidad, seguridad, costo, informes y penalizaciones.

b) Escalabilidad y elasticidad

Las entidades de la Administración Pública deben evaluar que el proveedor de servicio en la nube (servicio, infraestructura, plataforma) sea capaz de prestar el servicio acordado de forma rentable y en el tiempo adecuado; teniendo en cuenta la capacidad de gestionar cambios en los recursos demandados (variaciones en almacenamiento, memoria, etc.), así como la escalabilidad a largo plazo.

La entidad de la Administración Pública puede solicitar información sobre los siguientes parámetros o mediciones:

- Tolerancia de carga (carga máxima que puede soportar un sistema en comparación con la carga normal esperada).
- Tolerancia de tráfico (soportar cargas impredecibles, aislar el tráfico cruzado, provisiones anti-DoS[16]/DDoS[17], flash crowd, otros).
- Variabilidad de la carga de los servicios (diferencia entre demanda pico y demanda media).

c) Respuesta y recuperación (Respaldo y recuperación de datos)

La entidad de la Administración Pública debe solicitar al proveedor del servicio en la nube el procedimiento para realizar copias de respaldo que garantice la restauración de la información, así como también información sobre:

- Alcance de los respaldos.
- Política de copias de seguridad.
- Medidas de cifrado de información en respaldo.
- Procedimiento de solicitud de restauraciones de respaldo.
- Realización de pruebas de restauración.
- Traslado de copias de seguridad (si aplica).

[16] DoS: Ataque de denegación de servicio
[17] DDoS: Ataque de denegación de servicio distribuido

Asimismo, es relevante que la entidad cuente con información sobre los planes de respuesta y recuperación ante incidentes del proveedor, y de ser necesario, los resultados de aplicación de los mismos.

La entidad de la Administración Pública puede solicitar información sobre los siguientes parámetros o mediciones medir la eficacia y eficiencia de las estrategias de respuesta y recuperación:

- Tiempo medio de descubrimiento de la incidencia (demora): el tiempo que lleva descubrir la incidencia desde el momento en que tiene lugar.
- Tiempo para la activación: el tiempo que lleva darse cuenta de que la fase de recuperación-respuesta debe activarse (tiempo medio para la activación).
- Tiempo para reparar (tiempo medio para reparar): el tiempo que lleva recuperar el servicio dentro de un nivel aceptable.
- Tiempo medio de recuperación de la incidencia.

d) Cumplimiento de la legalidad y normativa

Durante la prestación del servicio también es necesario verificar el cumplimiento de las disposiciones legales y normativas vigentes relacionadas a datos personales, seguridad de la información, entre otros.

La entidad de la Administración Pública puede considerar los siguientes aspectos para la verificación:

- Retención de datos y trazabilidad

Evaluar el cumplimiento de las disposiciones y criterios definidos en el Reglamento de la Ley de Protección de Datos Personales referidos a contratación de servicios por medios tecnológicos tercerizados**.** Asimismo, puede considerar los siguientes:

  - Periodo mínimo y máximo de retención de datos.
  - Periodo mínimo y máximo de retención de registros.
  - Modalidad de almacenamiento de los datos.
  - Modalidad de almacenamiento del registro.
  - Tiempo de transferencia al origen.

- Confidencialidad (Revisar lo relacionado a seguridad de la información y datos personales).

8.3. Gestión de la continuidad

Para asegurar la continuidad del servicio la entidad de la Administración Pública debe solicitar al proveedor lo siguiente:

- Evidencia de la existencia de un plan de continuidad y plan de recuperación, cuyos alcances incluyan los servicios objeto de la prestación.

- Constancia de que los tiempos de recuperación identificados en el análisis de impacto están alineados con los criterios definidos en el ANS en cuanto a tiempo de recuperación del servicio.
- El procedimiento de coordinación ante incidentes y desastres que puedan afectar a los sistemas de la entidad, dicho procedimiento debe contemplar los flujos de información y las interacciones entre la entidad de la Administración Pública y el proveedor durante la gestión tanto de incidentes como de desastres.
- Información periódica de los incidentes que han afectado a los sistemas que soportan los sistemas de la entidad.
- Realizar pruebas periódicas que involucren a la entidad de la Administración Pública y a los diferentes proveedores y sub proveedores para validar el correcto funcionamiento de los planes y el cumplimiento de los plazos y servicios mínimos previstos.
- Información del Análisis de Impacto de Negocio (BIA por sus siglas en inglés).
- Evaluar el impacto de los cambios realizados por el proveedor (ya sean por actualización, mantenimiento u otros).

8.4. Gestión del cambio

Las entidades de la Administración Pública son responsables de la instrucción del personal existente respecto a los beneficios que supone el uso de los servicios en la nube para aliviar las inquietudes laborales; asimismo los proveedores de dichos servicios deben considerar el ofrecimiento de una variedad de opciones de formación para permitir que las entidades de la Administración Pública y sus usuarios adquieran las cualificaciones, los conocimientos y la experiencia necesarios para diseñar, implementar y gestionar aplicaciones en la plataforma de nube que han elegido.

Por otro lado, la actualización y/o mantenimiento de los sistemas que soportan el servicio en la nube es un aspecto clave que debe ser considerado por el proveedor de dicho servicio y la entidad de la Administración Pública contratante, ello con la finalidad de garantizar el correcto funcionamiento de los mismos.

Al respecto, la entidad de la Administración Pública debe solicitar al proveedor de servicios en la nube, un procedimiento de coordinación para el mantenimiento de los sistemas implicados en el servicio de nube, en el cual deben establecerse los plazos mínimos para notificar la ejecución de las actividades de mantenimiento; dichas notificaciones deben ejecutarse antes y después de realizar el mantenimiento.

Asimismo, la entidad de la Administración Pública debe solicitar y/o acordar con el proveedor de servicios en la nube:

- Políticas y estándares del cambio, de tal manera que se asegure el correcto funcionamiento del servicio.
- Requerimientos de cumplimiento regulatorio (revisar la regulación relacionada con seguridad de la información y datos personales).

- Pruebas y procedimientos de post-evaluación del cambio (pruebas funcionales y operativas), con la finalidad de evaluar que los cambios implementados han sido exitosos.
- Cronograma de cambios.

De igual manera, la entidad de la Administración Pública puede considerar realizar las siguientes métricas:

- Número de interrupciones, incidente y problemas que hubo con el servicio.
- Número de cambios no autorizados que se han llevado a cabo en el servicio.
- Número de cambios forzosos o de emergencia que se realizaron en el servicio.
- Tiempo, esfuerzo y costo que ocasiono el cambio en el servicio.

8.5. Gestión de incidentes

Los parámetros definidos para la gestión de incidentes comprenden todas aquellas acciones y medidas para evitar que se produzcan incidentes o reducir su impacto en el servicio contratado; en esa línea, la entidad de la Administración Pública debe asegurar el cumplimiento de los acuerdos establecidos en el ANS (calidad, tiempo y disponibilidad), así como también el cumplimiento de la normativa y legislación en seguridad de la información y protección de datos personales.

Asimismo, la entidad de la Administración Pública debe solicitar al proveedor de servicio en la nube el procedimiento para la gestión de incidentes, así como también:

- Procedimiento de notificación de incidentes.
- Tipología de incidentes incluidos en el servicio.
- Procedimientos específicos ante incidentes de seguridad.
- Tiempos de respuesta y resolución de incidentes. Cumplimiento del ANS.
- Mantenimiento y gestión del registro de incidentes.

8.6. Finalización del servicio

Sobre la finalización de los servicios la entidad de la Administración Pública debe solicitar al proveedor:

- Procedimientos para recuperar la información entregada (acotar formatos de datos y tiempos).
- Procedimientos para eliminar copias de la información en sus equipos (incluyen mecanismos de borrado, tiempos para destruir la información según legislación vigente).

Cabe resaltar que la aplicación de los procedimientos mencionados anteriormente también deben alcanzar a los terceros proveedores subcontratados.

8.7. Supervisión y auditoría

La entidad de la Administración Pública contratante, como responsable última de los posibles riesgos que afecten tanto a la información como a los servicios prestados, deberá disponer de un determinado nivel control sobre tales servicios. En este sentido y para garantizar el cumplimiento de las medidas de seguridad de aplicación en cada caso, la entidad de la Administración Pública deberá evaluar la conveniencia de disponer del derecho de auditoría, con la profundidad correspondiente, sobre el proveedor de servicios o de solicitar a éste la siguiente documentación:

- Una declaración de aplicabilidad de las medidas a aplicar.
- Una auditoría que verifique mediante evidencias el cumplimiento de las medidas de seguridad de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014" que sean de aplicación de acuerdo con el nivel del sistema.

El proveedor de servicios en la nube puede disponer de certificaciones o acreditaciones en materia de seguridad. Estas certificaciones pueden simplificar la auditoría completa del servicio prestado, en su condición de evidencias de cumplimiento a valorar por el equipo auditor. Por ejemplo:

- Auditorías recomendadas por Agencia Europea de Seguridad de las Redes y de la Información[18], o similares, para proveedores de servicios en la nube [ENISA-CCSL[19]].
- Sistema de Gestión de la Seguridad de la Información (SGSI) [ISO/IEC 27001:2013].
- Sistema de Gestión de la Continuidad [ISO 22301:2012].
- Cloud Controls Matrix [CCM][20].

[18] Conocida por su siglas en idioma inglés de ENISA por *European Union Agency for Network and Information Security*.
[19] Lista de Esquemas de Certificación de la Nube - ofrece una visión general de los diferentes esquemas de certificación existentes que podrían ser relevantes para los clientes de computación en la nube, el cual puede ser consultado en: https://goo.gl/mEieY2.
[20] La cual puede ser consultada en: https://cloudsecurityalliance.org/.

Anexos

Glosario de Términos y Abreviaturas

1. Términos

1.1. Activo: ítem, objeto o entidad que tiene valor real o potencial para una organización [ISO 55000:2014].

1.2. Anonimización: Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es irreversible. Ley Nº 29733, Ley de protección de datos personales.

1.3. Auditor de la nube: Responsable de realizar una auditoría de la provisión y el uso de servicios en la nube [ISO / IEC 17788: 2014].

1.4. Categorías de servicio en la nube: Clasificación de la funcionalidad proporcionada por un servicio en la nube para el cliente de dicho servicio en función de los recursos utilizados [ISO / IEC 17788: 2014].
Nota: Para los efectos del presente lineamiento, las categorías de la nube están en función a las capacidades de la aplicación, las capacidades de la infraestructura y las capacidades de la plataforma.

1.5. Disociación: Tratamiento de datos personales que impide la identificación o que no hace identificable al titular de estos. El procedimiento es reversible. Ley Nº 29733, Ley de protección de datos personales.

1.6. Servicio en la Nube: Paradigma para permitir el acceso a la red a un conjunto escalable y elástico de recursos físicos o virtuales compartibles con el aprovisionamiento de autoservicio y la administración según demanda. [ISO / IEC 17788: 2014].
Nota: Los ejemplos de recursos incluyen servidores, sistemas operativos, redes, software, aplicaciones y equipos de almacenamiento.

1.7. Portabilidad de los datos de la Nube: Portabilidad de datos de un servicio en la nube a otro servicio en la nube. [ISO / IEC 17788: 2014].

1.8. Servicio en la Nube: Una o más capacidades ofrecidas a través de la computación en la nube invocada utilizando una interfaz definida. [ISO / IEC 17788: 2014].
Nota: Para los efectos del presente lineamiento, una categoría de servicio en la nube puede incluir capacidades de uno o más tipos de capacidades de la nube.

1.9. Categoría de servicio en la Nube: Grupo de servicios en la nube que poseen un conjunto común de cualidades.
Nota: Una categoría de servicio en la nube puede incluir capacidades de uno o más tipos de capacidades de la nube. [ISO / IEC 17788: 2014].

1.10. Proveedor de servicio en la Nube: Parte que hace que los servicios en la nube estén disponibles. [ISO / IEC 17788: 2014].

1.11. Datos personales: Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados. Decreto Supremo Nº 003-2013-JUS que aprueba el Reglamento de la Ley Nº 29733, Ley de protección de datos personales.

1.12. Encargado del tratamiento: Es quien realiza el tratamiento de los datos personales, pudiendo ser el propio titular del banco de datos personales o el encargado del banco de datos personales u otra persona por encargo del titular del banco de datos personales en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice el tratamiento de datos personales por orden del responsable del tratamiento cuando este se realice sin la existencia de un banco de datos personales. Decreto Supremo Nº 003-2013-JUS que aprueba el Reglamento de la Ley Nº 29733, Ley de protección de datos personales.

1.13. Flujo transfronterizo de datos personales. Transferencia internacional de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban. Ley Nº 29733, Ley de protección de datos personales.

1.14. Nivel suficiente de protección para los datos personales. Nivel de protección que abarca por lo menos la consignación y el respeto de los principios rectores de esta Ley, así como medidas técnicas de seguridad y confidencialidad, apropiadas según la categoría de datos de que se trate. Ley Nº 29733, Ley de protección de datos personales.

1.15. Portabilidad de la Aplicación en la Nube: Posibilidad de migrar una aplicación de un servicio en la nube a otro servicio en la nube [ISO / IEC 17788: 2014].

1.16. Titular del banco de datos personales. Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad. Ley Nº 29733, Ley de protección de datos personales.

1.17. Transferencia de datos personales. Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta del titular de datos personales. Ley Nº 29733, Ley de protección de datos personales.

1.18. Tratamiento de datos personales. Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales. Ley Nº 29733, Ley de protección de datos personales.

1.19. Virtualización: Es la técnica que permite compartir y/o agregar recursos físicos, como sistemas operativos, software y servicios de tecnologías de la información – TI, de forma que se ocultan los detalles técnicos a los usuarios finales y se reduce el costo por unidad de servicio[21].

2. Abreviaturas

2.1. AES – siglas en idioma inglés de *Advanced Encryption Standard*.
2.2. ANS – Acuerdo de Nivel de Servicio.
2.3. APDP - Autoridad Nacional de Protección de Datos Personales.
2.4. DS – Decreto Supremo.
2.5. ECC – Siglas en idioma inglés de *Elliptic Curve Cryptography*.
2.6. ENISA – Siglas en idioma inglés de *European Union Agency for Network and Information Security*.
2.7. ISO/IEC – Siglas en idioma inglés respectivamente de *International Organization for Standardization* e *International Electrotechnical Commission*.
2.8. IaaS - Infraestructura como servicio (*Infrastructure as a Service*).
2.9. IPv6 – Protocolo de Internet versión 6.
2.10. ISP – Siglas en idioma inglés de *Internet Service Providers*.
2.11. NTP - Norma Técnica Peruana.
2.12. NIST - National Institute of Standards and Technology (Instituto Nacional de Normas y Tecnología del Departamento de Comercio de los Estados Unidos de América).
2.13. OCDE - Organización para la Cooperación y el Desarrollo Económico.
2.14. PaaS - Plataforma como servicio (*Platform as a Service*).
2.15. PCM - Presidencia del Consejo de Ministros.
2.16. PSN - Proveedor de Servicios en la Nube.
2.17. RM – Resolución Ministerial.
2.18. RSA – Siglas de sus desarrolladores (Rivest, Shamir y Adleman), es un algoritmo criptográfico de clave pública.
2.19. SeGDi - Secretaría de Gobierno Digital.
2.20. SEACE – Sistema Electrónico de Contrataciones del Estado.
2.21. SGSI – Sistema de Gestión de la Seguridad de la Información.
2.22. SaaS - Software como servicio (*Software as a Service*).
2.23. TIC - Tecnologías de la Información y la Comunicación.
2.24. TDES – en criptografía, Triple DES se le llama al algoritmo que hace triple cifrado del DES. También es conocido como TDES o 3DES.

[21] Turban, E; King, D; Lee, J; Viehland, D (2008). «*Chapter 19: Building E-Commerce Applications and Infrastructure*». *Electronic Commerce A Managerial Perspective* (5th edición). Prentice-Hall. p. 27., documento puede ser consultado en: https://goo.gl/ctUJC5.

Marco Legal

- Decreto Legislativo N° 604, que crea el Sistema Nacional de Informática.
- Ley N° 27658 – Ley Marco de la Modernización de la Gestión del Estado.
- Ley N° 29733 – Ley de Protección de Datos Personales.
- Ley N° 30225 – Ley de Contrataciones del Estado y su modificación efectuada mediante Decreto Legislativo N° 1341.
- Decreto Legislativo N° 1246, que aprueba diversas medidas de Simplificación Administrativa.
- Decreto Legislativo N° 1310, que aprueba medidas adicionales de Simplificación Administrativa.
- Decreto Legislativo N° 1353 que crea la Autoridad Nacional de Transparencia y Acceso a la Información Pública, y modifica la indicada Ley N° 29733.
- Decreto Supremo N° 066-2011-PCM, que aprueba el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital Peruana 2.0.
- Decreto Supremo N° 083-2011-PCM, aprueba la Plataforma de Interoperabilidad del Estado.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales.
- Decreto Supremo N° 081-2013-PCM, que aprueba la Política Nacional de Gobierno Electrónico 2013 – 2017.
- Decreto Supremo N° 350-2015-EF, modificado por Decreto Supremo N° 056-2017-EF, que aprueba el Reglamento de la Ley de Contrataciones del Estado aprobada mediante.
- Decreto Supremo N° 006-2017-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444 - Ley del Procedimiento Administrativo General.
- Decreto Supremo N° 022-2017-PCM, que aprueba el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, y crea la Secretaría de Gobierno Digital de PCM.
- Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la "Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la gestión de la Seguridad de la Información. 2da. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

Estándares

- Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la gestión de la Seguridad de la Información. 2da. Edición
- Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición".
- ISO / IEC 17788: 2014. Information technology — Cloud computing — Overview and vocabulary.

- ISO/IEC 27017 Controles de seguridad de la información basada en ISO/IEC 27002 específicamente para los servicios en nube.
- ISO / IEC 27018 Information technology — Cloud computing — Overview and vocabulary.

Referencias

- *National Institute of Standards and Technology Special Publication 800-145, The NIST Definition of Cloud Computing*, september 2011. https://goo.gl/CzuOg9.
- Seguridad y resistencia en las nubes de la Administración Pública. Informe para la toma de decisiones, publicada por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), Enero de 2011 (se tomó en consideración la traducción al español del informe realizada por el Instituto Nacional de Tecnologías de la Comunicación, INTECO www.inteco.es España). https://goo.gl/akrfgn.
- *National Institute of Standards and Technology Special Publication 800-146, Cloud Computing Synopsis and Recommendations*, may 2012. https://goo.gl/KNlaJM.
- *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service*, publicado por *Chief Acquisition Officers Council in coordination with the Federal Cloud Compliance Comitee*, *February 2012*. https://goo.gl/8BuqYE.
- Principios rectores para la adopción y el uso de la computación en la nube, Informe Oficial de ISACA Serie sobre Visión de la Computación en la Nube, Febrero de 2012. https://goo.gl/2CYqCa.
- *Privacy in Cloud Computing, ITU-T Technology Watch Report*, March 2012. https://goo.gl/p9S2Cg.
- *National Institute of Standards and Technology Special Publication 500-291, Versión 2, NIST Cloud Computing Reference Architecture*, july 2013, https://goo.gl/Al62b9.
- Directiva de Seguridad, elaborada por la Autoridad Nacional de Protección de Datos Personales, 2013. https://goo.gl/e3pX2g.
- GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-823): UTILIZACIÓN DE SERVICIOS EN LA NUBE, editado por el Centro Criptológico Nacional, 2014, Gobierno de España. https://goo.gl/NHE415.
- OECD (2014), "*Cloud Computing: The Concept, Impacts and the Role of Government Policy*", OECD Digital Economy Papers, No. 240, OECD Publishing, Paris. http://dx.doi.org/10.1787/5jxzf4lcc7f5-en.
- Normativa y certificación en la Nube, Estudio elaborado por el capítulo español de Cloud Security Alliance, 2015. https://goo.gl/DGAkCg.
- COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES. Iniciativa Europea de Computación en la Nube: construir en Europa una economía competitiva de los datos y del conocimiento, Bruselas, 19.4.2016. https://goo.gl/8Nz7gM.
- *AWS Cloud Transformation Maturity Model*, September 2016. https://goo.gl/1u3Q3W
- *A Revolution in Public Service, The Growing Case for Public Sector Cloud Adoption*, December 2016, by Innovative Analytics & Training, LLC (hereafter IAT). https://goo.gl/6SCYwS.

- *Using AWS in the context of Singapore Privacy Considerations*, December 2016, Amazon Web Services. https://goo.gl/EkiccR.
- Guía de Seguridad de las TIC CCN-STIC 804, editado por el Centro Criptológico Nacional, 2017, Gobierno de España. https://goo.gl/zii4Q7.
- Adquisición de servicios en la nube: prácticas recomendadas para los clientes del sector público, Amazon Web Services, Inc. (AWS), 2017.
- *THE PHILIPPINE GOVERNMENT'S CLOUD FIRST POLICY*, DEPARTMENT CIRCULAR NO. 2017 -002, de january 2017, Department of Information and Communications Technology, Republic of the Philippines. https://goo.gl/AoRFCL.