CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 823

UTILIZACIÓN DE SERVICIOS EN LA NUBE

SEPTIEMBRE 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.09.08 16:19:24 +02'00'

NIPO: 083-19-265-8

Fecha de Edición: diciembre de 2019
Instituto CIES ha participado en la realización y modificación del presente documento y sus anexos.

ÍNDICE

1. INTRODUCCIÓN

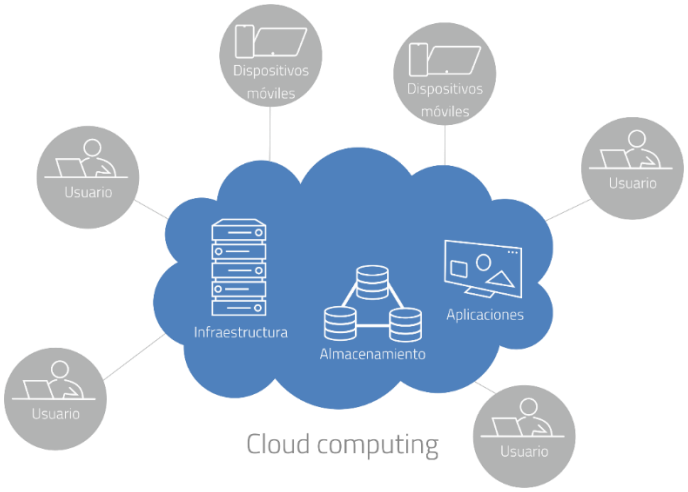
1.1 CONCEPTOS PREVIOS

1. En la actualidad el acceso a servicios a través de Internet se ha incrementado exponencialmente. Este hecho, así como la heterogeneidad de los dispositivos que dan acceso a estos servicios, ha supuesto un auge en el uso de las tecnologías web como un estándar.

2. La migración a entornos web, el uso de aplicaciones móviles y la introducción de dispositivos IoT han sido 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 una gran cantidad de servicios en red de forma ágil y flexible, con grandes posibilidades de escalabilidad y reduciendo al mínimo los tiempos de despliegue.

3. Los servicios en la nube consisten en la disposición de software, plataformas o infraestructuras por parte de un proveedor (CSP, Cloud Service Provider) 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.

4. Los sistemas “on premise” tradicionales ya no están tan aislados como en el pasado presentando una mayor superficie de exposición y difuminando el perímetro de la red. El uso de la nube permite utilizar tecnologías diseñadas específicamente para responder a necesidades de externalización introduciendo nuevas arquitecturas y paradigmas de seguridad, por lo que constituyen cada vez más una alternativa segura para procesar y almacenar datos.



5. La provisión de servicios en la nube es un modelo que permite 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 y gracias a la automatización en la gestión de los servicios, permiten una interacción con el proveedor de servicio mínima.

6. El modelo de servicios en la nube ofrece a las organizaciones grandes beneficios como pueden ser la deslocalización, la alta disponibilidad, el acceso a información desde cualquier lugar, la baja latencia, la flexibilidad en asignación de recursos y un ahorro económico significativo, además de facilitar nuevos modelos de producción como el teletrabajo, la telemedicina o el uso extendido del internet de las cosas.

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

8. Esta guía persigue recoger los aspectos que deberían de contemplarse para la adopción de la nube como paradigma tecnológico para la disposición de servicios con unas garantías de seguridad adecuadas, acordes con el Esquema Nacional de Seguridad (ENS).

1.2 CARACTERÍSTICAS DE LOS SERVICIOS EN LA NUBE

9. La característica principal de la nube es la accesibilidad de la información. Este modelo, unido a la capacidad de despliegue automático de servicios en cuestión de segundos a nivel global, facilita el acceso a la información por parte de los usuarios, con independencia del lugar o el tipo de dispositivo que se emplee: basta tener acceso a la red, aunque el uso de este paradigma implica habitualmente la necesidad de disponer de conexiones con una capacidad significativa.

10. Otra de las características que hacen de la nube un área en expansión es el ahorro económico. Generalmente el modelo de servicios en la nube permite reducir costes a la organización con respecto al modelo de servicio y alojamiento tradicional. Esto es debido al ahorro de recursos dedicados internamente a hardware, mantenimiento, personal dedicado, suministros, espacio e instalaciones, y también debido al uso de economías de escala en los servicios en la nube, donde cuanto mayor es la necesidad de recursos para proporcionar el servicio, menor será el coste de estos recursos.

11. Además, con el servicio en la nube, se permite a un cliente asumir los costes 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.

12. Por otro lado, los servicios en la nube se caracterizan por la deslocalización de datos, donde la principal ventaja es que el cliente puede decidir la geolocalización de la información y permite llevar los datos y los procesos al lugar más conveniente para la organización, además de mantener el control de acceso estén donde estén los datos.

13. De esta forma se pueden mantener copias del servidor repartidas en distintos puntos del planeta tanto para mejorar los tiempos de acceso y reducir la latencia al mínimo, como para evitar pérdidas de datos o servicios por la caída de un centro de proceso, manteniendo alta disponibilidad y durabilidad. Esta deslocalización tiene implicaciones de seguridad que las organizaciones deben evaluar convenientemente antes de hacer uso de los servicios en la nube, como la aplicación de legislaciones regionales sobre los datos o la baja disponibilidad de la infraestructura de red en la región, y deben aplicar medidas de seguridad y configuraciones adecuadas a cada escenario.

14. Por su parte, para los servicios en la nube se identifican cinco (5) características esenciales:

    - **Auto-servicio 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, tabletas, portátiles, equipos personales, servidores, etc.
    - **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.) y mantienen el control de acceso a sus recursos.
    - **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 auditado, proporcionando una gran transparencia tanto para el proveedor como para el consumidor del servicio utilizado.

15. Por último, cabe destacar la posible dependencia de terceros en los 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, etc.

16. Si bien esto es considerado generalmente como una ventaja, debe tenerse en cuenta que esta característica de externalización 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 el organismo contratante.

17. A la hora de contratar servicios en la nube 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 organización cliente, además de establecer medidas adecuadas de monitorización y vigilancia.

1.3 MODELOS DE DESPLIEGUE

18. Ante el abanico de despliegues posibles a la hora de crear un entorno de servicios en la nube, se pueden clasificar las infraestructuras en públicas, privadas, comunitarias o híbridas.

- **Nube pública.** La infraestructura de esta nube está mantenida y gestionada por terceras personas no vinculadas con la organización proporcionando recursos de forma abierta a entidades heterogéneas, sin más que un contrato con el mismo proveedor que controla dicha infraestructura.
- **Nube privada.** La infraestructura de esta nube o servicios provistos son completamente dedicados para un solo cliente que controla qué aplicaciones debe ejecutarse y dónde (infraestructura bajo demanda). Puede ser propiedad, ser administrado y operado por la organización, un tercero o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones.

  La *nube pública* presenta flexibilidad de contratación y la *nube privada*, en la mayoría de los casos, exige determinados compromisos de consumo o permanencia.
- **Nube híbrida.** Los servicios se ofrecen de forma pública y privada. Un usuario es propietario de unas partes y comparte otras, aunque de una manera controlada.
- **Nube comunitaria.** La infraestructura de esta nube o servicios provistos son compartidos en comunidad cerrada por varias organizaciones relacionadas entre ellas y que comparten requisitos con la finalidad de servir a una función o propósito común (seguridad, política, …).

  La *nube comunitaria* puede ser propiedad, administrada y operada por una o más de las organizaciones de la comunidad, un tercero o alguna combinación de ellas, y puede existir dentro o fuera de las instalaciones.

1.4 CATEGORÍAS DE SERVICIO

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

- **IaaS (Infrastructure as a Service).** Se encarga de entregar una infraestructura al usuario, proporcionando recursos de procesamiento y

almacenamiento a través de la red, sin ningún otro valor añadido (servicios de uso de almacenamiento, hardware, servidores y componentes de red).

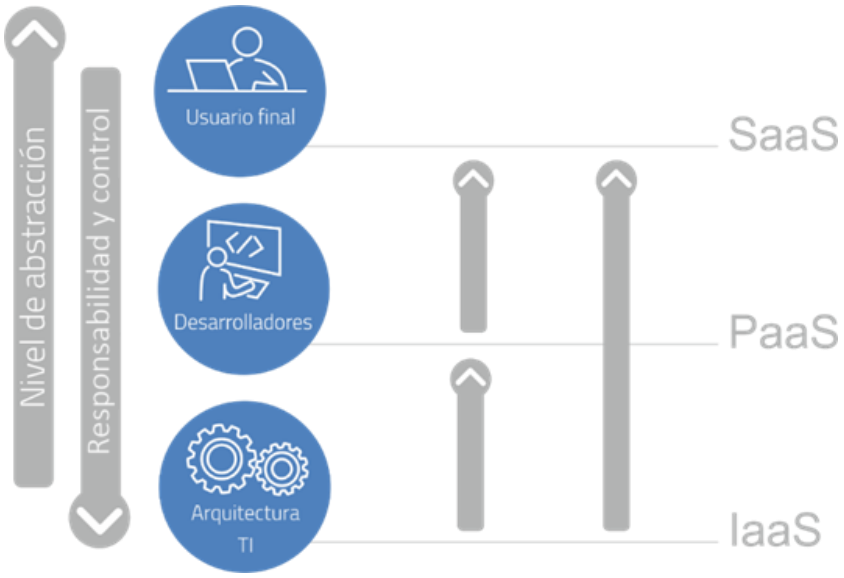
El proveedor se encarga de la administración de la infraestructura y el cliente tiene el control sobre los sistemas operativos, almacenamiento y aplicaciones desplegadas, así como el control de los componentes de red.

- **PaaS (Platform as a Service).** 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.

  Se proporcionan herramientas y utilidades para desarrollar aplicaciones sobre la nube como bases de datos o entornos de programación en las que el usuario puede desarrollar sus propias soluciones.

- **SaaS (Software as a Service).** Modelo de distribución de software en el que las aplicaciones están alojadas por un proveedor de servicio y puestas a disposición de los usuarios a través de red.

  El usuario encuentra en la nube las herramientas con las que puede implementar los procesos necesarios: aplicaciones ofimáticas, correo electrónico, etc… donde el cliente no administra ni controla la infraestructura en que se basa el servicio que utiliza.



1.5 RIESGOS DERIVADOS DE LOS SERVICOS EN LA NUBE

20. La adopción de servicios en la nube como estrategia para soportar servicios de tecnologías de la información y la comunicación (TIC) ofrecidos por distintos organismos introduce un amplio número de ventajas para éstos, como la reducción de costes o la flexibilidad en la incorporación de nuevos recursos.

21. Sin embargo, la adopción de este nuevo paradigma tecnológico introduce nuevos riesgos que es necesario controlar para poder prestar un servicio que garantice los requisitos exigibles por los marcos legales, como el ENS o la normativa vigente en materia de protección de datos personales, así como por los requisitos de seguridad que en cada caso las organizaciones establezcan como necesarios.

    - **Pérdida de control.** El cliente transfiere el control al proveedor de servicios.
    - **Ubicación de los datos.** Es necesario acordar con el proveedor para que el procesamiento de los datos esté sujeto al marco legal del país.
    - **Cumplimiento normativo.** Seguridad e integridad de los datos.
    - **Aislamiento de datos.** El cliente transfiere el control al proveedor de servicios.
    - **Portabilidad y viabilidad a largo plazo.** Implicaciones en la migración de datos.
    - **Acceso de usuarios con privilegios.** Acordado con el proveedor para usuarios de soporte.
    - **Recuperación.** Política de recuperación de datos en caso de desastre.
    - **Monitorización.** La monitorización y vigilancia son actividades muy dependientes de los mecanismos ofrecidos por el proveedor de servicios.

22. En línea con lo anterior, el cumplimiento de requisitos de seguridad y el modo de afrontar dicho cumplimiento legal o normativo difiere en función de que la infraestructura en la nube sea propiedad y esté administrada por un tercero o lo esté por el propio organismo.

23. En el supuesto de que sea el organismo el propietario 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 deberá cumplir los requisitos establecidos en la normativa de seguridad que sea de aplicación en lo que respecta a prestadores de servicios.

24. En cualquier caso, la responsabilidad del cumplimiento del ENS 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 el organismo propietario de la información, con independencia de la existencia de acuerdos, seguros u otras medidas compensatorias o complementarias de vigilancia.

25. Esta guía centra su contenido en identificar los requisitos que un organismo debería considerar para cumplir el ENS garantizando la seguridad tanto de la información como de los servicios proporcionados a través de la nube.

2. REQUISITOS DE SEGURIDAD

2.1 PRIMEROS PASOS

26. El organismo categorizará el sistema soportado por la solución en la nube según el ANEXO I del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

    Para ello se llevarán a cabo las siguientes acciones:

    - **Determinación de los niveles de seguridad (BAJO, MEDIO, ALTO, SIN VALORAR)** requeridos para cada una de las dimensiones de seguridad, Disponibilidad [D], Autenticidad [A], Integridad [I], Confidencialidad [C], Trazabilidad [T] de los servicios e Información proporcionados a través de la nube, mediante la determinación del impacto que tendría, sobre el organismo un incidente que afectara a la seguridad de la información o de los sistemas.

      Valoración que será realizada y aprobada formalmente por los respectivos Responsables de Servicios e Información.

    - **Determinación de la categoría del sistema (BÁSICA, MEDIA y ALTA) que soporta los servicios y la información proporcionados por la nube**, en función de la valoración máxima obtenida en alguna de las dimensiones. El responsable de su realización y aprobación formal será el Responsable del Sistema.

    - **Elaboración de la declaración de aplicabilidad**, mediante la selección de las medidas de seguridad del ANEXO II del Real Decreto 3/2010, de acuerdo a los valores máximos de seguridad obtenidos en cada una de las dimensiones de seguridad y/o de acuerdo a la categoría del sistema, según sea el caso.

      Este documento debe ser aprobado formalmente por el Responsable de Seguridad.

    - **Realización de un análisis de los riesgos**, a los que están expuestos los servicios y la información soportada por la nube. Si como resultado se requiere la implantación de medidas adicionales a las ya identificadas, estas se añadirán a la declaración de aplicabilidad.

- **Acogerse a un Perfil de Cumplimiento Específico**, en caso de que la nube disponga de un perfil aprobado por el Centro Criptológico Nacional, el organismo podrá acogerse a éste, siendo entonces de aplicación la declaración de aplicabilidad asociada a este perfil en concreto, su adopción deberá estar argumentada formalmente.

27. La categoría del sistema que soportan los servicios en la nube, así como las medidas adicionales que se consideren de aplicación, se propagarán a los elementos que lo componen, sean propios del organismo, sean de un CSP contratado, o sean de una cadena de subcontratación entre CSP.

2.2 CONSIDERACIONES PARA IMPLEMENTAR SEGURIDAD

28. A continuación, se analizarán las medidas de seguridad del marco organizativo, marco operacional y las medidas de protección del Anexo II del Real Decreto 3/2010.

2.2.1 Aspectos organizativos

29. El organismo dispondrá de una **política de seguridad** conocida por toda la organización, donde describirá los mecanismos implementados para la gestión continuada de la seguridad y donde también establecerá los responsables de velar por su cumplimiento. La solución en la nube deberá ser acorde a esta política.

30. La utilización de una solución en la nube requerirá una **normativa de seguridad** específica para comunicar a los usuarios del servicio los criterios de uso aceptable, como mínimo contendrá los siguientes aspectos:

- 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.).

31. También será necesario documentar los **procedimientos de seguridad**, que identifiquen las tareas a realizar, así como los responsables de su realización, relacionados según sea el caso, con:

- IaaS: los sistemas operativos, almacenamiento, aplicaciones desplegadas y componentes de red virtualizados.
- PaaS: las aplicaciones instaladas y su configuración.

- SaaS: la configuración y parametrización de la/s aplicación/es como servicio.

32. En la medida de que se tenga capacidad para la introducción de nuevos elementos en el sistema en la nube, esta acción requerirá de la definición e implantación en el organismo de un **proceso formal de autorización**, para la entrada de estos componentes en el sistema, siendo necesario la identificación de la responsabilidad de cada parte (organismo/CSP).

2.2.2 Aspectos operacionales de seguridad

2.2.2.1 Planificación del sistema

33. Para la realización del **análisis riesgos**, el organismo reflejará los activos en función de la modalidad de nube:

    - En el caso de un servicio SaaS, la solución en la nube se reflejará como un activo de "servicios externos", del que dependerán los servicios e información soportados por esta.
    - En el caso de un servicio PaaS y IaaS, se reflejarán los activos sobre los que se tiene control.

34. En el caso de que la provisión de los servicios se realice desde una nube privada "on premise", el organismo reflejará en el análisis de riesgos todos los activos involucrados en la prestación de los servicios.

35. Este mismo criterio se seguirá, para detallar los elementos (equipos, redes, cortafuegos, etc.) que definen la **arquitectura de seguridad**.

36. En la medida de que el organismo tenga capacidad para ello, el proceso de **adquisición de nuevos componentes** para el sistema que se encuentra en la nube, requerirá de un análisis para comprobar si estos son coherentes con la arquitectura de seguridad definida, si se tiene en cuenta los riesgos a los que está expuesto el sistema y las necesidades técnicas, de formación y de financiación.

37. Para el estudio de **dimensionamiento y la capacidad** necesaria, ante de poner en explotación cualquier nuevo elemento se tendrán en cuenta, en función de la modalidad de la nube, los siguientes aspectos:

    - En el caso de un servicio SaaS, la medida de la capacidad del servicio vendrá determinada por el propio proveedor, pudiendo estar basada en número de registros, instancias del software, número de usuarios concurrentes o cualquier otra medida generalmente referida a las funcionalidades del software contratadas.

      Sea cual sea el baremo para determinar la capacidad del servicio contratado, ésta deberá figurar expresamente en el acuerdo, así como las medidas de penalización a adoptar en el caso de que los parámetros de capacidad no se cumplan.

- En el caso de un servicio PaaS y IaaS es más frecuente medir la capacidad del servicio en términos de ciclos de CPU, tiempo de uso, datos transferidos, ancho de banda o capacidad de almacenamiento en disco, llegando en el caso de IaaS incluso a poder requerir las características del hardware contratado: tamaño de disco, memoria RAM, tipo de procesador, CPU o transferencia de datos. Se debe asegurar la existencia de servicios que permitan monitorizar el uso de estas capacidades.

38. En cualquier caso y con independencia de la forma de medir la capacidad del servicio, es necesario especificar las condiciones bajo las que se podrá modificar la capacidad contratada, ya sea para aumentarla o reducirla, incluso en tiempo real según la demanda de cada momento.

    El organismo definirá y reflejará convenientemente unos valores máximos y mínimos entre los cuales la asignación de recursos se haga de forma automática o semiautomática, sin necesidad de modificaciones sustanciales en los acuerdos de servicio con el proveedor.

39. Por último, el CSP proporcionará herramientas u otros recursos que permitan al organismo medir la capacidad del servicio y su rendimiento, de forma que se tengan datos fiables para garantizar que ante subidas o bajadas de carga la plataforma ha seguido trabajando con valores acordes a los servicios contratados.

2.2.2.2 Control de acceso

40. Cuando el organismo se haya acogido a un Perfil de Cumplimiento Específico, para la configuración de las medidas relativas al **control de acceso** a los recursos se seguirán las pautas descritas en las guías de configuración asociadas al perfil de aplicación.

2.2.2.3 Explotación

41. Para el mantenimiento del **inventario de activos**, se tendrá en cuenta, en función de la modalidad de nube que:

    - En el caso de un servicio SaaS, la solución en la nube se reflejará como un activo de “servicios externos”.
    - En el caso de servicios PaaS y IaaS, se reflejarán los activos sobre los que se tienen control. Pudiéndose hacer uso de las herramientas de inventario que proporcione el proveedor para complementar su propio inventario.

42. En el caso de que la provisión de los servicios se realice desde una nube privada “on premise”, el organismo reflejará en el inventario todos los activos involucrados en la prestación de los servicios.

43. Para la **configuración de seguridad** (bastionado) del equipamiento, en caso de que el organismo se haya acogido a un Perfil de Cumplimiento Específico se seguirán las pautas recogidas en las guías de configuración del perfil de aplicación.

44. Para la realización de las tareas **mantenimiento** y la **gestión de los cambios**, el organismo definirá las responsabilidades y protocolos de actuación con el CSP, previniendo de este modo paradas o errores imprevistos, que pudieran afectar a la prestación de los servicios.

45. El organismo dispondrá de un procedimiento integral para la **gestión y registro de incidentes de seguridad**, que tenga en cuenta también las obligaciones impuestas por la normativa de protección de datos.

    A este respecto, serán de aplicación respectivamente la "**Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad**[1]**"**, aprobada por Resolución, de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, donde se establece que las Administraciones Públicas notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información y el **artículo 33 "Notificación de una violación de la seguridad de los datos personales a la autoridad de control"** del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

46. Este procedimiento, incluirá los flujos de información que se hayan establecido con el CSP para garantizar la fluidez en las comunicaciones y el cumplimiento de los plazos establecidos en la gestión del incidente.

47. El organismo tendrá en cuenta que el CSP dispone de **registros de actividad de los usuarios** que permiten monitorizar, analizar, investigar y documentar acciones indebidas o no autorizadas, tanto a nivel operativo como de administración. Por tanto, se establecerá con el CSP la responsabilidad sobre los registros de actividad, estableciendo obligaciones en cuanto a su configuración, la consolidación periódica de datos, la retención de los registros y respecto a los mecanismos implementados para la **protección de los registros de actividad**.

    En caso de que el organismo se haya acogido a un Perfil de Cumplimiento Específico, se atenderá a lo establecido a este respecto, en la Guía de configuración del perfil de aplicación.

48. En caso de conservar claves criptográficas en la infraestructura del CSP, este pondrá en conocimiento del organismo las medidas implementadas para **proteger las claves criptográficas** durante todo su ciclo de vida (generación,

[1] Establece los criterios y procedimientos para la notificación por parte de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público al Centro Criptológico Nacional (CCN) de aquellos incidentes que tengan un impacto significativo en la seguridad de la información que manejan y los servicios que prestan en relación con la categoría del sistema, al objeto de poder dar adecuada respuesta al mandato del Capítulo VII, Respuesta a incidentes de seguridad, del Real Decreto 3/2010, de 8 de enero.

transporte, custodia, retirada y destrucción). En caso contrario, será responsabilidad del cliente su custodia y protección.

2.2.2.4 Contratación un proveedor de servicios en la nube

49. Para la contratación de un CSP, el organismo establecerá una serie de **condiciones contractuales** en la prestación del servicio, relativos a las características del servicio a proporcionar, las responsabilidades de ambas partes.

    A su vez se establecerán "acuerdos de nivel de servicio" para definir la calidad del servicio contratado, así como los mecanismos que se establecerán para su medición.

50. Además, se tendrá en cuenta la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, por la que se regulan los procedimientos de contratación de las Administraciones Públicas.

    Los servicios en la nube se encuentran dentro de la tipología de los contratos de servicio, de acuerdo con el artículo 17 de la citada Ley. Otros aspectos necesarios regulados por dicha Ley serían los relativos a la confidencialidad de la información de los licitadores, así como la de los organismos regulado en el artículo 133 y en qué condiciones el contratista adquiere la condición de encargado del tratamiento, regulado en la disposición adicional vigésimo quinta.

51. Así mismo, se tiene la obligación de requerir al CSP que provea sistemas que dispongan de la conformidad con el ENS, en la categoría alcanzada por los servicios a proporcionar a través de esta nube. Esta obligación se recoge en la "Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad", aprobada por Resolución, de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas.

52. **Estos aspectos, como norma general, se regularán con carácter previo a la contratación, en los pliegos y/o peticiones de ofertas**. Al menos se tendrán en cuenta los siguientes:

    - **Descripción del Servicio**: descripción detallada del servicio que el proveedor va a proporcionar, incluyendo los acuerdos de nivel de servicio y todas las especificaciones del mismo.
    - **Tipo de servicio e infraestructura**: el tipo de servicio e infraestructura a contratar, de acuerdo a lo especificado en el apartado "1.2 Características de los servicios en la nube".
    - **Dimensionado del servicio**: los recursos que conformarán el servicio, teniendo en cuenta lo establecido en el apartado de "Planificación" de la presente guía.

- **Acuerdos de nivel de servicio**: acordar los niveles de servicio (Service Level Agreement - SLA), que regirán la calidad del servicio contratado, reflejando aspectos relativos a capacidad, disponibilidad, continuidad o relativos a la gestión de incidentes, 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 períodos críticos en los que se requieren mayores niveles de disponibilidad. Se definirán tiempos de recuperación para los sistemas de información acordes a la categoría del sistema requerida al CSP.
  - **Peticiones de cambio e incidentes**: se definirán los tiempos de respuesta y resolución, así como el horario de atención a peticiones de cambio realizadas por la organización cliente o incidentes reportados automática o manualmente.

  De cada SLA, se requerirá la definición de los siguientes aspectos:
  - Parámetro: identificador del SLA.
  - Responsabilidades: quién recoge y facilita los datos necesarios para realizar los cálculos.
  - Fórmula: descripción del cálculo para la obtención del SLA.
  - 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 SLA.

53. Se determinará también la periodicidad de los informes de cumplimiento de los SLA y/o mecanismos proporcionados para su medición.

- **Responsabilidades y obligaciones**: se definirán las responsabilidades involucradas en la prestación del servicio, tanto en la parte del organismo contratante como del CSP: incidentes, gestión de cambios, mantenimiento, etc.
- **Registro de actividad**: se definirán las responsabilidades respecto a los registros de actividad, teniendo en cuenta lo establecido en el apartado de "Explotación" de la presente guía.

- **Gestión de incidentes**: se establecerán los flujos de información y responsables para su gestión, teniendo en cuenta lo establecido en el apartado de "Explotación" de la presente guía.
- **Respaldo y recuperación de datos**: se establecerá la responsabilidad sobre su realización, teniendo en cuenta lo establecido en el apartado de "Medidas de Protección de los activos" de la presente guía.
- **Continuidad del servicio**: se reflejarán las medidas que se implementarán para garantizar la continuidad de las operaciones, teniendo en cuenta lo establecido en el apartado de "Continuidad" de la presente guía.
- **Finalización del contrato**: se regularán aspectos relativos a la devolución de la información, en cuanto al formato de los datos, así como los plazos. O en su defecto, los relativos a la destrucción de la misma, requiriendo evidencias (certificados) de su realización.
- **Información sobre la subcontratación**: se incluirá la obligación de informar sobre las subcontrataciones que se van a realizar y evidenciar como estas cumplen con las obligaciones que le han sido requeridas al organismo con carácter previo a la contratación y que se hacen extensibles, a su vez, a sus proveedores y prestadores de servicios.
- **Requisitos legales**: incluirá aspectos relativos al cumplimiento de obligaciones legales, como:
  - Solicitar la **conformidad con el ENS**, en la categoría alcanzada por los sistemas que soportan los servicios a proporcionar a través de esta nube.
  - **Relativas a la confidencialidad de la información** ya sea de la información a la que va acceder los licitadores antes de la contratación, a la que va acceder el adjudicatario durante la ejecución del contrato, así como la aportada por los licitadores.
  - Relativas al **cumplimiento de la normativa vigente en materia de protección de datos**: RGPD[2] y LOPDGDD[3].
  - Cumplimiento de las obligaciones establecidas por **el "Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones"** que entre otras, establece aspectos relativos a la ubicación en la Unión Europea (UE) de los recursos técnicos utilizados para los sistemas de identificación y firma basados en clave concertada (o similares) o bien en España si estos contienen categorías especiales de datos y respecto también a la

[2] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

[3] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los Derechos Digitales.

ubicación (y prestación) en la UE de los sistemas de información y comunicaciones relacionados con el Padrón de habitantes, registros de población, gestión tributaria y el sistema nacional de Salud.

- En caso de que el objeto de contratación implique el **acceso a datos de carácter personal**, el CPS adquiere la condición de encargado del tratamiento y por tanto estará obligado al cumplimento de lo establecido en el artículo 28 Encargo del Tratamiento del RGPD, de conformidad a lo indicado en el apartado **"Medidas de protección de los activos"**.

- **Condicionantes geográficos**: se pueden establecer condiciones sobre la ubicación geográfica de los servidores y/o de las líneas de comunicaciones en función de la información (incluyendo los datos personales) que vayan a acoger o a transportar respectivamente.

  Estas condiciones, como norma general, derivan de requisitos que el propio organismo establezca como necesarios o bien por condicionantes legales, establecidos por el cumplimiento de las prescripciones sobre las transferencias internacionales de datos fuera de la U.E. del Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de derechos digitales así como los establecidos en otra normativa, criterios o directrices relacionados con la protección de datos o el "Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones".

54. Por otro lado, se regulará también como se va a realizar el **seguimiento de la calidad del servicio** proporcionado por el CSP, definiendo los mecanismos que el proveedor implementará para que el organismo pueda verificar que los niveles de calidad de servicio acordados se cumplen.

    Bien sea a través de controles técnicos propios o a través de la revisión y aprobación periódica de los informes de servicio proporcionados por el CSP. Informes que detallarán cualesquiera anomalía o desviación significativa producida durante el período, así como las acciones que se han ejecutado como respuesta a estas situaciones susceptibles de introducir riesgos en la organización.

55. Para supervisar el cumplimiento de la normativa de protección de datos, se pueden establecer controles de cumplimiento ya sea reservándose la opción de que el CSP pueda ser auditado por un tercero, o bien mediante la remisión de evidencias de cumplimiento, como, por ejemplo, informes de auditoría de la norma, contratos de confidencialidad formalizados con el personal, etc. Documentación que podría estar accesible para su consulta, en los sitios web del CSP.

56. **Se incluyen modelos de clausulado a incluir en los pliegos y/o peticiones de oferta en el Anexo MODELOS DE CLAUSULADO A INCLUIR EN PLIEGOS Y ACUERDO DE NIVEL DE SERVICIO.**

2.2.2.5 Continuidad

57. El organismo para la realización del **análisis de impacto**, identificará los requisitos de disponibilidad que le serán de aplicación a los servicios proporcionados por la nube y verificará que se corresponden con los contratados al CSP, de igual modo identificará todos los elementos que son críticos para la prestación de cada servicio.

58. La continuidad de los servicios soportados por la solución en la nube, necesaria para sistemas de categoría ALTA, será provista por el CSP. La disposición de la certificación ENS de categoría ALTA por parte del CSP será evidencia suficiente del cumplimiento de estos requisitos. En cualquier caso, se le podrán requerir evidencias del cumplimiento de los siguientes requisitos de seguridad:

    - Planificación de **medios alternativos para la provisión de los servicios** proporcionados por terceras partes a los contratados actualmente.
    - Existencia de un **plan de continuidad** con su correspondiente **plan de pruebas**.
    - Disposición de **personal alternativo** que pueda hacerse cargo de las tareas del actual en caso de indisponibilidad.
    - Existencia y disponibilidad de **instalaciones alternativas** en caso de indisponibilidad de las habituales.
    - Garantía de la existencia de **medios alternativos de comunicación** en caso de que los actuales fallen.
    - Disponibilidad de **medios alternativos de los que dispone el CSP para prestar los servicios** en caso de que fallen los habituales.

59. En el caso de que la provisión se realice desde una nube privada “on premise”, será el organismo el responsable de su aplicación.

2.2.2.6 Monitorización del sistema

60. El CSP dispondrá de herramientas de **prevención o detección de intrusión** en el caso de que los servicios se encuentren soportados por una nube privada “on premise” será el organismo el que tendrá que implementar estas funcionalidades.

61. Para la recopilación de los datos necesarios para conocer el grado de implantación de las medidas de seguridad, para dar respuesta al Informe Nacional sobre el Estado de la Seguridad, así como los de relativos al sistema de gestión de incidentes, se definirán los indicadores y el **sistema de métricas** asociado, teniendo en cuenta también los datos relacionados con los servicios soportados por la nube.

2.2.3 Medidas de protección de los activos

62. Las medidas de seguridad relativas a la **protección de las instalaciones e infraestructuras**, estarán cubiertas por el CSP. En caso de que la provisión se realice desde una nube privada "on premise", será el organismo el responsable de su aplicación.

63. Las medidas relativas a la seguridad en la **gestión del personal** (perfiles de puestos de trabajo, concienciación, formación, funciones y obligaciones) serán cubiertas por el CSP en lo relativo a la provisión de los servicios en la nube, no obstante, al organismo igualmente le serán de aplicación estas medidas, en relación con el personal relacionado con estos servicios.

64. Las medidas relativas a la **protección de los equipos** (bloqueo de puesto de trabajo, protección de los portátiles, etc.) serán cubiertas por el CSP en lo relativo a la provisión de los servicios en la nube, no obstante, al organismo igualmente le serán de aplicación estas medidas, respecto a los equipos relacionados con estos servicios.

65. Las medidas relativas a la **protección de las comunicaciones** (sistema de protección perimetral, confidencialidad, integridad y autenticidad de las comunicaciones, segregación de redes) serán cubiertas por el CSP en lo relativo a la provisión de los servicios en la nube, no obstante, al organismo igualmente le serán de aplicación estas medidas, respecto a las comunicaciones que realice sobre estos servicios.

66. Las medidas relativas a la **protección de los soportes de información** (etiquetado, cifrado, custodia, transporte, borrado y destrucción) serán cubiertas por el CSP en lo relativo a la provisión de los servicios en la nube, no obstante, al organismo igualmente le serán de aplicación estas medidas, respecto a los soportes relacionados con estos servicios.

67. Las medidas relativas a la **protección de las aplicaciones** (desarrollo seguro, pruebas de aceptación y puesta en servicio) serán cubiertos por el CSP en lo relativo al software relacionado con la provisión de los servicios en la nube, no obstante, al organismo igualmente le serán de aplicación esta medida, respecto al software de su competencia relacionado con los servicios.

68. En el caso de que los servicios en la nube conlleven en tratamiento de **datos de carácter personal**, con carácter previo a la contratación se recomienda tener en cuenta las recomendaciones establecidas por la Agencia Española de Protección de Datos, en la "Guía para clientes que contraten servicios de Cloud Computing".

69. A este respecto debemos tener en cuenta, que al tratar datos de carácter personal, el CSP adquiere la condición de encargado del tratamiento y por tanto estará obligado al cumplimento de lo establecido en el artículo 28 Encargado del Tratamiento del RGPD, que establece la necesidad de que este tratamiento se rija por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del

responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

- Tratará los datos para las finalidades establecidas y conforme a las instrucciones del organismo.
- La obligación de confidencialidad del personal del CSP respecto a los datos.
- Las medidas de seguridad que serán de aplicación. En este punto, se tendrá en cuenta lo establecido en la "Disposición adicional primera. Medidas de seguridad en el ámbito del sector público" de la LOPDGDD[4], donde se establece que se deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.
- Las cesiones previstas.
- Las subcontrataciones previstas.
- Régimen de subcontratación previsto. Subcontrataciones previstas inicialmente.
- Las transferencias internacionales de datos.
- Régimen transferencias internacionales de datos. Transferencias previstas.
- La existencia del delegado de protección de datos (en caso de que sea de aplicación).
- La ubicación de los tratamientos.
- Registro de Actividades de Tratamiento (RAT), en caso de que sea de aplicación.
- La responsabilidad respeto al tratamiento de los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas u otros reconocidos por la normativa aplicable.
- La gestión de las violaciones de seguridad, alineado con lo establecido para la gestión de incidentes de seguridad. Regulación de la comunicación y/o notificación de brechas de seguridad, plazos, medios y evidencias.
- Régimen de colaboración con el Responsable en otras obligaciones: elaboración de las Evaluaciones de Impacto sobre la Privacidad relativas a la protección de datos personales (EIPD), análisis de los riesgos asociados, etc.

[4] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los Derechos Digitales.

- Regulación de medidas de diligencia exigidas al proveedor, incluidas las posibles auditorias y/o controles de supervisión del cumplimiento de la normativa de protección de datos.
- Responsabilidad respecto al derecho a la información en la recogida de datos personales de las personas usuarias de los servicios.
- Regulación de la restitución de datos personales, alineado con las condiciones establecidas en la finalización del contrato.

70. En caso de que la provisión de los servicios se realice desde una nube privada "on premise", será responsabilidad del organismo el cumplimiento de la normativa de protección de datos, salvo en aquellos aspectos asociados al servicio de mantenimiento y/o soporte ante incidencias y evolutivos o parches de seguridad, cuando el mismo conlleve acceso a datos personales del Responsable.

71. En caso de que el CSP, provea mecanismos que permitan el etiquetado de la información alojada en la nube, el organismo podrá alinear su procedimiento de **calificación de la información** con este.

72. El proceso de limpieza de **limpieza de los documentos**, retirando de estos la información no necesaria contenida en campos ocultos y/o metadatos será responsabilidad del organismo propietario de los documentos gestionados por los servicios en la nube.

73. Cuando la realización de las **copias de seguridad** es responsabilidad del CSP, el organismo le solicitará información sobre el procedimiento de copias y las pruebas de respaldo implementadas, al menos sobre los siguientes aspectos:

- 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).

2.2.3.1 Protección de los servicios

74. La aplicación de medidas para la **protección del correo electrónico** de las amenazas propias de este medio será responsabilidad del organismo, salvo que el CSP proporcione la provisión del correo electrónico.

75. La aplicación de medidas para la **protección de los servicios y aplicaciones web** de las amenazas propias de este medio, será cubierta por el CSP en lo relativo a la provisión de los servicios en la nube en la modalidad de SaaS, en caso contrario será responsabilidad del organismo.

76. La aplicación de las medidas relativas a la **protección frente a la denegación de servicio**, estarán implementadas por el CSP, salvo que la provisión de los servicios se realice desde una nube privada "on premise", siendo entonces responsabilidad del organismo.

2.2.3.2 Auditoría

77. Si la provisión de los servicios se realiza desde un sistema soportado por una nube privada "on premise", donde la categoría sea ALTA, **se requerirá que el servicio en la nube haya superado, con éxito, una auditoría de prueba de penetración (pentesting)** por una tercera parte independiente para evaluar la madurez del servicio en materia de seguridad e identificar posibles vulnerabilidades existentes en el mismo.

    En esta auditoría se comprobará la ausencia de vulnerabilidades públicas que permitan comprometer la información manejada o el servicio prestado.

78. En el caso de que el servicio en la nube sea de seguridad, esa tercera parte deberá ser un laboratorio independiente acreditado por la Entidad Nacional de Acreditación (ENAC), siguiendo metodologías de evaluación reconocidas por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) del CCN.

2.2.3.3 Transparencia

79. El proveedor del servicio deberá ser capaz de:

    - Dar visibilidad al cliente de las herramientas de seguridad de las que dispone, incluyendo aquellas destinadas a la monitorización, análisis, recuperación y notificación de incidentes de seguridad.
    - Informar al usuario del tipo de virtualización utilizada y del nivel y mecanismos de segregación de sus datos o aplicaciones alojadas en la nube.
    - Informar al usuario de los mecanismos y procedimientos de borrado seguro de la información almacenada por el proveedor, que serán utilizados en el momento de la terminación del vínculo contractual.

2.2.3.4 Información de registro

80. Permitir al cliente el acceso y análisis de los diferentes registros (logs), registros de acceso y cualquier otra información que pudiera ser solicitada para garantizar el cumplimiento de las obligaciones legales.

    En caso de incidente de seguridad, toda la información requerida (configuración, logs, etc.) de los equipos físicos, dispositivos de red, servicios compartidos y dispositivos de seguridad debe ser entregada al cliente.

2.2.3.5 Cifrado y gestión de claves

81. El servicio deberá disponer de **mecanismos de cifra** que permitan que la información del usuario esté protegida, en tránsito y en reposo, para que no pueda ser leída o modificada en caso de acceso ilegítimo. Los mecanismos criptográficos deberán cumplir con lo especificado en la guía correspondiente de la serie CCN-STIC.

82. El proveedor deberá cumplir uno de los siguientes casos:

    - Ser capaz de garantizar el funcionamiento de los mecanismos de cifra sin que las claves sean almacenadas en la nube. Estas estarán en disposición del cliente quien es el encargado de su gestión y almacenamiento.
    - Almacenar las claves del cifrado en módulos de seguridad de hardware denominados dispositivos HSM (Hardware Security Modules), no accesibles por terceros. Dichos dispositivos deberán estar cualificados por el CCN e incluidos en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN.

2.2.3.6 Jurisdicción de los datos

83. El proveedor informará al cliente sobre la **ubicación geográfica de sus datos** (incluido copias de seguridad (backups) y almacenamiento de logs), antes y durante el suministro del servicio.

84. En cuanto a las limitaciones geográficas de los datos, se estará a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; la Ley Orgánica 3/2018, de 5 de diciembre y el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el presente real decreto.

3. CONCLUSIONES

85. Con carácter previo a la contratación es necesario identificar los **requisitos de seguridad a solicitar al CSP**, para su inclusión en las condiciones contractuales, como, por ejemplo:

    - Que disponga de la **conformidad con el ENS** del sistema que soporta los servicios que se contratan, en la categoría igual o superior a la que hayamos determinado en el proceso de categorización.
    - Incluir aquellas **medidas de seguridad adicionales** que se hayan identificado como necesarias, como por ejemplo la existencia de un plan de continuidad, cuando no se rea requerido por la categorización del sistema (ALTA).

- Define las **responsabilidades y obligaciones (CSP/organismo)** respecto a la implantación de medidas, mediante el análisis detallado de la declaración de aplicabilidad identificando las que son responsabilidad exclusiva del CSP o compartida.
- Establece los niveles de calidad de los servicios a contratar, mediante el establecimiento de **Acuerdos de Nivel de Servicio (SLA)** sobre la capacidad, disponibilidad, cambios, etc.
- Establece los **requisitos legales necesarios**, los relativos, a la normativa de protección de datos, confidencialidad, ubicación geográfica de los datos, etc.
- Contempla la posibilidad de **acogerse a un Perfil de Cumplimiento Específico**, lo que posibilitará implantar las medidas de seguridad necesarias y adaptadas a la nube, a la vez que disponer de guías de configuración.
- Incluye cualquier otro aspecto reflejado en esta Guía.

4. DECÁLOGO

	Decálogo de recomendaciones para la utilización de servicios en la nube
1	Determinar la categoría del sistema (BÁSICA, MEDIA o ALTA) que soportará la solución en la nube, según el ANEXO I del Real Decreto 3/2010.
2	Elaborar la declaración de aplicabilidad, según el ANEXO II del Real Decreto 3/2010.
3	Realizar un análisis de riesgos, para identificar requisitos adicionales de seguridad, que se reflejarán en la declaración de aplicabilidad.
4	Acogerse a un Perfil de Cumplimiento Específico (en caso de que sea de aplicación).
5	Establecer las condiciones contractuales, con carácter previo a la contratación, en los pliegos y/o peticiones de oferta.
6	En las condiciones contractuales, además de las relativas al cumplimiento de requisitos legales, detallar aspectos relativos al servicio, su infraestructura, el dimensionamiento, los registros de actividad, la gestión de incidentes, copias de seguridad, etc. y establecer condiciones relativas a la finalización del servicio.
7	Supervisar el cumplimiento, por parte del CSP, de los requisitos legales establecidos en las condiciones de contratación.
8	Realizar un seguimiento periódico del cumplimiento de los Acuerdos de Nivel

	de Servicio (SLA), establecidos con el CSP.
9	Planificar revisiones periódicas de la información, que el CSP proporciona a través de diversos mecanismos, como por ejemplo los registros de actividad, la capacidad, el almacenamiento, etc.
10	Elabora una normativa de seguridad específica para los usuarios de la nube.

5. ANEXO I Clausulado y Acuerdos de Nivel de Servicio

5.1 Conformidad con el Esquema Nacional de Seguridad (ENS)

Nota: En caso de contratación de servicios de nube a traves de una entidad intermediaria que actue como proveedora de servicios (ENTIDAD LICITADORA o ADJUDICATARIA), pero que no sea propietaria de los sistemas que prestarán los servicios de nube, será necesario exigir también la conformidad con el ENS de los sistemas finales que prestan los servicios de nube, propiedad del proveedor final de servicios en la nube.

Considerando lo dispuesto en el artículo 29 del Real Decreto Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se describe la obligación de exigir a los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, de conformidad con el Esquema Nacional de Seguridad, la ENTIDAD CONTRATANTE, considera necesario que los proveedores que vayan a concurrir a la licitación de que se trate, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad (cuando se haya declarado categoría BÁSICA del sistema), o la Certificación de Conformidad con el Esquema Nacional de Seguridad (cuando se haya declarado categoría MEDIA o categoría ALTA).

Así pues, en base a lo anterior, y al análisis de los riesgos a los que están expuestos los servicios objeto de la licitación, la ENTIDAD CONTRATANTE, establece como necesario que la ENTIDAD LICITADORA deberá estar en condiciones de exhibir la correspondiente Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad, para la categoría de seguridad de que se trate, de los sitemas que intervengan en la prestación de los servicios indicados, así como mantener la conformidad vigente durante la vigencia del contrato. En el supuesto de que el adjudicatario no pudiera mantener la conformidad con el ENS -por pérdida, retirada o suspensión de la Certificación de Conformidad o imposibilidad de mantener la Declaración de Conformidad-, deberá comunicar esta circunstancia, de forma inmediata y sin dilación indebida, a la ENTIDAD CONTRATANTE, quien considerará el impacto en la prestación objeto del contrato de dicha circunstancia.

Cuando el contrato contemple, total o parcialmente, el uso de sistemas on-premise (por ejemplo, software), de conformidad con lo establecido en *la Guía CCN-STIC 858 Implantación de sistemas SaaS en modo local (on-premise*) la ENTIDAD LICITADORA deberá aportar los siguientes documentos: Guía de instalación (dirigida a administradores), la Guía de uso seguro (dirigida a usuarios) y la Guía de relación entre proveedor y cliente.

La ENTIDAD ADJUDICATARIA asume su obligación de cumplir plenamente con el Esquema Nacional de Seguridad, y con la necesidad de que los sistemas de información de aquellos proveedores que resulten esenciales para la prestación del

servicio objeto del contrato sean asímismo conformes con el Real Decreto 3/2010, de 8 de enero.

5.2 Cláusulas de confidencialidad

5.2.1 Confidencialidad en la contratación

Sin perjuicio de lo dispuesto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, y de las disposiciones contenidas en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, relativas a la obligación de publicidad de la adjudicación y a la información que debe darse a los candidatos y a los licitadores, los órganos de contratación no podrán divulgar la información facilitada por las ENTIDADES LICITADORAS que estos hayan designado como confidencial en el momento de presentar su oferta.

El carácter de confidencial puede afectar, entre otros, a los secretos técnicos o comerciales, a los aspectos confidenciales de las ofertas y a cualesquiera otras informaciones cuyo contenido pueda ser utilizado para falsear la competencia, ya sea en el procedimiento de licitación en cuestión o en otros posteriores.

La obligación de confidencialidad no podrá impedir la divulgación pública de partes no confidenciales del contrato, como puede ser la liquidación, los plazos finales de ejecución de los servicios, la identidad del adjudicatario o las partes esenciales de la oferta, así como las modificaciones posteriores.

Así mismo, toda la documentación o información facilitada por la ENTIDAD CONTRATANTE a los licitadores al objeto de que dispongan de la información precisa para la presentación de las ofertas correspondientes, tiene carácter confidencial, debiendo ser tratada por éstos como tal.

Una vez adjudicado el contrato objeto de la licitación, si la ENTIDAD CONTRATANTE facilitara a la ENTIDAD ADJUDICATARIA información adicional necesaria para la prestación de los servicios, ésta deberá ser considerada confidencial, por lo que tanto la ENTIDAD ADJUDICATARIA como cualquiera persona que intervenga o esté relacionado con la ejecución del contrato, deberán tratarla como tal.

Cuando la información presentada incluya datos personales, será necesario considerar las disposiciones en relación a Protección de Datos establecidas en la normativa vigente.

Todas las personas que intervengan en cualquier fase del proceso de licitación, estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD).

Toda la información tratada, generada o relativa a la ejecución del contrato deberá ser procesada conforme a lo dispuesto en el correspondiente Pliego y descrito en el apartado que regula el tratamiento de datos personales por cuenta de terceros. En su defecto, cuando no se haya declarado o no exista tratamiento de datos personales, la ENTIDAD ADJUDICATARIA deberá proceder a la devolución de toda la información a la ENTIDAD CONTRATANTE o a quien esta designe, al finalizar el contrato.

5.2.2 Confidencialidad en la ejecución del contrato

.

De conformidad con lo establecido en el artículo 35.1.m) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, se determina la extensión objetiva y temporal del deber de confidencialidad impuesto a la ENTIDAD ADJUDICATARIA. Por tanto, la ENTIDAD ADJUDICATARIA estará obligada a mantener la plena confidencialidad y secreto con respecto a la información manejada durante la ejecución del contrato durante 5 años desde el conocimiento de la información concernida, salvo que en el correspondiente Pliego o en el contrato subsiguiente se determine un plazo distinto.

Se considerará confidencial, a todos los efectos, "toda la información y documentación relativa a la ENTIDAD CONTRATANTE, así como los buenos usos, prácticas y procedimientos internos", que pudiera conocer la ENTIDAD ADJUDICATARIA con motivo de la ejecución del contrato. La ENTIDAD CONTRATANTE no otorga derecho alguno a la ENTIDAD ADJUDICATARIA, por el acceso a su sistema de información. En la misma línea, se confiere el carácter confidencial a aquella información a la que tenga acceso con ocasión de la ejecución del contrato, que se le hubiese dado el referido carácter en los pliegos o en el contrato, o que por su propia naturaleza deba ser tratada como tal, incluyendo, expresamente, toda la información asociada a medidas de seguridad y de protección, configuraciones desarrolladas, protecciones del servicio y aplicaciones, elementos y descripciones de infraestructura y arquitectura, procesos de autenticación y protocolos de seguridad, comunicaciones, incidencias, informes de terceros, controles de capacidad y evaluaciones de las disponibilidades implicadas, análisis automáticos, redes y protecciones del perímetro, elementos adscritos a la continuidad, registros de actividad y protecciones asociadas, protocolos de copias y restauraciones, elementos de mantenimiento y garantías implicadas, y cuantos otros elementos puedan considerarse un riesgo a los efectos del servicio contratado o la información vinculada al mismo.

La ENTIDAD ADJUDICATARIA se compromete a no divulgar, no ceder o exponer la información titularidad de la ENTIDAD CONTRATENTE sin su previo consentimiento expreso y por escrito. Asimismo, la ENTIDAD ADJUDICATARIA deberá abstenerse de emplear la documentación y/o información conocida o facilitada durante la ejecución del contrato para fines ajenos a los propios de la ejecución del contrato.

Cuando el contrato no requiera el acceso al sistema de información de la ENTIDAD CONTRATANTE pero suponga el acceso a las instalaciones, la ENTIDAD ADJUDICATARIA se compromete a mantener plena confidencialidad de la información que pudiera conocers de manera accidental por los accesos a las instalaciones, y especialmente, aquella que pueda suponer un riesgo para la ENTIDAD CONTRATANTE en caso de ser conocida y/o pueda suponer una brecha de seguridad.

Cuando la información presentada incluya datos personales, será necesario considerar las disposiciones en relación a Protección de Datos, en la normativa vigente y declaradas en el correspondiente Pliego. Para el caso de que la contratación implique el acceso de la ENTIDAD ADJUDICATARIA a datos de carácter personal de

cuyo tratamiento sea responsable la ENTIDAD CONTRATANTE, la ENTIDAD ADJUDICATARIA y todas las personas que intervengan en cualquier fase del proceso de contratación, estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD) y declarado en el presente pliego. La ENTIDAD ADJUDICATARIA se compromete a formalizar acuerdos de confidencialidad con el personal que, adscrita a la ejecución del contrato, y mantener una sensibilización y formación constante.

5.3 Normativa aplicable en materia de protección de datos

Si el objeto de la prestación contenida en el contrato objeto de licitación exigiera el tratamiento de datos personales, se estará a lo dispuesto en el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) -con especial incidencia a lo preceptuado en su Disposición adicional primera)- y a la restante normativa que resulte de aplicación, así como, cuando corresponda, y, cuando corresponda, a lo establecido en el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, que resultarán de aplicación a la ENTIDAD ADJUDICATARIA y a sus posibles subcontrataciones, durante toda la vigencia del contrato, independientemente de la ubicación de los sistemas implicados en la prestación de los servicios.

La finalidad del tratamiento de los datos personales por parte de la ENTIDAD ADJUDICATARIA será la de la prestación de los servicios comprendidos en el contrato. El uso de los datos personales para finalidades distintas a las anteriormente indicadas supondrá un incumplimiento por parte de la ENTIDAD ADJUDICATARIA, lo que podrá dar luga a la resolución del contrato.

5.4 Declaración de ubicación

Tal y como se establece en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, considerando la naturaleza del servicio, la ENTIDAD ADJUDICATARIA deberá facilitar la identificación de la ubicación de los sistemas de información vinculados con los servicios objeto del contrato, incluyendo todas las ubicaciones asociadas al almacenamiento y prestación del servicio, contemplando todas las actividades implicadas, tales como recogida, almacenamiento, procesamiento y gestión.

Es necesario que la ENTIDAD ADJUDICATARIA identifique a todas las entidades subcontratadas que participarán en la ejecución de los servicios objeto de la licitación, tanto en la oferta presentada como durante la vigencia del contrato, debiendo identificar la ubicación y los servicios concretos prestados por cada una de ellas.. La subcontratación quedará en todo caso sometida a las disposiciones contenidas en la normativa de protección de datos, sin excepción.

Se considerarán, a todos los efectos, las limitaciones establecidas en la normativa de protección de datos relativas a transferencias internacionales de datos, siendo condición esencial el cumplimiento de tales previsiones, que se extenderán a las entidades subcontratadas. . Esta obligación se considera esencial al contrato y se mantendrá durante toda la vigencia del mismo.

Cualquier modificación a lo largo del contrato relativa a las exigencias establecidas en el presente apartado, deberá ser comunicada sin dilación, a la ENTIDAD CONTRATANTE.

5.5 Transferencia Internacional de Datos

No podrán realizarse transferencias a un tercer país o una organización internacional fuera de la Unión Europea, salvo en los supuestos específicamente autorizados por el Reglamento (UE) 2016/679 General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), siendo la única excepción contemplada, la transferencia a países, organizaciones o territorios que hayan sido declarados con un nivel adecuado de protección por parte de las autoridades de control en materia de protección de datos, o cuando sea precisa la transferencia en cumplimiento de una obligación legal, convenio internacional o requerimiento judicial.

La ENTIDAD ADJUDICATARIA deberá comunicar sin dilación indebida, cualquier cambio en relación a las condiciones para la transferencia de datos personales, especialmente la perdida de la condición de "nivel adecuado de protección" para transferencia internacional, conforme al RGPD. Se considera expresamente incluidos los supuestos en los que la Comisión determine la perdida de la adecuación de un país, organización, entidad o empresa, incluidas aquellas que dejen de estar adheridas a eventuales acuerdos internacionales que permitan tranferencias internacionales de datos.

5.6 Servicio asociado a la verificación electrónica de identidad

Considerando lo dispuesto en la Ley 39/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y en el caso de que el servicio licitado por la ENTIDAD CONTRATANTE incluya un sistema de identificación mediante clave concertada a los efectos de lo descrito el artículo 9.2c) de la precitada ley, será necesario que las ofertas presentadas por las ENTIDADES LICITADORAS incluyan o faciliten la identificación de la ubicación y prestación del servicio, así como los recursos técnicos que vayan a ser asignados para la recogida, almacenamiento, tratamiento y gestión, los cuales solo podrán estar ubicados en el territorio de la Unión Europea, según lo dispuesto en el artículo 122.2c) de la ley 9/2017, de 8 de noviembre de Contratos del Sector Público. Cuando estuvieran implicadas categorías especiales de datos, según lo dispuesto en el artículo 9 del Reglamento (UE) 2016/679 General de Protección de Datos (RGPD), la ubicación se circunscribirá al territorio nacional.

A todos los efectos, cuando el servicio licitado permitiera la subcontratación, ésta quedará sometida en idénticos términos a lo descrito. Por ello, será necesario declarar expresamente la localización de los servicios o recursos concernientes a los procesos subcontratados. Cuando existieran varios subcontratados, será necesario declararlo de cada uno de ellos, de manera individualizada.

Cuando el contrato ya hubiera sido adjudicado, y existiera una modificación que afectará a la ubicación o prestación del servicio, incluyendo cambios en la subcontratación, deberán ser comunicados sin demora, a la ENTIDAD CONTRATANTE, identificando claramente los cambios producidos, quedando la ENTIDAD CONTRATANTE facultada para resolver el contrato.

La ENTIDAD ADJUDICATARIA será a todos los efectos responsable directo de los incumplimientos derivados de tal subcontratación y de las obligaciones declaradas.

5.7 Tratamiento de datos de los tipos descritos en el artículo 46 bis de la Ley 40/2015

Considerando lo dispuesto en el artículo 46 bis de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y en los casos en que el servicio licitado por la ENTIDAD CONTRATANTE afectara a datos relativos al censo electoral, padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del Sistema Nacional de Salud, , será necesario que las ENTIDADES LICITADORAS incluyan en sus ofertas la ubicación y prestación del servicio, que solo podrá prestarse dentro del territorio de la Unión Europea.

A todos los efectos, cuando el servicio licitado permitiera la subcontratación, ésta quedará sometida en idénticos términos a lo descrito. Por ello, será necesario declarar expresamente la localización de los servicios o recursos concernientes a los procesos subcontratados. Cuando existieran varios subcontratados, será necesario declararlo de cada uno de ellos, de manera individualizada.

Cuando el contrato hubiera sido adjudicado, y existiera una modificación que afectará a la ubicación o prestación del servicio, incluyendo cambios en la subcontratación, deberán ser comunicados sin demora, a la ENTIDAD CONTRATANTE, identificando claramente los cambios producidos, quedando la .ENTIDAD CONTRATANTE facultada para resolver el contrato.

La ENTIDAD ADJUDICATARIA será a todos los efectos responsable directo de los incumplimientos derivados de tal subcontratación y de las obligaciones declaradas.

5.8 Regulación de la finalización del contrato: Transferencia de tecnología

Durante la ejecución del contrato, la ENTIDAD ADJUDICATARIA se compromete a facilitar a las personas designadas por la ENTIDAD CONTRATANTE toda la información y documentación que estas soliciten para disponer de un total conocimiento técnico de

las circunstancias en las que se desarrollan los servicios, sus actividades y, en general, de todas las operaciones técnicas, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos, y herramientas utilizados para resolverlos.

Una vez finalizado el contrato, la ENTIDAD ADJUDICATARIA deberá desarrollar las acciones precisas para la transferencia del conocimiento y de la información, implicados en el servicio. El proceso incluirá, necesariamente y a petición de la ENTIDAD CONTRATANTE, la devolución de toda la información a la propia ENTIDAD CONTRATANTE o a quien esta designe, en un plazo máximo que estará determinado en el correspondiente Pliego, mediante los medios seguros que sean necesarios y debiendo estar la información en un formato que se determinará en el correspondiente Pliego.

Para el proceso de restitución y transferencia tecnológica será preciso que la ENTIDAD ADJUDICATARIA presente una planificación detallada, contemplando los medios que serán empleados, las acciones de contingencia diseñadas y los riesgos que pudieran presentarse en el proceso. Cuando sea necesario, y especialmente cuando existiera una nueva entidad adjudicataria, se incluirá el periodo de transición destinado a la gestión organizada del proceso de transferencia y restitución.

A los efectos del cumplimiento de la normativa vigente en materia de protección de datos, se considerarán los periodos de retención legal que pudieran ser obligatorios para la entidad adjudicataria saliente.

Esta cláusula será obligatoria cuando la finalización del servicio fuera anticipada, siendo responsabilidad de la entidad adjudicataria saliente, una transferencia y restitución ordenada.

5.9 Gestión de copias de seguridad y restauración de datos

La ENTIDAD ADJUDICATARÍA deberá disponer de los mecanismos necesarios para implementar una política de respaldo y de pruebas de recuperación que contemplen como mínimo los siguientes requsitos:

- Identificación del 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).

5.10 Gestión de recuperación ante desastres (Plan de continuidad)

Para garantizar la continuidad de los servicios objeto del contrato, la ENTIDAD ADJUDICATARIA, deberá disponer y presentar un plan de recuperación ante cualquier contingencia. Este plan se activará ante la indisponibilidad total o parcial de los

recursos principales, que por cualquier motivo provoque la indisponibilidad de los servicios objeto del contrato. Este Plan incluirá:

- La identificación y descripción de los medios alternativos planificados para la provisión de los servicios, personal alternativo, existencia o planificación de instalaciones y medios de comunicación alternativos, etc.
- Realización de, al menos, una prueba de recuperación anual. . El informe final de la prueba deberá ser remitido al responsable que determine la ENTIDAD CONTRATANTE, así como un plan de trabajo con acciones correctivas si se detectaran eventos o acciones a corregir.
- Actualización de la documentación del plan de recuperación ante desastres tanto como sea necesario.

5.11 Acuerdo de nivel de servicio tipo

5.11.1 Alcance de los servicios

Sin perjuicio de lo dispuesto en el correspondiente Pliego de Prescripciones Técnicas, la ENTIDAD ADJUDICATARIA deberá incluir en su oferta el horario previsto para la prestación del servicio objeto del contrato (por ejemplo, "durante las 24 horas de los 365 días", etc.).

En el apartado de acuerdo de nivel de servicio, se establecerá el margen aceptado para cada uno de los indicadores descritos, a excepción de las franjas establecidas para las ventanas de mantenimiento.

5.11.2 Comunicaciones e incidencias

Todas las comunicaciones relacionadas con los servicios o con el correspondiente Acuerdo de Nivel de Servicio se deberán realizar por las áreas o departamentos de la ENTIDAD CONTRATANTE declarados al efecto en el correspondiente Pliego.

Asimismo, el Pliego señalará el medio que deberá ser usado para las comunicaciones (por ejemplo, correo electrónico y/ o llamadas telefónicas, etc.).

Será obligatorio que el servicio proporcionado por la ENTIDAD ADJUDICATARIA, disponga de un registro operativo de las peticiones o notificaciones realizadas por la ENTIDAD CONTRATANTE, empleando, en su caso, la herramienta señalada en el correspondiente Pliego. A todos los efectos este registro deberá ser también el registro de incidencias y peticiones, y deberá cumplir las premisas establecidas en la normativa de protección de datos.

5.11.3 Niveles de Servicio requeridos

5.11.3.1 Disponibilidad de los servicios contratados

La ENTIDAD ADJUDICATARIA deberá proporcionar en su oferta la siguiente información:

Indicador 1: garantizar la disponibilidad de los servicios contratados.

Descripción del indicador: porcentaje de tiempo en el que los servicios han estado activos y dando servicio.

Unidad de medida: porcentaje.

Métrica: I1= Tp-Tc/Tp*100.

- **Tc:** Tiempo total, medido en minutos, en el que los servicios están fuera de servicio durante el periodo medido.
- **Tp:** Tiempo total, medido en minutos, del periodo medido.

Periodicidad mínima de los análisis: mensual.

Valor objetivo: > 99,5 %.

Penalización: 1,3 % de la facturación del periodo.

5.11.3.2 Disponibilidad de los servicios contratados (condiciones particulares)

Indicador 3: garantizar la disponibilidad de los servicios contratados en determinada franja horaria, por ejemplo, horario diurno 07:00 a 22:00.

Descripción del indicador: porcentaje de disponibilidad de los servicios en horario diurno (07:00 a 22:00 horas) durante el periodo medido.

Unidad de medida: porcentaje.

Métrica: I3= 900-Tc/900*100.

- **Tc:** Tiempo total, medido en minutos, en el que los servicios están fuera de servicio durante el periodo medido y en horario de 07:00 a 22:00 horas.

Periodicidad mínima de los análisis: mensual.

Valor objetivo: > 98 %.

Penalización: 1,3 % de la facturación del periodo.

5.11.3.3 Disponibilidad de almacenamiento

Indicador 4: garantizar la disponibilidad de almacenamiento.

Descripción del indicador: porcentaje de tiempo en el que el almacenamiento ha estado activo y dando servicio.

Unidad de medida: porcentaje.

Métrica: I4= Tp-Tc/Tp*100.

- **Tc:** Tiempo total, medido en minutos, en el que el almacenamiento está fuera de servicio durante el periodo medido.
- **Tp:** Tiempo total, medido en minutos, del periodo medido.

Periodicidad mínima de los análisis: mensual.

Valor objetivo: > 99,5 %.

Penalización: 2,5 % de la facturación del periodo.

5.11.3.4 Resolución de incidencias, problemas

Indicador 5: maximizar el número de incidencias, problemas resueltos.

Descripción del indicador: porcentaje de incidencias, problemas aceptados y resueltos

Unidad de medida: porcentaje.

Métrica: I5= Nr/Nt*100.

- **Tr:** número de incidencias, problemas resueltos durante el periodo de medición
- **Tp:** número total de incidencias, problemas que estaban abiertos al inicio de periodo de medición sumados a aquellos que se han abierto durante dicho periodo.

Periodicidad mínima de los análisis: mensual.

Valor objetivo: > 95 %.

Penalización: 3,2 % de la facturación del periodo.

Las incidencias y peticiones de servicio mantendrán un flujo con el comunicante, debiendo proceder a su cierre cuando se hubiera comunicado al mismo y no se considere ningúna acción adicional.

Se incluirá necesariamente en el registro:

- Hora de inicio de incidencia y hora de finalización. (Incluyendo la hora en la que se produce la incidencia, la hora en la que se notifica y la hora de finalización de la resolución).
- Hora de comunicación de inicio y hora de comunicación de finalización.
- Tiempos de resolución.
- Conclusiones y mejora.

En este sentido se tendrán en cuenta los puntos requeridos por la normativa aplicable, para la identificación, gestión y registro de incidencias, que puedan afectar al servicio, que serán acordados con la ENTIDAD CONTRATANTE.

Ante las incidencias acaecidas y comunicadas correctamente, la ENTIDAD ADJUDICATARIA dispondrá de un tiempo de respuesta para la resolución de las mismas, que estará definido en el correspondiente Pliego, de:

- Incidencia crítica: (Por ejemplo: 1 hora laboral o 4 no laborales).
- Incidencia importante: (Por ejemplo:2 horas laborales o 12 no laborales).
- Incidencia menor: (Por ejemplo: 3 horas laborales o 72 no laborales).

Se recopilarán datos para valorar el sistema de gestión de la incidencia, permitiendo conocer el número de incidentes de seguridad tratados (y específicamente):

- Tiempo empleado para cerrar el 50% de los incidentes.
- Tiempo empleado para cerrar el 90% de los incidentes.

Anualmente, se remitirán estos valores en modo informe a la ENTIDAD CONTRATANTE.

5.11.3.5 Resolución peticiones de cambio y/o actualizaciones

Indicador 6: fomentar la correcta realización de cambios y/o actualizaciones.

Descripción del indicador: porcentaje de instalaciones, cambios y actualizaciones de hardware/software correctamente ejecutados y con tiempo de resolución máximo de 2 días.

Unidad de medida: porcentaje.

Métrica: I6= Nr/Nt*100

- **Nr:** número de cambios y/o actualizaciones correctamente ejecutados y con tiempo máximo de resolución de 2 días durante el periodo de medición.
- **Tp:** de cambios y/o actualizaciones durante el periodo de medición.

Periodicidad mínima de los análisis: mensual.

Valor objetivo: > 99 %.

Penalización: 4,5 % de la facturación del periodo.

Se programarán las pruebas necesarias y, en su caso, previo acuerdo con la ENTIDAD CONTRATANTE, generando el menor impacto en la operatividad del servicio. Todas las paradas técnicas del servicio serán en horarios previamente acordados con la ENTIDAD CONTRATANTE.

5.11.3.6 Disponibilidad de copias de seguridad

Indicador 7: garantizar la disponibilidad de las copias de seguridad.

Descripción del indicador: porcentaje de copias de seguridad planificadas que se han ejecutado con éxito.

Unidad de medida: porcentaje.

Métrica: I7= Np-Nf/Np*100.

- **Nf:** número de backups planificados y no completados con éxito durante el periodo medido.
- **Np:** número de backups planificados durante el periodo medido.

Periodicidad mínima de los análisis: mensual.

Valor objetivo: > 99,9 %.

Penalización: 2,5 % de la facturación del periodo.

5.11.3.7 Fiabilidad de la recuperación de datos

Indicador 8: garantizar la fiabilidad de la recuperación de datos.

Descripción del indicador: porcentaje de recuperación de datos desde copias de seguridad ejecutadas correctamente.

Unidad de medida: porcentaje.

Métrica: I8= Nr/Nt*100.

- **Nr:** número de restauraciones de backups completadas con éxito durante el periodo medido.
- **Np:** número de restauraciones desde backups solicitadas durante el periodo medido.

Periodicidad mínima de los análisis: mensual.

Valor objetivo: > 99 %.

Penalización: 2,5 % de la facturación del periodo.

5.11.3.8 Activación del servicio de respaldo

Indicador 9: garantizar un tiempo máximo de activación del servicio de respaldo para los servicios indicados.

Descripción del indicador: tiempo consumido en poner en marcha el servicio de respaldo.

Unidad de medida: tiempo medido en horas.

Métrica: I9= Ta.

- **Ta:** tiempo medido en horas, empleado en preparar el servicio de respaldo para que ofrezca un servicio correcto, durante el periodo medido.

Periodicidad mínima de los análisis: mensual.

Valor objetivo: < 24.

Penalización: 2,4 % de la facturación del periodo.

5.11.3.9 Disponibilidad de la capacidad contratada

Indicador I10: gestionar la capacidad contratada.

Descripción del indicador: garantizar que no se superan los umbrales de capacidad contratada, estableciéndose un umbral en el que será necesario que la ENTIDAD ADJUDICATARÍA, avise a la ENTIDAD CONTRANTE, al objeto de autorizar el aumento de recursos.

Unidad de medida: tiempo medido en días.

Métrica: I10= Ta.

- **Ta:** tiempo medido en días en el que se comunica que se ha sobrepasado el umbral del 85 % en uso de los recursos contratados, durante el periodo medido.

Periodicidad mínima de los análisis: mensual.

Valor objetivo: <= 30.

Penalización: 2,5 % de la facturación del periodo.