GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CCN
CENTRO CRIPTOLÓGICO NACIONAL

GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-823)

UTILIZACIÓN DE SERVICIOS EN LA NUBE

ens
Esquema Nacional de Seguridad

DICIEMBRE 2014

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

NIPO: 002-14-031-5

Fecha de Edición: diciembre de 2014

S2 Grupo ha elaborado el presente documento y sus anexos. El Sr. José Antonio Mañas ha participado en la elaboración del presente documento y sus anexos

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

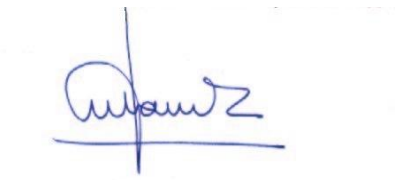
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Diciembre de 2014



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

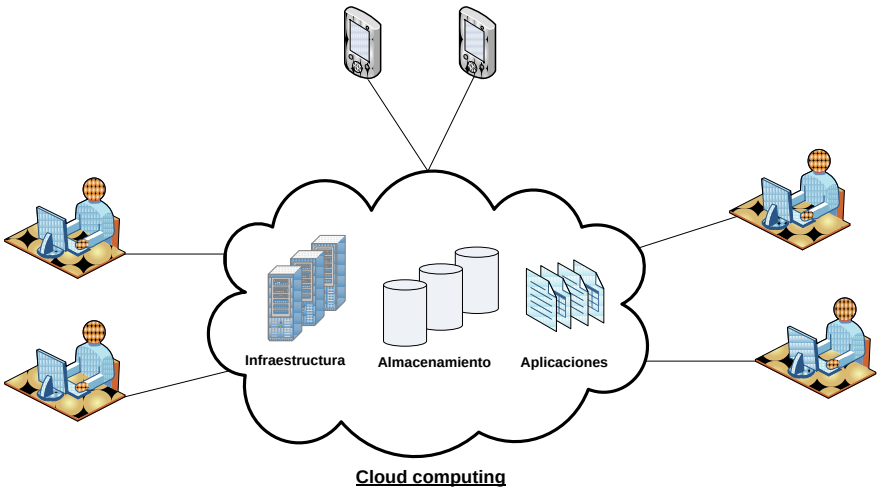
ÍNDICE

1 INTRODUCCIÓN 5
1.1 CONCEPTOS PREVIOS 5
1.2 CARACTERÍSTICAS DE LOS SERVICIOS EN LA NUBE 6
1.3 MODELOS DE DESPLIEGUE 7
1.4 CATEGORÍAS DE SERVICIO 7
1.5 ASPECTOS RELATIVOS A LA SEGURIDAD DE LA INFORMACIÓN 8
2 REQUISITOS DE SEGURIDAD 9
2.1 ROLES Y FUNCIONES 9
2.2 CATEGORIZACIÓN (ENS - ANEXO I) 10
2.2.1 COMUNIDADES 10
2.3 RECOMENDACIONES 11
2.4 MEDIDAS DE PROTECCIÓN (ENS - ANEXO II) 11
2.5 RESTRICCIONES ADICIONALES 11
2.5.1 COMUNIDAD BAJA 12
2.5.2 COMUNIDAD MEDIA 12
2.5.3 COMUNIDAD ALTA 12
3 REQUISITOS DERIVADOS DE LA EXISTENCIA DE DATOS DE CARÁCTER PERSONAL 13
4 NORMATIVA INTERNA 16
5 CONTRATACIÓN 17
5.1 DESCRIPCIÓN DEL SERVICIO 18
5.1.1 TIPO DE SERVICIO 18
5.1.2 TIPO DE INFRAESTRUCTURA 18
5.1.3 DIMENSIONADO DEL SERVICIO 18
5.2 SUBCONTRATACIÓN 19
5.3 PROTECCIÓN DE LA INFORMACIÓN 19
5.4 ACUERDOS DE NIVEL DE SERVICIO 20
5.5 ACCESO AL SERVICIO 21
5.6 CONDICIONANTES GEOGRÁFICOS 21
5.7 RESPONSABILIDADES Y OBLIGACIONES 21
5.8 REGISTRO DE ACTIVIDAD 22
5.9 FINALIZACIÓN DEL SERVICIO 22
6 OPERACIÓN 23
6.1 PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD 23
6.2 SEGUIMIENTO DEL SERVICIO 23
6.3 GESTIÓN DE CAMBIOS 24
6.4 GESTIÓN DE INCIDENTES 25
6.5 RESPALDO Y RECUPERACIÓN DE DATOS 25
6.6 CONTINUIDAD DEL SERVICIO 25
6.7 FINALIZACIÓN 26
7 SUPERVISIÓN Y AUDITORÍA 26
ANEXO A. CUMPLIMIENTO DEL ENS 28
ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS 38
ANEXO C. REFERENCIAS 44

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 estándar. La migración a entornos web ha sido un catalizador para la externalización de los sistemas de información de un amplio número de organizaciones.
2. Como consecuencia de esta situación surge el modelo de servicios en la nube, como una propuesta tecnológica capaz de ofrecer servicios en red de forma ágil y flexible. 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.



3. Una de las definiciones de Servicios en la nube con mayor aceptación es la propuesta por el NIST [NIST SP-800-145]: "La provisión de servicios en la nube es un modelo para permitir el acceso por red, de forma práctica y bajo demanda, a un conjunto de recursos de computación configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser suministrados y desplegados rápidamente con una mínima gestión o interacción con el proveedor de servicio."
4. 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 flexibilidad en asignación de recursos y un ahorro económico significativo.
5. Existen diversas modalidades de servicios en la nube, tanto en lo referente al modelo de despliegue (privada, pública, comunitaria o híbrida) como en los categorías de servicio que se ofrecen (*Infrastructure-as-a-Service (**IaaS**), Platform-as-a-Service (**PaaS**) o Software-as-a-Service (**SaaS**)).*

6. Esta guía recoge los aspectos de seguridad necesarios que deberán contemplarse para la adopción de la nube como paradigma tecnológico para la disposición de servicios con las garantías de seguridad pertinentes. Se han identificado las medidas de seguridad y los requisitos que deben cumplir los proveedores de servicios para dar cumplimiento tanto a los marcos legislativos aplicables, en especial el Esquema Nacional de Seguridad (ENS) [RD 3/2010] o la normativa vigente en materia de protección de datos personales [RD 1720/2007], como a los códigos de buenas prácticas o estándares reconocidos internacionalmente.

1.2 CARACTERÍSTICAS DE LOS SERVICIOS EN LA NUBE

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

8. 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. Además con el servicio en la nube, se permite a un cliente pagar solo por los recursos que utiliza, ya sea facturando en función de parámetros como los ciclos de procesador consumidos, el ancho de banda o las máquinas virtuales dedicadas, permitiendo además añadir o eliminar recursos de forma sencilla y en tiempo real.

9. Por otro lado, los servicios en la nube se caracterizan por la deslocalización de datos, donde la principal ventaja es que el cliente puede 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. De esta forma se pueden mantener copias del servidor repartidas en distintos puntos del planeta tanto para mejorar los tiempos de acceso como para evitar pérdidas de datos o servicios por la caída de un centro de proceso. Como veremos, esta deslocalización tiene implicaciones de seguridad que las organizaciones deben evaluar convenientemente antes de hacer uso de servicios en la nube.

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

11. **Auto-servicio a demanda.** El cliente puede ajustar la capacidad necesaria de forma unilateral, sin necesidad de involucrar al personal del proveedor.

12. **Amplio acceso a través de redes.** Acceso estándar a través de redes, habilitando todo tipo de dispositivos de acceso: teléfonos, *tablets*, portátiles, equipos personales, servidores, etc.

13. **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).

14. **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.

15. **Servicio consumido.** El proveedor puede controlar el servicio prestado efectivo en cada momento, al nivel de abstracción que se especifique por contrato; por ejemplo, capacidad de almacenamiento, capacidad de procesamiento, ancho de banda, cuentas de usuario, etc. El uso de recursos puede ser monitorizado, controlado y reportado, proporcionando una gran transparencia tanto para el proveedor como para el consumidor del servicio utilizado.
16. 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. Si bien esto es considerado generalmente como una ventaja, debe tenerse en cuenta que esta característica nunca debe conllevar una pérdida del control de la información, o una despreocupación por la seguridad, debido a que la responsabilidad final siempre recae en el organismo contratante. A la hora de contratar estos servicios es fundamental estudiar adecuadamente las condiciones del servicio y las medidas de seguridad aplicadas para confirmar que son adecuadas para los requisitos exigidos a la organización cliente.

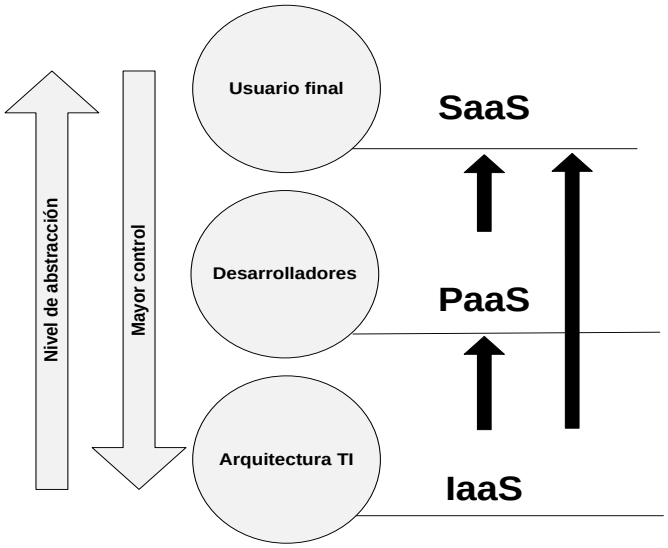
1.3 MODELOS DE DESPLIEGUE

17. Ante el abanico de despliegues posibles a la hora de crear un entorno de servicios en la nube, han clasificado las infraestructuras en públicas, privadas, comunitarias o híbridas; a continuación explicaremos cada uno de estos tipos de infraestructura.
18. **Nube pública**: La infraestructura de esta nube está disponible para el público en general o para un gran grupo de industria y dicha infraestructura la controla un proveedor de servicios en la nube.
19. **Nube privada**: La infraestructura de esta nube es operada únicamente por y para una organización.
20. **Nube comunitaria**: La infraestructura de esta nube es compartida por varias organizaciones relacionadas entre ellas y que comparten requisitos de servicio. Uno de los miembros del colectivo controle los recursos.
21. **Nube híbrida**: Es la composición de dos o más modelos, por ejemplo privada y pública, que permanecen como entidades únicas pero que coexisten por tener tecnología que permite compartir datos o aplicaciones entre las mismas.

1.4 CATEGORÍAS DE SERVICIO

22. Se ofrecen una serie de categorías de servicio que se detallan a continuación:
23. ***IaaS*** *(Infrastructure as a Service)*. Se encarga de entregar una infraestructura al usuario, normalmente mediante una plataforma de virtualización. 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 virtualizados.
24. ***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.
25. ***SaaS*** *(Software as a Service).* El *CSP* es el encargado de ofrecer al cliente el software como un servicio. Las aplicaciones son accesibles desde varios dispositivos cliente a través de una interfaz de cliente ligero, como por ejemplo un navegador web; el cliente no

administra ni controla la infraestructura en que se basa el servicio que utiliza. Las suites ofimáticas a las que se puede acceder online son un buen ejemplo de este modelo.



26. En términos generales, en función del tipo de servicio contratado, conforme va incrementándose el nivel de abstracción disminuye el control que el cliente tiene sobre la infraestructura. Del mismo modo cuanto mayor control tiene la organización cliente sobre la infraestructura que proporciona el servicio, mayor nivel de seguridad y control puede aplicar sobre ésta y por tanto sobre la información tratada.

1.5 ASPECTOS RELATIVOS A LA SEGURIDAD DE LA INFORMACIÓN

27. La adopción de servicios en la nube como estrategia para soportar los servicios 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; 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 existentes, 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.

28. En línea con lo anteriormente citado en relación al cumplimiento de requisitos de seguridad, 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. 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, detallado más adelante en esta guía. 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.

29. Esta guía centra su contenido en identificar los requisitos que un organismo debe solicitar a un prestador de servicios en la nube para que la contratación de servicios esté alineada con el ENS y la LOPD, garantizando la seguridad tanto de la información como de los servicios prestados por el organismo. Como referencia principal para identificar las medidas a tener en cuenta se seguirán los aspectos que son de aplicación en el ENS, es decir, gestión de riesgos, la gestión de servicios externos [op.ext], el cumplimiento de las medidas del ANEXO II del ENS que sean de aplicación y otros requisitos legales como los provenientes de la LOPD.

2 REQUISITOS DE SEGURIDAD

2.1 ROLES Y FUNCIONES

30. El Responsable de la Información y el Responsable del Servicio son funciones propias del organismo, individuales o colegiadas, que deben ser ejercidas por el organismo, en cuanto establecen los requisitos de seguridad de acuerdo a la legislación y normativa vigente y son los últimos responsables de rendir de cuentas. Ver guía CCN-STIC-801.

31. La figura del Responsable de la Seguridad puede ser múltiple. Debe existir un Responsable de la Seguridad dentro del organismo. Este responsable tendrá como interlocutor al Responsable de la Seguridad del CSP.

32. La figura de Responsable del Sistema puede ser múltiple, siendo el organismo responsable de la operación de sus medios propios y de la contratación de productos y servicios. El responsable del sistema del CSP tiene idéntica responsabilidad sobre sus medios y contrataciones.

33. El Responsable de la Información del organismo contratante deberá prestar especial atención y aprobar el uso de recursos externos, en especial aquellos que se encuentren en diferentes ubicaciones geográficas, cerciorándose de que se garantizan los deberes y obligaciones de custodia y la capacidad de persecución de incumplimientos legales, normativos y contractuales.

34. El Responsable de la Seguridad deberá cerciorarse de que puede garantizar la capacidad efectiva del organismo de resolver incidentes, en particular cuando el CSP recurre a equipos o servicios en diferentes jurisdicciones.

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

36. A menudo aparecen en el despliegue proveedores de comunicaciones (por ejemplo, ISP – Internet Service Providers). A estos se les considerará proveedores con igual responsabilidad sobre los medios que le son propios.

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

2.2 CATEGORIZACIÓN (ENS - ANEXO I)

38. El organismo categorizará sus sistemas según el Anexo I del ENS. Esta labor corresponde a los Responsables de la Información y de los Servicios.

39. Los requisitos o niveles de seguridad en términos de Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad se propagarán a los elementos que los soporten, sean propios del organismo, sean de un CSP contratado, o sean de una cadena de subcontratación entre CSPs.

40. La propagación del valor puede verse truncada si se emplean técnicas apropiadas tales como

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

41. Un escenario habitual es el de servicios de almacenamiento en la nube, sin tratamiento de datos en la nube. En este caso es recomendable que todos los datos se cifren antes de salir del organismo, de forma que los requisitos de seguridad sobre los proveedores se reducen a la dimensión de disponibilidad. El organismo será el único en poder de las claves de cifra, a las que aplicará lo previsto en el Anexo II del ENS.

dimensión	**D**	**I**	**C**	**A**	**T**
organismo	la que corresponda	la que corresponda	la que corresponda	la que corresponda	la que corresponda
CSP	la que corresponda	n.a.	n.a.	n.a.	n.a.

2.2.1 COMUNIDADES

42. Vamos a definir 3 comunidades de usuarios de servicios en la nube.

43. Comunidad BAJA. Formada por aquellos usuarios que transfieren al CSP unos requisitos de seguridad no superiores a nivel BAJO en cualquiera de las dimensiones I, C, A o T.

44. Comunidad MEDIA. Formada por aquellos usuarios que transfieren al CSP unos requisitos de seguridad no superiores a nivel MEDIO en cualquiera de las dimensiones I, C, A o T.

45. Comunidad ALTA. Formada por aquellos usuarios que transfieren al CSP unos requisitos de seguridad no superiores a nivel ALTO en cualquiera de las dimensiones I, C, A o T.

dimensión	**I**	**C**	**A**	**T**
Comunidad BAJA	≤ BAJO	≤ BAJO	≤ BAJO	≤ BAJO
Comunidad MEDIA	≤ MEDIO	≤ MEDIO	≤ MEDIO	≤ MEDIO
Comunidad ALTA	≤ ALTO	≤ ALTO	≤ ALTO	≤ ALTO

46. Cada CSP indicará a qué comunidad puede prestar servicios. Un CSP puede proporcionar diferentes servicios con diferentes niveles de servicio. Diremos que soporta diferentes comunidades. Más adelante se imponen algunas restricciones sobre los elementos que pueden compartirse entre diferentes comunidades.

47. Los usuarios sólo podrán utilizar servicios en la nube de un CSP si sus niveles de seguridad en las dimensiones I, C, A y T son soportables por la comunidad correspondiente.

2.3 RECOMENDACIONES

48. Sin tener un carácter obligatorio, se pueden recomendar los siguientes puntos.

49. Las claves de cifra no se almacenarán en claro en la nube, ni se utilizarán en aplicaciones que se ejecuten en la nube.

50. El proceso de autorización de usuarios (altas, bajas y gestión de derechos de acceso) no se realizará en la nube.

51. Las aplicaciones de firma electrónica y de sellos de tiempo no se ejecutarán en CSPs de carácter general, sino con los medios propios o de terceras partes de confianza de acuerdo a la legislación aplicable en la materia.

52. Los registros de la actividad de los usuarios se tratarán de forma específica, preferentemente reteniéndolos en el propio organismo; es decir, que no estén hospedados en el CSP.

2.4 MEDIDAS DE PROTECCIÓN (ENS - ANEXO II)

53. A efectos de disponibilidad, el CSP queda obligado a cumplir todas las medidas del Anexo II del ENS pertinentes para el nivel de disponibilidad requerido por el cliente.

54. A efectos de Integridad, Confidencialidad, Autenticidad y Trazabilidad, el CSP queda obligado a cumplir todas las medidas del Anexo II del ENS pertinentes para esa valoración en todas las dimensiones citadas. Es decir:

dimensión	**I**	**C**	**A**	**T**
Comunidad ALTA	ALTO	ALTO	ALTO	ALTO
Comunidad MEDIA	MEDIO	MEDIO	MEDIO	MEDIO
Comunidad BAJA	BAJO	BAJO	BAJO	BAJO

2.5 RESTRICCIONES ADICIONALES

55. El CSP debe cumplir el Anexo II del ENS en la medida en que disponga de los tipos de activos correspondientes. Esto incluye instalaciones y personal. Las citadas medidas de seguridad podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (ENS - Anexo I) y se satisfacen los principios básicos recogidos en el Capítulo II.

56. En particular, el CSP elaborará un análisis de riesgos según [op.pl.1].

57. Los elementos virtualizados y los elementos de virtualización se tratarán igual que los elementos físicos correspondientes a efectos de configuración, mantenimiento, reglas de seguridad y aspectos regulatorios.
58. Las imágenes de los elementos virtuales se tratarán como datos con los mismos requisitos de seguridad que la información y los servicios manejados por dichos elementos virtuales.
59. Debe cumplir los requisitos de la norma CCN-STIC 811 relativa a interconexión, en función de la categoría del sistema propio y del otro lado de la interconexión.

2.5.1 COMUNIDAD BAJA

60. Los componentes de seguridad del tipo DMZ, cortafuegos o agentes (proxy) no deberán residir en la misma máquina base que los componentes de producción.
61. El perímetro de la red física que soporte la comunidad cumplirá los requisitos de la guía CCN-STIC-811 relativa a puntos de interconexión.
62. Se registrarán todas las actuaciones de creación, traslado, activación y destrucción de elementos virtuales. Así mismo se registrará el montaje y la retirada de soportes de información, físicos o virtuales.
63. Los requisitos de identificación y autenticación del administrador del hipervisor corresponderán a los de un sistema de categoría MEDIA según el ENS.
64. Implicaciones (o ejemplos)
65. La red dedicada a usuarios ENS es una red físicamente diferenciada de otras redes que pueda tener el proveedor.
66. Si el usuario contrata una interconexión al proveedor, por ejemplo a Internet, el proveedor tendrá una máquina separada que preste los servicios de frontera.

2.5.2 COMUNIDAD MEDIA

67. Además de los requisitos para Comunidad BAJA:
68. No se compartirán equipos base con otras comunidades.
69. No se compartirá el mismo hipervisor con otras comunidades.
70. La administración del hipervisor estará separada de la administración de los elementos virtualizados: diferentes interfaces, diferentes cuentas de administrador, y diferentes administradores.
71. Los requisitos de identificación y autenticación del administrador del hipervisor corresponderán a los de un sistema de categoría ALTA según el ENS.

2.5.3 COMUNIDAD ALTA

72. Además de los requisitos para Comunidad MEDIA:
73. La red administrativa estará separada lógica (red privada virtual) o físicamente (red específica) de la red administrativa de otras comunidades.

3 REQUISITOS DERIVADOS DE LA EXISTENCIA DE DATOS DE CARÁCTER PERSONAL

74. En lo referente a protección de datos de carácter personal, siempre que en la prestación de servicio se contemple la posibilidad de que la nube pueda albergar datos personales deberán cumplirse, de forma adicional a los requisitos expuestos por el ENS, los requisitos establecidos tanto por la LOPD [Ley 15/1999] como por el Reglamento que la desarrolla [RD 1720/2007]. Estos requisitos están definidos en el artículo 12 de la LOPD y en el artículo 82 del RDLOPD, debiendo ser suscritos contractualmente.

75. La Agencia Española de Protección de datos [AEPD] elaboró en 2013 una guía sobre el tratamiento de datos en servicios de *"cloud computing"*. Cabe destacar algunos puntos de la misma:

1	**¿Qué debo analizar y tener en cuenta antes de contratar servicios de 'cloud computing'?**
	- debe decidir para qué datos personales contratará servicios de *cloud computing* y cuáles prefiere mantener en sus propios sistemas de información. Esta decisión es importante porque delimitará las finalidades para las que el proveedor de *cloud* puede tratar los datos. En consecuencia, debe garantizarse expresamente que no utilizará los datos para otra finalidad que no tenga relación con los servicios contratados.
2	**Desde la perspectiva de la normativa de protección de datos, ¿cuál es mi papel como cliente de un servicio de 'cloud'?**
	- El cliente que contrata servicios de *cloud computing* sigue siendo responsable del tratamiento de los datos personales. Aunque los contrate con una gran compañía multinacional la responsabilidad no se desplaza al prestador del servicio, ni siquiera incorporando una cláusula en el contrato con esta finalidad. - El que ofrece la contratación de *cloud computing* es un prestador de servicios que en la ley de protección de datos tiene la calificación de 'encargado del tratamiento'.
3	**¿Cuál es la legislación aplicable?**
	- El cliente que contrata servicios de *cloud computing* sigue siendo responsable del tratamiento de los datos por lo que la normativa aplicable al cliente y al prestador del servicio es la legislación española sobre protección de datos (Ley Orgánica 15/1999, de 13 de diciembre y Reglamento de desarrollo –RLOPD– aprobado por R.D. 1720/2007). - La aplicación de la legislación española no puede modificarse contractualmente. - Aunque le informen de que los datos personales están disociados, no cambia la ley aplicable ni la responsabilidad del cliente y del prestador del servicio.
4	**¿Cuáles son mis obligaciones como cliente?**
	- Debe solicitar y obtener información sobre si intervienen o no terceras empresas (subcontratistas) en la prestación de servicios de *cloud computing*. Lo habitual es que intervengan terceras empresas. De ser así: o Tiene que dar su conformidad a la participación de terceras empresas, al

	menos delimitando genéricamente los servicios en los que participarán (p. ej. en el alojamiento de datos). Para ello, el prestador del servicio de *cloud computing* tiene que informarle sobre la tipología de servicios que pueden subcontratarse con terceros. ○ Tiene que poder conocer las terceras empresas que intervienen (p. ej. pudiendo acceder a una página web o a través de otras opciones que le facilite el prestador del servicio). ○ El proveedor de *cloud* debe asumir en el contrato que los subcontratistas le ofrecen garantías jurídicas para el tratamiento de los datos equivalentes a los que él mismo asume. - El contrato que firma ha de incorporar cláusulas contractuales para la protección de los datos personales según se detalla en las siguientes preguntas.
5	**¿Dónde pueden estar ubicados los datos personales?** **¿Es relevante su ubicación?**
	- La localización de los datos tiene importancia porque las garantías exigibles para su protección son distintas según los países en que se encuentren. - Los países del Espacio Económico Europeo ofrecen garantías suficientes y no se considera legalmente que exista una transferencia internacional de datos. El Espacio Económico Europeo está constituido por los países de la Unión Europea e Islandia, Liechtenstein y Noruega. - Si los datos están localizados en países que no pertenecen al Espacio Económico Europeo habría una transferencia internacional de datos, en cuyo caso, y dependiendo del país en que se encuentren, deberán proporcionarse garantías jurídicas adecuadas.
6	**¿Qué garantías se consideran adecuadas para las transferencias internacionales de datos?**
	- Se considera una garantía adecuada que el país de destino ofrezca un nivel de protección equivalente al del Espacio Económico Europeo y así se haya acordado por la Agencia Española de Protección de Datos o por Decisión de la Comisión Europea. En ese caso será suficiente con hacer constar la transferencia en la notificación del fichero realizada a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos. - Las proporcionadas por las empresas ubicadas en los Estados Unidos que hayan suscrito los principios de Puerto Seguro. Al igual que en el caso anterior será suficiente con hacer constar la transferencia en la notificación del fichero a la Agencia Española de Protección de Datos. - En otro caso, la transferencia internacional de datos necesitará autorización del Director de la Agencia Española de Protección de Datos, que podrá otorgarse en caso de que el exportador de datos aporte garantías adecuadas. Pregunte al prestador de servicios de *cloud computing* si hay transferencias internacionales de datos y, en caso afirmativo, con qué garantías. - Cuando los datos están localizados en terceros países podría suceder que una Autoridad competente pueda solicitar y obtener información sobre los datos personales de los que el cliente es responsable. En este caso el cliente debería ser informado por el proveedor de esta circunstancia (salvo que lo prohíba la ley del país tercero).
7	**¿Qué medidas de seguridad son exigibles?**

	- Las medidas de seguridad son indispensables para garantizar la integridad de los datos personales, evitar accesos no autorizados y recuperar la información en caso de que se produzcan incidencias de seguridad. - El nivel de seguridad exigible depende de la mayor o menor sensibilidad de los datos personales. - Asimismo, el acceso a la información a través de redes de comunicaciones debe contemplar un nivel de medidas de seguridad equivalente al de los accesos en modo local. - Pregunte al proveedor de *cloud computing* sobre los niveles de seguridad que le ofrece y garantiza.
8	**¿Cómo puedo garantizar o asegurarme de que se cumplen las medidas de seguridad?**
	- Como cliente debe tener la opción de comprobar las medidas de seguridad, incluidos los registros que permiten conocer quién ha accedido a los datos de los que es responsable. - El proveedor de *cloud computing* le acredita que dispone de una certificación de seguridad adecuada. - Puede acordarse que un tercero independiente audite la seguridad. En este caso, debe conocerse la entidad auditora y los estándares reconocidos que aplicará. - Solicite información al proveedor de *cloud* sobre cómo se auditarán las medidas de seguridad. El cliente debe ser informado diligentemente por el proveedor de *cloud* sobre las incidencias de seguridad que afecten a los datos de los que el propio cliente es responsable, así como de las medidas adoptadas para resolverlas o de las medidas que el cliente ha de tomar para evitar los daños que puedan producirse (p. ej. informar a sus propios clientes sobre cómo proteger su información personal). - El cifrado de los datos personales es una medida que debe valorarse positivamente. Solicite información al proveedor de *cloud* sobre el cifrado de los datos.
9	**¿Qué compromisos de confidencialidad de los datos personales debo exigir?**
	- El proveedor del servicio de *cloud* debe comprometerse a garantizar la confidencialidad utilizando los datos sólo para los servicios contratados. - Asimismo debe comprometerse a dar instrucciones al personal que depende de él para que mantenga la confidencialidad.
10	**¿Cómo garantizo que puedo recuperar los datos personales de los que soy responsable (portabilidad)?**
	- La portabilidad significa que el proveedor ha de obligarse, cuando pueda resolverse el contrato o a la terminación del servicio, a entregar toda la información al cliente en el formato que se acuerde, de forma que éste pueda almacenarla en sus propios sistemas o bien optar porque se traslade a los de un nuevo proveedor en un formato que permita su utilización, en el plazo más breve posible, con total garantía de la integridad de la información y sin incurrir en costes adicionales. - En particular, el cliente debe tener la opción de exigir la portabilidad de la información a sus propios sistemas de información o a un nuevo prestador de *cloud* cuando considere inadecuada la intervención de algún subcontratista o

	la transferencia de datos a países que estime no aportan garantías adecuadas. - También es particularmente importante en los casos en que el proveedor de *cloud* modifique unilateralmente las condiciones de prestación del servicio dado su poder de negociación frente al cliente. - Solicite información y garantías al proveedor sobre la portabilidad de los datos personales.
11	**¿Cómo puedo asegurarme de que el proveedor de '*cloud*' no conserva los datos personales si se extingue el contrato?**
	- Deben preverse mecanismos que garanticen el borrado seguro de los datos cuando lo solicite el cliente y, en todo caso, al finalizar el contrato. (Un mecanismo apropiado es requerir una certificación de la destrucción emitido por el proveedor de *cloud computing* o por un tercero).
12	**¿Cómo puedo garantizar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO)?**
	- El cliente de *cloud computing*, como responsable del tratamiento de datos, debe permitir el ejercicio de los derechos ARCO a los ciudadanos. - Para ello, el proveedor de *cloud* debe garantizar su cooperación y las herramientas adecuadas para facilitar la atención de dichos derechos. - Infórmese sobre las condiciones que le ofrece el proveedor para cumplir con ese deber de cooperación para garantizar el ejercicio de estos derechos.

76. En cualquier caso, la Administración Pública cliente del servicio deberá tener en cuenta la Ley 30/1992 con respecto a los derechos de los ciudadanos de poder ejercer el derecho de acceso a la información personal contenida en archivos y registros administrativos. Los límites establecidos para el acceso de los ciudadanos quedan definidos en la Ley anteriormente citada; por tanto, se deberá garantizar el acceso a los datos de los ciudadanos, debiendo tomar además las medidas de seguridad y confidencialidad adecuadas.

4 NORMATIVA INTERNA

77. Se debe documentar, publicar y comunicar internamente a los usuarios del servicio los criterios de uso aceptable del servicio, incluyendo:

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

5 CONTRATACIÓN

78. En cuanto a la prestación de servicios en la nube por parte de un tercero la primera medida a implantar es la que recoge el apartado [op.ext.1] Contratación y acuerdos de nivel de servicio del Anexo II del ENS. Esta medida se encuentra desarrollada a su vez en la Guía CCN-STIC-804, Guía de implantación.

79. La medida recoge la necesidad de establecer una serie de requisitos contractuales en la prestación del servicio, debiendo contemplar las características del servicio prestado y las responsabilidades de ambas partes. A su vez se establecerán acuerdos de nivel de servicio para definir la calidad del servicio contratado.

80. Cabe tener en cuenta el Real Decreto Legislativo 3/2011 por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público, el cual regula los procedimientos de contratación de las Administraciones Públicas. Los servicios en la nube se encuentran tipificados como contratos de servicio, de acuerdo con el artículo 10 de dicho Real Decreto. La flexibilidad para realizar cambios sobre las características del servicio, así como el pago por uso, requieren la adaptación de los modelos contractuales por parte de las Administraciones Públicas. Estos contratos deberán reflejar al menos los siguientes aspectos:

- Descripción del servicio
- Tipo de servicio.
- Tipo de infraestructura.
- Capacidad del servicio.
- Protección de la información.
- Acuerdos de nivel de servicio (niveles, tiempos de respuesta, penalizaciones, etc.).
- Mecanismos de acceso al servicio.
- Responsabilidades y obligaciones
- Requisitos legales
- Requisitos para el cumplimiento del ENS
- Gestión de cambios
- Registro de actividad
- Gestión de incidentes
- Eliminación de información
- Respaldo y recuperación de datos
- Continuidad del servicio
- Finalización del servicio.
- Requisitos para la protección de datos personales

5.1 DESCRIPCIÓN DEL SERVICIO

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

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

5.1.1 TIPO DE SERVICIO

83. Para determinar el tipo de servicio se tendrán en cuenta las necesidades de la organización y en función de estas necesidades se deberá optar por un servicio IaaS, PaaS o SaaS de acuerdo a lo especificado en el punto 1.4. Algunos de los elementos a considerar para elegir el tipo de servicio son los siguientes:

84. Las soluciones SaaS proporcionan un software como servicio, integrando una gran cantidad de funciones y herramientas. La implementación se delega en el proveedor, así como gran parte de las medidas de seguridad a implantar.

85. Las soluciones PaaS proporcionan entornos para desplegar aplicaciones desarrolladas. La organización cliente dispone de más control sobre el entorno y por tanto es responsable final de la seguridad de las aplicaciones.

86. Por último las soluciones IaaS proporcionan una infraestructura, por norma general virtualizada, en la que el cliente es responsable del software que esa infraestructura soportará, incluyendo los sistemas operativos y aplicaciones base. En este modelo la implementación de la seguridad de la información en su mayor parte es responsabilidad de la organización cliente, por lo que a priori puede considerarse el modelo de servicio que mayor nivel de control proporciona a la organización.

5.1.2 TIPO DE INFRAESTRUCTURA

87. En cuanto al tipo de infraestructura, se deberá seleccionar la más adecuada para la organización en función del nivel de seguridad requerido.

88. Aunque en muchas ocasiones los criterios iniciales de migración de servicios a la nube son económicos, a la hora de determinar el tipo de infraestructura óptima para esta migración cada organismo deberá tener en cuenta criterios de seguridad que puedan determinar el tipo de infraestructura a elegir; en función de este tipo de infraestructura puede existir un uso de recursos de modo compartido con otras organizaciones, lo que puede comprometer la seguridad de la información albergada o simplemente no ser acorde a las políticas de seguridad definidas en la organización.

5.1.3 DIMENSIONADO DEL SERVICIO

89. El acuerdo contractual reflejará los recursos que conformarán el servicio. 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.

90. En el caso de PaaS y de IaaS es más frecuente medir la capacidad del servicio en términos de ciclos de CPU, 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, transferencia de datos…

91. 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. La organización debe definir y reflejar 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.

92. Por último, el CSP debe proporcionar herramientas u otros recursos que permitan a la organización contratante 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.

5.2 SUBCONTRATACIÓN

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

94. Ejemplos

- contratación de personal
- contratación de instalaciones
- contratación de servicios de comunicaciones
- contratación de servicios de copias de respaldo

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

96. Las obligaciones del proveedor en materia de seguridad se transmiten de forma transitiva a las partes subcontratadas. En particular los niveles de seguridad de la información a la que tenga acceso el proveedor, y de los servicios que de este último dependan. La parte subcontratada deberá atender a los requisitos de seguridad derivados del ENS según se recoge en la sección 2 de esta guía.

5.3 PROTECCIÓN DE LA INFORMACIÓN

97. El contrato debe determinar la propiedad de la información a la que va a tener acceso el proveedor, sea de la parte contratante o de terceras partes.

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

99. Por lo que respecta a la legislación que afecta a la contratación de servicios en la nube, es de aplicación al menos la legislación referente a

    - Protección de Datos de Carácter Personal, LOPD [Ley 15/1999] y su Reglamento de desarrollo [RD 1720/2007],
    - legislación referente a Servicios de la Sociedad de la Información (LSSI) [Ley 11/2007]
    - y legislación de cumplimiento obligatorio por Administraciones Públicas en el ámbito TIC: Esquemas nacionales de seguridad, ENS [RD 3/2010], e interoperabilidad, ENI [RD 4/2010].

5.4 ACUERDOS DE NIVEL DE SERVICIO

100. Deben acordarse unos niveles de servicio (*Service Level Agreement* - SLA). Estos SLAs deben ser aceptables para la organización cliente y el proveedor que los prestará y deberán reflejar aspectos referentes a capacidad, disponibilidad, continuidad o gestión de incidentes, así como peticiones de cambio, entre otros, con al menos los siguientes criterios.

101. 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.

102. Disponibilidad: se establecerán porcentajes de disponibilidad del servicio en función de la criticidad del mismo, identificándose si hubiera periodos críticos en los que se requieren mayores niveles de disponibilidad.

103. Se definirán tiempos de recuperación para los sistemas de información en línea con los criterios de valoración de disponibilidad de los servicios según el Anexo I del ENS.

104. 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.

105. 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.

106. Se determinará la periodicidad de los informes de cumplimiento de los SLA.

107. En el servicio de tipo COMUNIDAD ALTA, la parte contratante se reservará el derecho de auditar los datos y el proceso de recogida de información y elaboración de los indicadores acordados.

5.5 ACCESO AL SERVICIO

108. Se determinarán

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

5.6 CONDICIONANTES GEOGRÁFICOS

109. El contrato puede imponer condiciones sobre la ubicación geográfica de los servidores y/o de las líneas de comunicaciones en función de la información que vayan a acoger o a transportar respectivamente. Estas condiciones típicamente derivan de condicionantes legales respecto de la información (por ejemplo, en datos de carácter personal) o requisitos del propietario de la información.

110. Estas limitaciones suelen materializarse en la forma de países específicos, países que pertenecen a una cierta comunidad (por ejemplo Unión Europea) o países que han firmado ciertos tratados de colaboración.

111. En caso de que la información se almacene o se transmita de forma cifrada, se estará a lo determinado por el Anexo II del ENS.

5.7 RESPONSABILIDADES Y OBLIGACIONES

112. El contrato definirá los roles de las personas involucradas en la prestación del servicio, tanto en la parte del organismo contratante como del CSP.

113. A continuación se describen las responsabilidades mínimas que deberán estar cubiertas en cada caso.

114. Por parte del proveedor y del organismo contratante, se deben considerar las siguientes responsabilidades mínimas. Al tratarse de procedimientos de coordinación, ambas partes deben definir a sus relativos interlocutores.

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

5.8 REGISTRO DE ACTIVIDAD

115. Uno de los aspectos que persigue el ENS es disponer de trazabilidad de las acciones realizadas sobre los sistemas de información. De esta manera y también en línea con lo definido por el RDLOPD en su artículo 103 Registro de accesos, los sistemas proporcionados por el CSP deberán disponer de registros de acceso que permitan monitorizar, analizar, investigar y documentar acciones indebidas o no autorizadas, tanto a nivel operativo como de administración.

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

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

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

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

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

121. En el servicio de tipo COMUNIDAD ALTA, la parte contratante se reservará el derecho de requerir una auditoría de que los procesos de registro y tratamiento de los registros sean acordes a lo contratado. Las condiciones exactas por las cuales se pueda requerir una auditoría se fijarán por contrato, cubriendo tanto auditorías rutinarias (periódicas) como singulares en caso de incidente grave de seguridad.

5.9 FINALIZACIÓN DEL SERVICIO

122. El contrato especificará las condiciones, procedimientos y plazos para una terminación pactada y una terminación abrupta por incumplimiento de los supuestos contractuales.

123. La finalización del servicio deberá estar recogida en la descripción del propio servicio, identificando la necesidad que pueda existir de que el proveedor devuelva la información a la finalización de la relación contractual y debiendo constar esto en una cláusula junto al tiempo que tardará el proveedor en realizar la migración de los datos. A este respecto se buscará la “neutralidad tecnológica” del servicio que facilite todo tipo de retorno o migración.

124. Deberá estar recogida la necesidad de que el proveedor elimine la información a la finalización de la relación contractual y debiendo constar esto en una cláusula junto a los mecanismos y el tiempo que tardará el proveedor en realizar la destrucción de los datos. Estas cláusulas deben recoger las obligaciones de retención de datos que pudieran ser obligatorias por política o por imperativo legal, indicando los periodos correspondientes y

las obligaciones del proveedor en lo que respecta a confidencialidad y control de acceso. Por último deben recogerse las obligaciones del proveedor para garantizar que la destrucción es efectiva; por ejemplo auditorías.

6 OPERACIÓN

6.1 PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD

125. Algunas operaciones del servicio deben ser realizadas de forma conjunta por ambas partes: contratada y contratante, debiendo establecerse los roles, responsabilidades (capacidad de autorizar y obligación de rendir cuentas) y protocolos adecuados para llevarlas a cabo.

126. Cabe destacar las siguientes actividades, sin que sean las únicas a procedimentar:

- [op.exp.2 y op.exp.3] Configuración de seguridad
- [op.exp.4 y op.exp.5] Mantenimiento y gestión de cambios
- [op.exp.7] Gestión de incidentes
- [op.cont] Continuidad – Recuperación de desastres
- [mp.per] Gestión del personal
- [mp.info.9] Recuperación de datos de copias de seguridad

6.2 SEGUIMIENTO DEL SERVICIO

127. En los servicios prestados por terceros a la organización, tan importante es el acuerdo contractual con el proveedor de servicios como el seguimiento a realizar sobre el servicio prestado. Para poder tener el control de los servicios, y por tanto también poder exigirle al proveedor el cumplimiento de cualesquiera medidas de seguridad aplicables, es necesaria una monitorización de los mismos.

128. Esto se encuentra reflejado en el punto [op.ext.2.] del Anexo II del ENS Gestión diaria y especifica tres aspectos principales a seguir:

- La medición del cumplimiento del servicio y el procedimiento para restaurar las desviaciones estipuladas contractualmente.
- El proceso de coordinación para el mantenimiento de los sistemas implicados.
- El proceso de coordinación ante incidentes o desastres.

129. En cuanto al primer aspecto y dadas las características de la prestación de servicios en la nube, en ocasiones con aspectos relevantes fuera del control de la organización cliente y también dada su forma de pago, en función del uso, es muy importante reflejar de un modo claro los términos del cumplimiento. Es necesario identificar en el contrato los derechos de la organización cliente para poder monitorizar el funcionamiento del servicio y de este modo poder comprobar el cumplimiento de las medidas de seguridad, los controles y las políticas que garantizan la integridad, confidencialidad y disponibilidad de los datos, y del mismo modo poder realizar la comprobación de que el nivel de prestación es el pactado. La definición y el control de los SLAs son vitales para poder garantizar el cumplimiento de lo estipulado en el contrato.

130. La organización debe monitorizar de forma independiente el cumplimiento de los términos establecidos en el contrato, bien a través de controles técnicos propios o a través de la

revisión y aprobación periódica de los informes de servicio proporcionados por el CSP. Es necesario ejecutar esta monitorización sobre al menos los siguientes controles de seguridad y servicio con independencia de la categoría del sistema:

- Niveles de calidad, disponibilidad y capacidad del servicio ofrecido, incluyendo el cumplimiento de las obligaciones de servicio acordadas y la respuesta ofrecida por el proveedor ante desviaciones significativas.
- Gestión de incidentes de seguridad, incluyendo toda la información necesaria para determinar orígenes, objetivos, riesgos… asociados a cualquier incidente relevante.
- Controles de acceso a los servicios, incluyendo listado actualizado de usuarios autorizados para utilizar los servicios disponibles, y los privilegios asociados en cada caso.
- Cumplimiento normativo y legislativo entre el prestador y el cliente de los servicios, incluyendo los aspectos de cumplimiento de aplicación sobre el prestador que correspondan en cada caso, como auditorías LOPD, ISO, financieras…
- Situación actualizada de las medidas de protección de la información establecidas por el proveedor, incluyendo aspectos de seguridad física, protección contra software malicioso, seguridad del personal, copias de seguridad…
- Mecanismos de comprobación regular de los controles de seguridad por parte del proveedor y resultados de dichas comprobaciones.

131. Toda la información de los controles anteriores proporcionada periódicamente por el proveedor de servicios debe incluir de forma obligatoria cualesquiera anomalías o desviaciones significativas producidas durante el periodo, así como las acciones ejecutadas en cada caso como respuesta a estas situaciones susceptibles de introducir riesgos en la organización. Adicionalmente, debemos solicitar al proveedor de servicios la información de auditoría y no conformidades de aplicación en cada caso para poder verificar que las medidas de seguridad tomadas por éste son las correctas y oportunas para solventar desviaciones halladas durante el proceso de auditoría.

6.3 GESTIÓN DE CAMBIOS

132. Otro aspecto a tratar en la gestión diaria del servicio es el referente a la gestión y coordinación del mantenimiento de los sistemas. En este sentido se deberá establecer contractualmente de acuerdo con los requisitos mínimos del ENS, la obligación de mantener actualizados los sistemas para garantizar el correcto funcionamiento de los mismos, así como eliminar las posibles vulnerabilidades que puede afectar a los sistemas.

133. Deberá definirse un procedimiento de coordinación en el mantenimiento de sistemas entre ambas partes para prevenir paradas o errores en la prestación del servicio; este procedimiento estará en línea con el proceso de gestión de cambio e incluirá la notificación con suficiente antelación de la realización de mantenimientos por parte del proveedor, identificando los tiempos en los que puede interrumpirse el servicio. La notificación se realizará previa y posteriormente al mantenimiento y tras éste se pedirá al cliente conformidad del correcto funcionamiento del servicio.

134. Por otra parte siempre que el mantenimiento o actualización implique un cambio mayor o pueda suponer el funcionamiento incorrecto de los sistemas de la organización cliente, el proveedor habilitará previamente un entorno actualizado para que el cliente puede verificar el correcto funcionamiento de sus sistemas en preproducción. Además el proveedor deberá

informar periódicamente de los mantenimientos y actualizaciones realizados en los sistemas que albergan los sistemas del cliente.

6.4 GESTIÓN DE INCIDENTES

135. De acuerdo con el ENS y con el RDLOPD, el proveedor deberá disponer de un procedimiento de gestión de incidentes [op.exp.7]. Se deberá informar a la organización cliente de:

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

136. Deberá definirse un procedimiento de coordinación ante incidentes que puedan afectar a los sistemas del cliente, procedimiento que deberá contemplar los flujos de información y las interacciones entre cliente y proveedor durante la gestión del incidente. A su vez el proveedor deberá informar periódicamente de los incidentes que han afectado a los sistemas que soportan los sistemas del cliente.

137. En los niveles de servicio COMUNIDA MEDIA o ALTA, en el caso de incidentes que afecten a la información o a los servicios del organismo contratante, el proveedor deberá facilitar toda la información forense necesaria para analizar el incidente y su gestión.

6.5 RESPALDO Y RECUPERACIÓN DE DATOS

138. En línea con lo especificado por el ENS y por el RDLOPD, el proveedor deberá disponer de un procedimiento de copias de respaldo que garantice la restauración de la información como describe [mp.info.9]. El proveedor deberá informar a la organización cliente de:

- 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).

6.6 CONTINUIDAD DEL SERVICIO

139. De acuerdo con el ENS los sistemas afectados deberán disponer de medidas para la continuidad del servicio [op.cont.2]. Si bien los niveles de disponibilidad, así como los tiempos de recuperación en la prestación de servicios, se encuentran recogidos contractualmente a través de los SLAs, se deberá solicitar al proveedor evidencia de la existencia de un plan de continuidad de negocio que garantice la restauración de los servicios. El proveedor deberá informar a la organización cliente de:

- Existencia de plan de continuidad de negocio.
- Evidencia satisfactoria de la ejecución periódica de pruebas de continuidad.

- Análisis de impacto del servicio proporcionado.

140. Cabe destacar que en la sección referente a servicios externos, descrito en el punto [op.ext] del Anexo II del ENS, se detallan los requisitos que deben cumplir en este ámbito.

141. Sin perjuicio de que el CSP cumpla los requisitos previstos en el Anexo II del ENS relativos a continuidad del servicio y medios alternativos, se considerarán los siguientes aspectos en función del nivel de disponibilidad requerido:

142. Se deberá requerir al proveedor evidencia de la existencia de un plan de continuidad de negocio cuyo alcance incluya los servicios objeto de la prestación.

143. Se exigirá constancia de que los tiempos de recuperación identificados en el análisis de impacto están alineados con los criterios definidos en los SLAs en cuanto a tiempo de recuperación del servicio.

144. Deberá definirse un procedimiento de coordinación ante incidentes y desastres que puedan afectar a los sistemas del cliente, procedimiento que deberá contemplar los flujos de información y las interacciones entre cliente y proveedor durante la gestión tanto de incidentes como de desastres. A su vez el proveedor deberá informar periódicamente de los incidentes que han afectado a los sistemas que soportan los sistemas del cliente.

145. Se realizarán pruebas periódicas que involucren al organismo y a los diferentes proveedores y subproveedores para validar el correcto funcionamiento de los planes y el cumplimiento de los plazos y servicios mínimos previstos

6.7 FINALIZACIÓN

146. Salvo cuando la parte contratante disponga de una copia actualizada de su información, se deberán establecer los procedimientos para que la parte contratante recupere la información entregada al proveedor. En estos procedimientos se deben acotar formatos de datos y tiempos.

147. Salvo cuando la parte contratante no haya transferido información en claro al proveedor, se deberán establecer procedimientos para la eliminación de las copias en los equipos del proveedor. Estos procedimientos deben incluir los mecanismos de borrado y las garantías de que han sido aplicados correctamente. Los tiempos de destrucción de la información deberán tener en cuenta los requisitos legales de retención, si los hubiera.

148. Los procedimientos anteriores deben tener en el proveedor la parte correspondiente para prolongarlos a posibles terceros proveedores subcontratados.

7 SUPERVISIÓN Y AUDITORÍA

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

- Una declaración de aplicabilidad de las medidas a aplicar.
- Una auditoría que verifique mediante evidencias el cumplimiento de las medidas de seguridad del Anexo II del ENS que sean de aplicación de acuerdo con el nivel del sistema.

- Auditorías de cumplimiento de normativa necesaria para satisfacer los requisitos de seguridad de la información del organismo contratante. Por ejemplo, LOPD, SAS70, PCI-DSS, etc.

150. Las auditorías recogidas en el punto anterior tendrán carácter obligatorio en el nivel de servicio denominado COMUNIDAD ALTA.

151. En cualquier caso, deberá requerirse siempre al proveedor que cumpla los principios y los requisitos mínimos establecidos por el ENS.

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

- Auditorías recomendadas por ENISA para proveedores de servicios en la nube [ENISA-CCSL]
- Sistema de Gestión de la Seguridad de la Información (SGSI) [ISO/IEC 27001:2013]
- Sistema de Gestión de la Continuidad [ISO 22301:2012]
- *Cloud Controls Matrix* [CCM]

153. El Anexo A recoge los controles de las normas 27002 y la matriz CCM, junto con su correspondencia para satisfacer los requisitos del ENS. Cabe esperar que futuras versiones de esta guía incorporen otros perfiles de seguridad que tengan un respaldo internacional bien de iure, bien de facto.

ANEXO A. CUMPLIMIENTO DEL ENS

nivel	comentario
0	cubierto siempre conviene validar que se contemplan los detalles específicos del ENS
1	probablemente cubierto hay que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo; pero cabe esperar que el esfuerzo adicional sea marginal
2	probablemente se necesite completar hay que verificar que se cubren todos y cada uno de los aspectos contemplados en el ENS para los niveles de seguridad requeridos por el sistema y la categoría del mismo; pero cabe esperar que el esfuerzo adicional sea significativo
3	no cubierto son aspectos que no se cubren en los controles de la norma 27002 ni en los requisitos de la norma 27001, por lo que deberán ser objeto de una auditoría específica

MEDIDAS DE SEGURIDAD		ISO 27000			CCM	
org	Marco organizativo	nivel	2005	2013	nivel	v3
org.1	Política de seguridad	1	27001: • 4.2.1 • 5.1 27002: • 5.1.1 • 5.1.2 • 6.1.1 • 6.1.2 • 6.1.3 • 15.1.1	27001: • 4 • 5.2 • 5.3 27002: • 6.1.1 • 18.1.1	1	GRM-05 GRM-09

MEDIDAS DE SEGURIDAD		ISO 27000			CCM	
org.2	Normativa de seguridad	1	27002: • 6.1.7 • 7.1.3 • 13.2.1 • 15.2.1	27002: • 5.1.1 • 5.1.2 • 6.1.4 • 8.1.3 • 10.8.1 • 11.4.1 • 13.2.1 • 15.1.1 • 16.1.1 • 18.2.2	1	DSI-02 GRM-06 HRS-09 MOS-03 MOS-05
org.3	Procedimientos de seguridad	1	27002: • 6.1.6 • 10.1.1 • 13.2.1 • 15.1.2 • 15.2.2	27002: • 6.1.3 • 12.1.1 • 13.2.1 • 16.1.1 • 18.1.2 • 18.2.3	1	DSI-02 GRM-06 HRS-09 MOS-07
org.4	Proceso de autorización	1	27002: • 6.1.4 • 6.2.3 • 10.6.1 • 10.6.2 • 10.7.1 • 10.7.3 • 12.4.1 • 12.5.3	27002: • 6.1.1 • 6.2.1 • 8.2.3 • 8.3.1 • 12.5.1 • 12.6.2 • 13.1.1 • 13.1.2 • 14.2.4	1	CCC-01 CCC-04 IAM-09 MOS-02 MOS-04 MOS-06

MEDIDAS DE SEGURIDAD		ISO 27000			CCM	
op	**Marco operacional**					
op.pl	Planificación					
op.pl.1	Análisis de riesgos	1	27001: • 4.2.1 • 4.2.2 27002: • 6.2.1 • 6.2.2 • 10.8.5	27001: • 6.1 • 6..1 • 6.1.2 • 6.1.3 • 8.2 • 8.3	1	DSI-02 GRM-02 GRM-08 GRM-10 GRM-11 GRM-12 IAM-07
op.pl.2	Arquitectura de seguridad	1	27002: • 7.1.1 • 7.1.2 • 10.6.1 • 10.7.4 • 12.2.1 • 12.2.2 • 12.2.3 • 12.2.4	27002: • 8.1.1 • 8,1,2 • 13.1.1 • 14.2.5	1	AIS-03 BCR-04 GRM-04 IVS-09
op.pl.3	Adquisición de nuevos componentes	2	27002: • 12.1.1	27002: • 14.1.1	3	no
op.pl.4	Dimensionamiento / Gestión de capacidades	1	27002: • 10.3.1	27002: • 12.1.3	1	IVS-04 STA-03
op.pl.5	Componentes certificados	3	27002: • 12.1.1	no	3	no
op.acc	Control de acceso					
op.acc.1	Identificación	1	27002: • 11.2.1 • 11.5.2	27002: • 9.2.1	1	EKM-01 IAM-04 IAM-08
op.acc.2	Requisitos de acceso	1	27002: • 11.1.1 • 11.5.4 • 11.6.1 • 12.4.3 • 15.1.5	27002: • 9.1.1 • 9.1.2 • 9.4.1 • 9.4.4 • 9.4.5	1	IAM-02 IAM-03 IAM-10 IAM-11 IAM-12 IVS-09
op.acc.3	Segregación de funciones y tareas	0	27002: • 10.1.3	27002: • 6.1.2	0	IAM-05
op.acc.4	Proceso de gestión de derechos de acceso	1	27002: • 8.3.3 • 11.1.1 • 11.2.2 • 11.2.4	27002: • 9.2.2 • 9.2.3 • 9.2.5 • 9.2.6	1	IAM-02 IAM-04 IAM-10 IAM-13 IVS-11

MEDIDAS DE SEGURIDAD		ISO 27000			CCM	
op.acc.5	Mecanismo de autenticación	3	27002: • 11.2.3 • 11.3.1 • 11.5.2 • 11.5.3	27002: • 9.2.4 • 9.3.1 • 9.4.3	3	MOS-16
op.acc.6	Acceso local (local logon)	1	27002: • 11.5.1	27002: • 9.4.2	3	no
op.acc.7	Acceso remoto (remote login)	1	27002: • 11.4.2	27002: • 9.4.2 • 10.1.1 • 13.1.1 • 13.1.2 • 18.1.5	3	no
op.exp	Explotación					
op.exp.1	Inventario de activos	0	27002: • 7.1.1 • 7.1.2	27002: • 8.1.1 • 8.1.2	0	DSI-07 DCS-01
op.exp.2	Configuración de seguridad	3	no	no	1	GRM-01 IVS-07
op.exp.3	Gestión de la configuración	3	no	no	1	GRM-01
op.exp.4	Mantenimiento	1	27002: • 9.2.4	27002: • 11.2.4	1	IVS-05 MOS-15 MOS-19 TVM-02
op.exp.5	Gestión de cambios	1	27002: • 10.1.2 • 12.5.1 • 12.5.2	27002: • 12.1.2 • 14.2.2 • 14.2.3	1	MOS-15
op.exp.6	Protección frente a código dañino	0	27002: • 10.4.1 • 10.4.2	27002: • 12.2.1	0	MOS-17 TVM-01 TVM-03
op.exp.7	Gestión de incidencias	0	27002: • 6.1.6 • 6.1.7 • 10.10.5 • 13.1.1 • 13.1.2 • 13.2.2 • 13.2.3	27002: • 6.1.3 • 6.1.4 • 16.1.2 • 16.1.3 • 16.1.4 • 16.1.5 • 16.1.6 • 16.1.7	0	SEF-01 SEF-02 SEF-03

MEDIDAS DE SEGURIDAD		ISO 27000			CCM	
op.exp.8	Registro de la actividad de los usuarios	0	27002: • 10.10.1 • 10.10.2 • 10.10.4	27002: • 12.4.1 • 12.4.3	0	IVS-03 SEF-04
op.exp.9	Registro de la gestión de incidencias	0	27002: • 13.2.3	27002: • 16.1.5 • 16.1.7	0	SEF-05 STA-02
op.exp.10	Protección de los registros de actividad	0	27002: • 10.10.3 • 10.10.6 • 15.3.2	27002: • 12.4.2 • 12.4.4	0	IAM-01 IVS-01 SEF-04
op.exp.11	Protección de claves criptográficas	1	27002: • 12.3.2	27002: • 10.1.2	1	EKM-04
op.ext	Servicios externos					
op.ext.1	Contratación y acuerdos de nivel de servicio	1	27002: • 6.2.3 • 10.8.2	27002: • 13.2.2 • 15.1.1 • 15.1.2 • 15.1.3	1	HRS-08 STA-05
op.ext.2	Gestión diaria	1	27002: • 10.2.1 • 10.2.2 • 10.2.3	27002: • 15.2.1 • 15.2.2	1	STA-09 TVM-02
op.ext.9	Medios alternativos	2	no	no		no
op.cont	Continuidad del servicio					
op.cont.1	Análisis de impacto	0	27002: • 14.1.1 • 14.1.2	27002: • 17.1.1	0	BCR-09 DCS-01
op.cont.2	Plan de continuidad	0	27002: • 14.1.3 • 14.1.4	27002: • 17.1.2	0	BCR-01 BCR-07 BCR-10
op.cont.3	Pruebas periódicas	0	27002: • 14.1.5	27002: • 17.1.3	0	BCR-02
op.mon	Monitorización del sistema					
op.mon.1	Detección de intrusión	2	no	no		IVS-06
op.mon.2	Sistema de métricas	1	27002: • 4.2.2 • 4.2.3	27002: • 9 • 9.1		STA-07

MEDIDAS DE SEGURIDAD		ISO 27000			CCM	
mp	**Medidas de protección**					
mp.if	Protección de las instalaciones e infraestructuras					DCS-06
mp.if.1	Áreas separadas y con control de acceso	0	27002: • 9.1.1 • 9.1.2 • 9.1.3 • 9.1.4 • 9.1.5 • 9.2.1 • 11.6.2	27002: • 11.1.1 • 11.1.2 • 11.1.3 • 11.1.4 • 11.1.5 • 11.1.6 • 11.2.1	0	BCR-06 DCS-02 DCS-06 DCS-08
mp.if.2	Identificación de las personas	0	27002: • 9.1.2	27002: • 11.1.2	0	DCS-07 DCS-08 DCS-09
mp.if.3	Acondicionamiento de los locales	0	27002: • 9.2.2 • 9.2.3	27002: • 11.2.2 • 11.2.3	0	BCR-03 BCR-08
mp.if.4	Energía eléctrica	0	27002: • 9.2.2	27002: • 11.2.2	0	BCR-03 BCR-08 DCS-04
mp.if.5	Protección frente a incendios	0	27002: • 9.1.4	27002: • 11.1.4	0	BCR-03 BCR-05 BCR-08
mp.if.6	Protección frente a inundaciones	0	27002: • 9.1.4	27002: • 11.1.4	0	BCR-03 BCR-05 BCR-08
mp.if.7	Registro de entrada y salida de equipamiento	0	27002: • 9.2.5 • 9.2.7	27002: • 11.2.5 • 11.2.6	3	no
mp.if.9	Instalaciones alternativas	1	no	27002: • 17.2.1	3	no

MEDIDAS DE SEGURIDAD		ISO 27000			CCM	
mp.per	Gestión del personal					DCS-06
mp.per.1	Caracterización del puesto de trabajo	0	27002: • 8.1.1 • 8.1.2	27002: • 7.1.1	0	HRS-02
mp.per.2	Deberes y obligaciones	0	27002: • 6.1.5 • 8.1.3 • 8.2.1 • 8.2.3 • 8.3.1 • 8.3.2	27002: • 7.1.2 • 7.2.1 • 7.2.3 • 7.3.1 • 8.1.4 • 13.2.4	0	GRM-07 HRS-03 HRS-04 HRS-07 HRS-08
mp.per.3	Concienciación	0	27001: • 4.2.2 • 5.2.2 27002: • 8.2.2	27001: • 7.3 27002: • 7.2.2	0	GRM-03 HRS-10 HRS-11 MOS-01 MOS-05 SEF-03
mp.per.4	Formación	0	27001: • 4.2.2 • 5.2.2 27002: • 8.2.2	27001: • 7.2 27002: • 7.2.2	0	HRS-10
mp.per.9	Personal alternativo	1	no	27002: • 17.2.1	1	BCR-07
mp.eq	Protección de los equipos					
mp.eq.1	Puesto de trabajo despejado	0	27002: • 11.3.3	27002: • 11.2.9	3	no
mp.eq.2	Bloqueo del puesto de trabajo	0	27002: • 11.3.2 • 11.5.5 • 11.5.6	27002: • 11.2.8	0	HRS-12

MEDIDAS DE SEGURIDAD		ISO 27000			CCM	
mp.eq.3	Protección de portátiles	1	27002: • 11.7.1	27002: • 6.2.1	1	HRS-06 MOS-08 MOS-09 MOS-10 MOS-11 MOS-12 MOS-13 MOS-14 MOS-15 MOS-17 MOS-18 MOS-19 MOS-20
mp.eq.9	Medios alternativos	1	no	27002: • 17.2.1	1	HRS-12
mp.com	Protección de las comunicaciones					
mp.com.1	Perímetro seguro	2	27002: • 10.6.2 • 11.4.6 • 11.4.7	27002: • 13.1.2	2	IVS-12
mp.com.2	Protección de la confidencialidad	1	27002: • 10.6.1 • 10.6.2 • 15.1.6	27002: • 10.1.1 • 13.1.1 • 13.1.2 • 14.1.2 • 18.1.5	1	DSI-03 EKM-03 IVS-12 IPY-04
mp.com.3	Protección de la autenticicidad y de la integridad	1	27002: • 10.6.1 • 10.6.2 • 11.4.2 • 11.4.3 • 11.4.4	27002: • 10.1.1 • 13.1.1 • 13.1.2 • 14.1.2	1	DSI-03 IVS-12 IPY-04
mp.com.4	Segregación de redes	0	27002: • 11.4.5	27002: • 13.1.3	0	IVS-10
mp.com.9	Medios alternativos	1	no	27002: • 17.2.1		BCR-03 BCR-08
mp.si	Protección de los soportes de información					
mp.si.1	Etiquetado	0	27002: • 7.2.2 • 10.7.1	27002: • 8.2.2 • 8.3.1	0	DSI-01 DSI-04

MEDIDAS DE SEGURIDAD		ISO 27000			CCM	
mp.si.2	Criptografía	1	27002: • 10.7.1 • 12.3.1	27002: • 8.3.1 • 10.1.1	1	DSI-05 EKM-03
mp.si.3	Custodia	0	27002: • 10.7.1	27002: • 8.3.1	0	DSI-05
mp.si.4	Transporte	0	27002: • 10.8.3	27002: • 8.3.3 • 11.2.5	0	DSI-05
mp.si.5	Borrado y destrucción	0	27002: • 9.2.6 • 10.7.2	27002: • 8.3.2 • 11.2.7	0	DSI-08 DCS-05 MOS-18
mp.sw	Protección de las aplicaciones informáticas					
mp.sw.1	Desarrollo	0	27002: • 10.1.4 • 12.4.2 • 12.4.3 • 12.5.5	27002: • 9.4.5 • 12.1.4 • 14.2.1 • 14.2.5 • 14.2.6 • 14.2.7 • 14.3.1	0	CCC-02 CCC-03 DSI-06 IAM-06 IVS-08
mp.sw.2	Aceptación y puesta en servicio	1	27002: • 10.1.4 • 10.3.2 • 12.4.1 • 12.4.2 • 12.5.5 • 12.6.1	27002: • 12.1.4 • 12.5.1 • 12.6.1 • 14.2.8 • 14.2.9 • 14.3.1 • 14.2.7	1	CCC-03 DSI-06
mp.info	Protección de la información					
mp.info.1	Datos de carácter personal	0	27002: • 15.1.4	27002: • 18.1.4	3	no
mp.info.2	Calificación de la información	0	27002: • 7.1.2 • 7.2.1	27002: • 8.1.2 • 8.2.1	0	DSI-01
mp.info.3	Cifrado de la información	2	27002: • 12.3.1 • 10.6.1 • 10.6.2 • 10.8.3 • 10.9.2 • 15.1.6	27002: • 10.1.1 • 8.3.3 • 13.1.1 • 13.1.2 • 18.1.5	2	EKM-03

MEDIDAS DE SEGURIDAD		ISO 27000			CCM	
mp.info.4	Firma electrónica	3	27002: • 10.9.2 • 12.3.1 • 15.1.6	27002: • 10.1.1 • 14.1.3 • 18.1.5	3	no
mp.info.5	Sellos de tiempo	3	27002: • 10.9.2	27002: • 14.1.3	3	no
mp.info.6	Limpieza de documentos	3	27002: • 12.5.4	no	3	no
mp.info.9	Copias de seguridad (backup)	0	27002: • 10.5.1	27002: • 12.3.1	0	BCR-12 MOS-17
mp.s	Protección de los servicios					
mp.s.1	Protección del correo electrónico	0	27002: • 10.8.4	27002: • 13.2.3	3	no
mp.s.2	Protección de servicios y aplicaciones web	3	no	no	3	no
mp.s.8	Protección frente a la denegación de servicio	3	27002: • 10.3.1	27002: • 12.1.3	3	no
mp.s.9	Medios alternativos	2	no	27002: • 17.2.1	3	no

ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

acrónimo	descripción
AEPD	Agencia Española de Protección de Datos
ANS	Acuerdo de Nivel de Servicio (ver SLA)
ARCO	Conjunto de derechos (Acceso, Rectificación, Cancelación y Oposición), a través de los cuales una persona puede ejercer el control sobre sus datos personales.
CCM	*Cloud Controls Matrix*
CCN	Centro Criptológico Nacional
CSA	*Cloud Security Alliance*
CSP	*Cloud Service Provider*
ENI	Esquema Nacional de Interoperabilidad
ENS	Esquema Nacional de Seguridad
IaaS	*Infrastructure as a Service*
LOPD	Ley Orgánica de Protección de Datos de Carácter Personal
PaaS	*Platform as a Service*
SaaS	*Software as a Service*
SLA	*Service Level Agreement* (ver ANS)

Auditoría

Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.
Nota 1: Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).
Nota 2: "Evidencia de auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011.
[ISO, Anexo SL]

cloud application portability

ability to migrate an application from one cloud service to another cloud service
[ISO/IEC 17788:2014]

cloud auditor

cloud service partner with the responsibility to conduct an audit of the provision and use of cloud services
[ISO/IEC 17788:2014]

cloud capabilities type
classification of the functionality provided by a cloud service to the cloud service customer, based on resources used
NOTE – The cloud capabilities types are application capabilities type, infrastructure capabilities type and platform capabilities type.
[ISO/IEC 17788:2014]

cloud computing
paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand
NOTE – Examples of resources include servers, operating systems, networks, software, applications, and storage equipment.
[ISO/IEC 17788:2014]

cloud data portability
data portability from one cloud service to another cloud service
[ISO/IEC 17788:2014]

cloud deployment model
way in which cloud computing can be organized based on the control and sharing of physical or virtual resources
NOTE – The cloud deployment models include community cloud, hybrid cloud, private cloud and public cloud.
[ISO/IEC 17788:2014]

cloud service
one or more capabilities offered via cloud computing invoked using a defined interface
[ISO/IEC 17788:2014]

cloud service category
group of cloud services that possess some common set of qualities
NOTE – A cloud service category can include capabilities from one or more cloud capabilities types.
[ISO/IEC 17788:2014]

cloud service customer
party which is in a business relationship for the purpose of using cloud services
NOTE – A business relationship does not necessarily imply financial agreements.
[ISO/IEC 17788:2014]

cloud service customer data
class of data objects under the control, by legal or other reasons, of the cloud service customer that were input to the cloud service, or resulted from exercising the capabilities of the cloud service by or on behalf of the cloud service customer via the published interface of the cloud service
NOTE 1 – An example of legal controls is copyright.
NOTE 2 – It may be that the cloud service contains or operates on data that is not cloud service customer data; this might be data made available by the cloud service providers,

or obtained from another source, or it might be publicly available data. However, any output data produced by the actions of the cloud service customer using the capabilities of the cloud service on this data is likely to be cloud service customer data, following the general principles of copyright, unless there are specific provisions in the cloud service agreement to the contrary.
[ISO/IEC 17788:2014]

cloud service partner
party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both
[ISO/IEC 17788:2014]

cloud service provider
party which makes cloud services available
[ISO/IEC 17788:2014]

cloud service provider data
class of data objects, specific to the operation of the cloud service, under the control of the cloud service provider
NOTE – Cloud service provider data includes but is not limited to resource configuration and utilization information, cloud service specific virtual machine, storage and network resource allocations, overall data centre configuration and utilization, physical and virtual resource failure rates, operational costs and so on.
[ISO/IEC 17788:2014]

cloud service user
natural person, or entity acting on their behalf, associated with a cloud service customer that uses cloud services
NOTE – Examples of such entities include devices and applications.
[ISO/IEC 17788:2014]

community cloud
cloud deployment model where cloud services exclusively support and are shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection
[ISO/IEC 17788:2014]

Compute as a Service (CompaaS)
cloud service category in which the capabilities provided to the cloud service customer are the provision and use of processing resources needed to deploy and run software
NOTE – To run some software, capabilities other than processing resources may be needed.
[ISO/IEC 17788:2014]

data portability
ability to easily transfer data from one system to another without being required to re-enter data

NOTE – It is the ease of moving the data that is the essence here. This might be achieved by the source system supplying the data in exactly the format that is accepted by the target system. But even if the formats do not match, the transformation between them may be simple and straightforward to achieve with commonly available tools. On the other hand, a process of printing out the data and rekeying it for the target system could not be described as "easy."
[ISO/IEC 17788:2014]

Data Storage as a Service (DSaaS)
cloud service category in which the capability provided to the cloud service customer is the provision and use of data storage and related capabilities
NOTE – DSaaS can provide any of the three cloud capabilities types.
[ISO/IEC 17788:2014]

hybrid cloud
cloud deployment model using at least two different cloud deployment models
[ISO/IEC 17788:2014]

Infrastructure as a Service (IaaS)
cloud service category in which the cloud capabilities type provided to the cloud service customer is an infrastructure capabilities type
NOTE – The cloud service customer does not manage or control the underlying physical and virtual resources, but does have control over operating systems, storage, and deployed applications that use the physical and virtual resources. The cloud service customer may also have limited ability to control certain networking components (e.g., host firewalls).
[ISO/IEC 17788:2014]

infrastructure capabilities type
cloud capabilities type in which the cloud service customer can provision and use processing, storage or networking resources
[ISO/IEC 17788:2014]

measured service
metered delivery of cloud services such that usage can be monitored, controlled, reported and billed

multi-tenancy
allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another
[ISO/IEC 17788:2014]

on-demand self-service
feature where a cloud service customer can provision computing capabilities, as needed, automatically or with minimal interaction with the cloud service provider
[ISO/IEC 17788:2014]

Platform as a Service (PaaS)
cloud service category in which the cloud capabilities type provided to the cloud service customer is a platform capabilities type
[ISO/IEC 17788:2014]

platform capabilities type
cloud capabilities type in which the cloud service customer can deploy, manage and run customer-created or customer-acquired applications using one or more programming languages and one or more execution environments supported by the cloud service provider
[ISO/IEC 17788:2014]

private cloud
cloud deployment model where cloud services are used exclusively by a single cloud service customer and resources are controlled by that cloud service customer
[ISO/IEC 17788:2014]

public cloud
cloud deployment model where cloud services are potentially available to any cloud service customer and resources are controlled by the cloud service provider
[ISO/IEC 17788:2014]

Puerto Seguro (Safe Harbor)
Marco de actuación establecido por Estados Unidos y la Unión Europea para salvar las diferencias entre ambos en tratamiento de la privacidad y la protección de datos. Este marco regula el tratamiento de datos personales de ciudadanos europeos por parte de empresas estadounidenses.

resource pooling
aggregation of a cloud service provider's physical or virtual resources to serve one or more cloud service customers
[ISO/IEC 17788:2014]

reversibility
process for cloud service customers to retrieve their cloud service customer data and application artefacts and for the cloud service provider to delete all cloud service customer data as well as contractually specified cloud service derived data after an agreed period
[ISO/IEC 17788:2014]

service level agreement (SLA)
documented agreement between the service provider and customer that identifies services and service targets
NOTE 1 – A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier.
NOTE 2 – A service level agreement can be included in a contract or another type of documented agreement.
[ISO/IEC 20000-1:2011]

Software as a Service (SaaS)

cloud service category in which the cloud capabilities type provided to the cloud service customer is an application capabilities type
[ISO/IEC 17788:2014]

tenant

one or more cloud service users sharing access to a set of physical and virtual resources
[ISO/IEC 17788:2014]

ANEXO C. REFERENCIAS

AEPD

Guía para clientes que contraten servicios en *cloud computing*, Agencia Española de Protección de Datos, 2013.

CCM

Cloud Controls Matrix, CSA, v3.0.1, July 2014

CCN-STIC-401

Guía 401. Glosario y Abreviaturas.

CCN-STIC-800

Guía 800 - Glosario de Términos y Abreviaturas del ENS

CCN-STIC-801

Guía 801 del Esquema Nacional de Seguridad. Responsabilidades y funciones.

CCN-STIC-802

Guía 802 del Esquema Nacional de Seguridad. Guía de Auditoría.

CCN-STIC-804

Guía 804 del Esquema Nacional de Seguridad. Medidas de implantación del ENS.

CCN-STIC-807

Guía 807 del Esquema Nacional de Seguridad. Criptología de empleo en el ENS.

CSA:2009

Guía de seguridad en áreas críticas de atención al *Cloud Computing*. CSA (*Cloud Security Alliance*). Noviembre de 2009

DC 2010/87/UE

Decisión de la comisión de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo

ENISA CCSL

Cloud Computing Certification Schemes List – CCSL and CCSM

ENISA:2011

Security and Resilience in Governmental Clouds.

Guía de seguridad y resiliencia en ENISA. Enero de 2011

ISO/IEC 17788:2014

Information technology – Cloud Computing – Overview and Vocabulary

ISO/IEC 17789:2014

Information technology – Cloud Computing – Reference architecture

ISO 22301:2012

Societal security -- Business continuity management systems --- Requirements

ISO/IEC 27001:2013

Information technology -- Security techniques -- Information security management systems – Requirements

ISO/IEC 27017:?

Information technology -- Security techniques -- Code of practice for information security controls for cloud computing services based on ISO/IEC 27002

ISO/IEC 27018:2014

Information technology -- Security techniques -- Code of practice for PII protection in public cloud acting as PII processors

Ley 11/2007

Ley 11/2007, de 22 junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. BOE de 23 de junio de 2007

Ley 15/1999

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE de 14 de diciembre de 1999.

Ley 30/1992

Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. BOE de 27 de noviembre de 1992.

NIST SP-800-144

Guidelines on Security and Privacy in Public Cloud Computing, Dec. 2011

NIST SP-800-145

The NIST Definition of Cloud Computing, Sept. 2011

NIST SP-800-146

Cloud Computing Synopsis and Recommendations, May 2012

RD 1720/2007

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE de 19 de enero de 2008.

RD 3/2010

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. BOE de 29 de enero de 2010.

RD 4/2010

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. BOE de 29 de enero de 2010