Anexo N° 14
Sobre los "Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano"

La plataforma ***cloud*** que soporte la solución (es decir el "***Proveedor de servicios nube - PSN***") deberá cumplir con los "***Lineamientos para el Uso de Servicios en la Nube para entidades de la Administración Pública del Estado Peruano***" (establecidos mediante ***Resolución de Secretaría de Gobierno Digital Nº 001-2018-PCM/SEGDI***) en lo referente a:

1. Todas las condiciones exigidas en el presente documento son de obligatorio cumplimiento tanto para el contratista como para los proveedores terceros subcontratados por éste.

2. La solución brindada deberá operar en un esquema de nube pública.

3. Sobre el tipo de infraestructura en el cual se implementará la solución, se aclara que éste deberá ser una plataforma totalmente nube bajo los esquemas ***SaaS*** o ***PaaS***. Asimismo, se precisa que se aceptará propuestas que contemplen componentes ***IaaS*** siempre y cuando se cumplan las condiciones estipuladas en el presente documento (ver apartado "***Requerimientos técnicos de la solución de gestión de procesos***").

4. Para la compresión del presente documento, se manejarán las siguientes definiciones:
    a. 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.
    b. 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.
    c. 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.

5. El contratista deberá hacer entrega de la documentación del "***Proveedor de servicios nube - PSN***" siguiente[1] (ver apartado "***Entregables***"):
    a. Certificación ISO/IEC 27001 y/o
    b. Certificación ISO/IEC 27017 y/o
    c. Certificación ISO/IEC 27018

    La seguridad física de la infraestructura subyacente será validada con base en las certificaciones previamente mencionadas.

[1] En el caso de los certificados ISO, estos deben haber sido emitidos por una organización de auditoría independiente, como: ***Federal Risk and Authorization Management Program*** (***FedRAMP***), entre otros.

Asimismo, tanto el contratista como el "***Proveedor de servicios nube*** - ***PSN***" cumplirán con las políticas, normas de seguridad de la Información, las NTP e ISO que apruebe el Estado Peruano, así como con los convenios y acuerdos internacionales que sobre seguridad de la información el Perú suscribiese o de los que sea parte.

6. El contratista deberá hacer entrega de documentación (evidencia o declaración jurada) del "***Proveedor de servicios nube*** - ***PSN***" que garantice el manejo de los protocolos de cifrado exigidos (ver apartado "***Entregables***"):
    a. AES (128 bits o superior)
    b. TDES (Teclas de doble longitud)
    c. RSA (1024 bits o superior)
    d. ECC (160 bits o superior)

    Asimismo, se aclara que toda la información deberá encontrarse cifrada tanto en tránsito como en reposo en la solución ofertada.

7. Tanto el contratista como "***Proveedor de servicios nube*** - ***PSN***" reconocen que toda información almacenada y/o en tránsito es de propiedad exclusiva del OSIPTEL, y que, en caso de resolverse el contrato de prestación de servicios, la información no permanecerá almacenada, ni será replicada, procesada o copiada por el contratista ni por el "***Proveedor de servicios nube*** - ***PSN***".
    a. 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.
    b. El contratista se compromete a mantener la confidencialidad en el tratamiento de la información, a no divulgar o acceder indebidamente a la información sin la autorización expresa del OSIPTEL, así como dar instrucción al personal que tratará los datos para que mantengan la misma confidencialidad. Este compromiso será evidenciado en un acuerdo de confidencialidad.
    c. La información y los servicios internos involucrados en la prestación del servicio están clasificados en el nivel "Muy Alto" de la seguridad de la Información (Confidencialidad, Integridad y Disponibilidad), lo que significa que un incidente en ellos tiene un impacto muy alto para el OSIPTEL.

8. El contratista y el "***Proveedor de servicios nube*** - ***PSN***" son íntegramente responsables de seleccionar una ubicación geográfica, desde donde opere la solución, garantizando que se permita el cumplimiento de las obligaciones adquiridas contractualmente con las entidades públicas peruanas (como la "***Ley de Protección de Datos Personales***") y se brinde seguridad, óptimo rendimiento y tiempos de respuesta de cara al usuario.

9. Exigencias en materia de protección de datos personales:
    a. El contratista, asume el rol de "***Encargado del Tratamiento***" del OSIPTEL, por tanto, mediante una declaración jurada, acepta conocer y cumplir con las disposiciones emitidas en la ***Ley 29733 – Protección de datos personales***, el ***Decreto Supremo N° 0003-2013-JUS - Reglamento de la Ley Nº 29733***, así como sus normas complementarias (ver apartado "***Entregables***"):
        i. 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".

ii. 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*".

iii. En relación con los puntos antes mencionados, el contratista se compromete a no utilizar los datos de la solución implementada para otra finalidad ajena a la contratada. El contratista debe hacer extensiva esta exigencia al "***Proveedor de servicios nube*** – ***PSN***". La entidad se reserva el derecho de iniciar las acciones legales, contractuales y demás pertinentes si considera que se ha violado este requerimiento.

b. El contratista es responsable de que los elementos y procesos que soportan el presente servicio, ya sean de un "***Proveedor de servicios nube – PSN***" contratado o de una cadena de subcontratación entre ***PSN***'s, cumplen con los requisitos y niveles de seguridad solicitados por el OSIPTEL, garantizando que se evite la alteración, destrucción, pérdida, divulgación, tratamiento o acceso no autorizado de los datos personales.

c. El contratista remitirá un documento "***Cumplimiento de Normativa de Protección de Datos Personales, controles y estándares***" (ver apartado "***Entregables***") donde incluirá información detallada de cómo satisface la regulación en materia de protección de datos personales, controles de acceso a la infraestructura y datos, política de seguridad del OSIPTEL, lineamientos de la nube, trazabilidad y auditabilidad.

d. En caso exista una fuga o compromiso de los datos, el **Encargado del Tratamiento** debe notificar al OSIPTEL de forma inmediata

e. Para el caso de la ejecución de los derechos ARCO, se indica:

i. Se ejecutarán como respuesta a solicitudes trasladadas por los ciudadanos hacia el OSIPTEL.

ii. En caso fuese necesario, el OSIPTEL trasladará dichas solicitudes al contratista a fin de que ejecute las labores pertinentes para atender el pedido del ciudadano. En este caso, se deberán respetar los siguientes plazos (según el tipo de pedido):

1. Información: se atenderá en un plazo no mayor a 2 días calendario;
2. Acceso: se atenderá en un plazo no mayor a 7 días calendarios;
3. Rectificación, Cancelación y Oposición: se atenderá en un plazo no mayor a 3 días calendarios
4. A efectos de la aplicación de los Acuerdos de Nivel de Servicio – ANS; las solicitudes de ejecución de derechos ARCO trasladadas al contratista serán atendidas como "***Petición de cambio***" y, por ente, estarán sujetas a la aplicación de las mismas penalidades.

10. En caso de producirse algún tipo de controversia durante la ejecución del contrato (o a su término, en caso aplicase) el contratista acepta que dicha

controversia sea solucionada dentro del marco regulatorio del estado peruano. Lo mismo para el "***Proveedor de servicios nube*** – ***PSN***" en caso aplicase.

11. El OSIPTEL debe poder recuperar (descargar) la totalidad de sus datos desde la plataforma del "***Proveedor de servicios nube - PSN***" y eliminarlos de la mencionada plataforma en el momento en que lo considere oportuno y sin necesidad de solicitar asistencia/acceso/autorización del contratista o algún tercer ajeno al OSIPTEL.
    a. Asimismo, la información contenida en la plataforma implementada por parte del contratista debe poder ser migrada a otras plataformas o servicios nube de terceros (portabilidad).

12. En relación con los registros de actividad ("registros de auditoria", "registros de eventos" o "*event log*"); la solución ofertada debe disponer de registros de acceso que permitan monitorizar, analizar, investigar y documentar acciones indebidas o no autorizadas, tanto a nivel operativo como de administración
    a. Los registros de actividad deberán permanecer durante toda la duración del servicio, es decir, no se aceptará la depuración o eliminación periódica o cíclica de los registros: todos los registros de actividad deben ser retenidos durante todo el periodo del servicio.
    b. La solución deberá permitir el envío de registros de actividad mediante el protocolo ***SYSLOG***. En el transcurso de la duración del servicio, el OSIPTEL se reserva el derecho de solicitar que los registros de actividad sean enviados a una determinada ubicación/herramienta para los fines que la entidad estime pertinentes; en este escenario, la entidad comunicará oportunamente al contratista los datos de la ubicación/herramienta a la cual deberán remitirse los registros de actividad.
    c. El servicio de nube debe ser auditable y transparente al usuario.

13. Sobre los mecanismos técnicos a usar en la solución implementada:
    a. Los mecanismos de identificación y autenticación para el acceso de los usuarios al servicio deberán gestionarse de acuerdo a lo indicado en el resto del documento: - - Deberá integrarse a un repositorio LDAP y/o Microsoft Active Directory para la gestión de usuarios y roles (ver apartado "Requerimientos técnicos de la solución de gestión de procesos").
    b. Los mecanismos de identificación y autenticación para el acceso de los administradores deberán gestionarse de acuerdo a lo indicado en el resto del documento: Deberá integrarse a un repositorio LDAP y/o Microsoft Active Directory para la gestión de usuarios y roles (ver apartado "Requerimientos técnicos de la solución de gestión de procesos ").
    c. Los mecanismos de protección de la autenticidad del servidor deberán gestionarse de acuerdo a lo indicado en el resto del documento: Deberá integrarse a un repositorio LDAP y/o Microsoft Active Directory para la gestión de usuarios y roles (ver apartado "Requerimientos técnicos de la solución de gestión de procesos ").
    d. Los mecanismos de protección de la confidencialidad y la integridad de la información que se transfiera través de redes fuera del absoluto control de las partes será según lo indicado en el presente documento: toda la información deberá encontrarse cifrada tanto en tránsito como en reposo en la solución ofertada.

14. Durante la operación (ejecución) del servicio se deberán respetar las siguientes exigencias:

a. Respecto a las características de escalabilidad y elasticidad que pueda brindar la plataforma nube ofertada se indica que en el presente documento se ha pretendido brindar la información pertinente para que los postores puedan realizar un dimensionamiento adecuado de las capacidades necesarias para el cumplimiento del servicio, por lo cual es responsabilidad del contratista y del "***Proveedor de servicios nube*** - ***PSN***" contar con los recursos técnicos, tecnológicos, logísticos, humanos y demás que sean necesarios para asegurar la continuidad del servicio y el cumplimiento de los niveles de servicio exigidos en el presente.
b. Respecto al respaldo y recuperación de datos durante la ejecución del servicio, el contratista deberá presentar un "***Procedimiento de Respaldo de Información***" (ver apartado "***Entregables***") el cual contemplará, como mínimo, lo siguiente:
    i. El alcance de los respaldos de información deberá ser toda la solución implementada.
    ii. La política de respaldos de información (la cual debe respetar lo exigido en el presente documento).
    iii. El mecanismo mediante el cual se cifrarán los respaldos de información.
    iv. El procedimiento para solicitar la restauración de un respaldo de información.
    v. Las exigencias establecidas en el presente documento:
        1. Las tareas de ejecución de respaldos de información deberán realizarse, como mínimo, una vez por día.
        2. Las tareas de ejecución de respaldos de información no deben mermar el rendimiento de la solución de cara a los usuarios.
        3. Los respaldos de información deberán almacenarse en la misma plataforma ***cloud*** desde donde opera el resto de la solución.
        4. El periodo de retención de los respaldos de información será por toda la duración del servicio.
        5. La institución se reserva el derecho de solicitar al contratista el restablecimiento de algún respaldo de información con motivos de validación (para validar la correcta operación del servicio de respaldo).
c. Respecto al cumplimiento de la legalidad y normativa durante la ejecución del servicio, el OSIPTEL se reserva el derecho de realizar las supervisiones, validaciones y/o auditorias que estime conveniente a fin de asegurar que se cumple con la normativa vigente y exigida.
    i. Tanto el contratista como el "***Proveedor de servicios nube*** - ***PSN***" se comprometen a facultar que un tercero independiente audite la seguridad de la empresa proveedora del servicio de nube.
d. Respecto a la continuidad del servicio
    i. El contratista deberá presentar evidencia de la existencia de un plan de continuidad y recuperación ante desastres por parte suya y/o del "***Proveedor de servicios nube*** - ***PSN***" y que dicho plan contempla medidas (como tiempos de recuperación) que hacen posible el cumplimiento de lo estipulado en el presente documento (ver apartado "***Entregables***").
    ii. El contratista deberá presentar un "***Procedimiento de Coordinación ante Desastres***" (ver apartado "***Entregables***") el cual contenga, como mínimo, los flujos de información y las interacciones con el OSIPTEL durante la gestión de desastres, la

remisión de un informe detallado de la incidencia, la realización de pruebas que involucren los componentes contratados por la entidad e información del Análisis de Impacto de Negocio (del inglés ***Business Impact Analysis*** - ***BIA***).

iii. El contratista deberá presentar un "***Informe de afectaciones a la continuidad del servicio***", en el periodo de tiempo correspondiente, junto a los Entregables 06, 08, 11, 13, 14 y 15 (ver apartado "***Entregables***"). El mencionado informe deberá detallar los eventos que han afectado la continuidad de la plataforma ofertada en el periodo de tiempo correspondiente.

iv. El contratista deberá realizar pruebas periódicas que involucren al OSIPTEL 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. Estas pruebas deberás ejecutarse, como mínimo, una vez por año.

v. El contratista deberá brindar información del Análisis de Impacto de Negocio (BIA por sus siglas en inglés) (ver apartado "***Entregables***").

vi. Finalmente, el proveedor deberá evaluar el impacto de los cambios realizados por sus actividades (ya sean por actualización, mantenimiento u otros), para lo cual deberá presentar un informe con los resultados de la evaluación (ver apartado "***Entregables***").

e. Respecto a la gestión de incidentes durante el servicio, el contratista deberá presentar un "***Procedimiento de Gestión de Incidentes***" (ver apartado "***Entregables***"), el cual contenga, como mínimo, los siguiente:

i. Procedimiento para la notificación de incidentes.

ii. Tipología de incidentes incluidos en el servicio (en este punto se debe considera el cumplimiento de lo estipulado en el ***ANS - Atenciones***).

iii. Procedimientos específicos en el caso de incidentes de seguridad.

iv. Tiempos de respuesta y resolución de incidentes (en este punto se debe considera el cumplimiento de lo estipulado en el ***ANS - Atenciones***).

v. Mantenimiento y gestión del registro de incidentes.

f. Respecto a la gestión de cambios durante el servicio, el contratista deberá presentar un "***Procedimiento de Coordinación de Mantenimientos***" (ver apartado "***Entregables***"), el cual contenga, como mínimo, lo siguiente:

i. Los plazos para notificar a la entidad de la ejecución de labores de mantenimiento (notificaciones previas y posteriores a la ejecución).

ii. Políticas y estándares del cambio, de tal manera que se asegure el correcto funcionamiento del servicio.

iii. Requerimientos de cumplimiento regulatorio (los cambios realizados deben mantener el respeto a toda la normativa vigente y a lo estipulado en el presente documento).

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

v. Cronograma de cambios (en caso las labores de mantenimiento pudiesen ser programadas con anticipación).

g. Asimismo, durante la ejecución del servicio se deberán respetar los ***Acuerdos de Nivel de Servicio*** - ***ANS*** señalados en el apartado "Acuerdos de Nivel de Servicios" de los términos de referencia.
h. El contratista y el "***Proveedor de servicios nube*** - ***PSN***" se comprometen a brindar el servicio de nube de forma eficiente, transparente, segura, de acuerdo con lo establecido en los ANS.

15. Sobre los Interlocutores responsables durante la ejecución del servicio; el OSIPTEL y el contratista definirán contactos a cargo de una serie de roles que permitan una comunicación fluida entre ambas partes en lo relacionado a temas críticos para la adecuada ejecución del servicio.
    a. Se deberán definir, como mínimo, los siguientes roles:
        i. Área/Equipo/Funcionario responsable de la seguridad.
            1. Por parte de la entidad, este rol será asumido por el Oficial de Seguridad de la Información.
        ii. Área/Equipo/Funcionario de contacto para incidentes de seguridad.
            1. Por parte de la entidad, este rol será asumido por el Oficial de Seguridad de la Información.
        iii. Área/Equipo/Funcionario de contacto para cambios y mantenimiento de sistemas.
            1. Por parte de la entidad, este rol será asumido por la Oficina de Tecnologías de la Información – OTI.
        iv. Área/Equipo/Funcionario de contacto para incidencias relativas a los indicadores de servicio (Acuerdos de nivel de servicio - ANS).
            1. Por parte de la entidad, este rol será asumido por la Oficina de Tecnologías de la Información – OTI y/o la Secretaria Técnica de Solución de Reclamos – STSR, según corresponda.
        v. Área/Equipo/Funcionario de contacto para aspectos contractuales.
            1. Por parte de la entidad, este rol será asumido por la Oficina de Administración y Finanzas – OAF.
        vi. Área/Equipo/Funcionario de contacto para temas jurídicos y regulatorios, en particular en lo relativo a datos de carácter personal.
            1. Por parte de la entidad, este rol será asumido por la Secretaria Técnica de Solución de Reclamos – STSR.
    b. Los datos de contacto del personal para estos roles por parte del OSIPTEL le serán entregados al postor ganador de la Buena Pro de forma posterior a la firma de contrato.
    c. Los datos de contacto (como mínimo: nombre completo, dirección de correo electrónico, numero de contacto) del personal de contacto para estos roles por parte del contratista deberá encontrarse en la "***Ficha de contactos***".

16. A fin de garantizar un adecuado seguimiento a los niveles de seguridad del servicio, el contratista deberá presentar los informes de auditoría y no conformidades de aplicación para verificar las medidas de seguridad empleadas por este. Estos informes deberán ser presentados (conteniendo la información del periodo de tiempo correspondiente) junto a los Entregables 06, 08, 11, 13, 14 y 15 (ver apartado "***Entregables***").

17. A la finalización del servicio, se deberán respetar las siguientes exigencias:

a. Al término del contrato (y de forma previa a este evento), tanto el contratista como el "***Proveedor de servicios nube*** - ***PSN***" se comprometen a no ejecutar ningún tipo de actividad que pudiese alterar la operación de los servicios implementados como parte del presente contrato. Asimismo, en caso de forma previa al término del contrato se hubiese adjudicado a un nuevo contratista para la gestión del servicio o la institución hubiese determinado que lo administrará con sus propios recursos, el contratista y el "***Proveedor de servicios nube*** - ***PSN***" brindarán todas las facilidades técnicas y documentales para el traspaso de la gestión; en este último supuesto, el OSIPTEL comunicará de forma oportuna al contratista que se debe iniciar el proceso de transferencia de gestión/información.
    i. De forma previa a la finalización del contrato, se deberán seguir las siguientes pautas:
        1. 30 (treinta) días calendario previos a la finalización del contrato o cuando OSIPTEL lo solicite:
            a. En caso de haberse adjudicado a un nuevo contratista la gestión del servicio:
                i. El contratista deberá realizar la transferencia de toda la documentación de gestión que resulte necesaria para que el nuevo contratista se haga cargo de la administración del servicio; esto incluye la participación en las reuniones de coordinación y traspaso de información.
                ii. El contratista deberá generar y/o transferir todas las credenciales de acceso y/o administración que resulten necesarias para que el nuevo contratista pueda asumir la gestión de la solución implementada.
                iii. El contratista deberá acompañar las pruebas de validación que resulten necesarias a fin de verificar que el nuevo contratista cuenta con todo lo necesario para continuar con la gestión de la solución implementada.
            b. En caso la institución haya decidido migrar el servicio a su propia infraestructura:
                i. El contratista deberá entregar todos los respaldos de información que la entidad solicite a fin de poder replicar la solución en su propia infraestructura.
                ii. Luego de que la entidad disponga de la información que haya estimado pertinente y haya logrado replicar los servicios en su propia infraestructura, solicitará al contratista la eliminación total de toda información relacionada a la entidad, así como también de toda configuración relacionada a la implementación realizada. El contratista deberá llevar a cabo esta eliminación y presentar evidencia de dicha labor.
        2. 05 (cinco) días calendarios previos a la finalización del contrato:

a. El contratista, con supervisión de personal de la institución, deberá eliminar todas las credenciales de acceso y gestión que correspondan a su personal, asimismo, deberá entregar las credenciales de administración de la plataforma (los super-usuarios o usuarios administradores) a la entidad o al nuevo contratista, según corresponda.

b. En caso de una finalización abrupta del contrato [2] (antes del periodo de duración establecido), el contratista y el "***Proveedor de servicios nube*** - ***PSN***" se comprometen a que la solución implementada (hasta el momento de la finalización abrupta) permanecerá accesible y operativa por un periodo mínimo de 90 días calendarios contados desde el día siguiente de la formalización de la finalización abrupta del contrato.
    i. Durante este periodo de tiempo no se exigirá al contratista que brinde soporte, mantenimiento, atención de incidentes, atención de requerimientos o algún otro tipo de pedido sobre la plataforma.
    ii. Durante este periodo de tiempo el contratista no deberá acceder a la plataforma implementada ni modificar/alterar de forma alguna la operación de esta; caso contrario, se interpretará el hecho como un intento de sabotaje y se iniciarán las acciones legales pertinentes. Este último escenario no aplica si el acceso/modificación a la plataforma es realizada por el contratista bajo pedido expreso del OSIPTEL.

c. El OSIPTEL debe poder solicitar la eliminación (total o parcial) de su información contenida en la plataforma del "***Proveedor de servicios nube*** – ***PSN***", y este último no debe conservar ningún tipo de copia o respaldo de la información de la institución; es decir, la eliminación debe ser total.
    i. Esto debe respetarse tanto al término del contrato (sea este de forma programada o abrupta) como bajo pedido de la institución en cualquier momento de la contratación.
    ii. La eliminación total de la información de la institución deberá culminarse en un periodo no mayor de 72 horas desde la realización del pedido expreso por parte de la entidad.
    iii. El OSIPTEL se reserva el derecho de realizar las validaciones que estime pertinentes a fin de asegurar que su información ha sido eliminada de la plataforma del "***Proveedor de servicios nube*** - ***PSN***".

d. El contratista deberá presentar un "***Procedimiento de Recuperación de Información***" (ver apartado "***Entregables***") en el cual se detalle el protocolo a seguir en caso el OSIPTEL solicite recuperar su información desde la plataforma nube implementada.

e. El contratista deberá presentar un "***Procedimiento de Eliminación de Información***" (ver apartado "***Entregables***") en el cual se detalle el protocolo a seguir en caso el OSIPTEL solicite la eliminación de su información de la plataforma nube implementada. Este procedimiento debe contemplar, como mínimo, la eliminación total o parcial de la

[2] Es pertinente mencionar que un contrato puede finalizar, entre otros, por alguno de los siguientes motivos:
- 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.

información del OSIPTEL, el mecanismo de borrado y los tiempos para la destrucción de la información.