

GUÍA PARA LA PRESTACIÓN DE APLICACIONES EN MODO SERVICIO



GOBIERNO
DE ESPAÑA

MINISTERIO
DE HACIENDA
Y ADMINISTRACIONES PÚBLICAS

SECRETARÍA DE ESTADO DE
ADMINISTRACIONES PÚBLICAS

DIRECCIÓN DE TECNOLOGÍAS DE LA
INFORMACIÓN Y LAS COMUNICACIONES

TÍTULO: Guía para la prestación de aplicaciones en modo servicio

Elaboración y coordinación de contenidos:

Dirección de Tecnologías de la Información y las Comunicaciones (DTIC)

Características: Adobe Acrobat 5.0

Responsable edición digital: Subdirección General de Información, Documentación y Publicaciones

1ª edición electrónica: abril de 2016

Disponible esta publicación en el Portal de Administración Electrónica (PAe):

<http://administracionelectronica.gob.es/>

Edita:

© Ministerio de Hacienda y Administraciones Públicas

Secretaría General Técnica

Subdirección General de Información,

Documentación y Publicaciones

Centro de Publicaciones

Colección: administración electrónica

NIPO: 630-16-262-8



El presente documento está bajo la licencia Creative Commons Reconocimiento-No comercial-Compartir Igual versión 4.0 España.

Usted es libre de:

- Copiar, distribuir y comunicar públicamente la obra
- Hacer obras derivadas

Bajo las condiciones siguientes:

- Reconocimiento. Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciadore (pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra).
- Compartir bajo la misma licencia. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

Nada en esta licencia menoscaba o restringe los derechos morales del autor.

Esto es un resumen legible por humanos del texto legal (la licencia completa) disponible en

<http://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

ÍNDICE

0.	CONSIDERACIONES PREVIAS	6
1.	INTRODUCCIÓN	7
2.	OBJETIVO Y ALCANCE DE LA GUÍA	9
2.1.	Qué NO incluye la Guía.....	9
3.	ÁMBITO DE APLICACIÓN Y DESTINATARIOS	10
4.	ACUERDOS DE PRESTACIÓN DE APLICACIONES EN MODO SERVICIO	11
4.1.	Regulación y formas jurídicas.....	12
4.2.	Definición y alcance del servicio	14
4.3.	Actores intervinientes	15
5.	CONDICIONES DE PRESTACIÓN DE SERVICIO	19
5.1.	Acuerdos de Nivel de Servicio	19
5.2.	Ejemplos de Indicadores de Nivel de Servicio	20
5.2.1.	Horario de prestación del servicio	20
5.2.2.	Disponibilidad del servicio.....	20
5.2.3.	Tiempos de respuesta por prioridad e impacto	20
5.2.4.	Transacciones por segundo.....	21
6.	MODELO Y ALCANCE DE SOPORTE	22
6.1.	Niveles de Soporte	22
6.1.1.	Nivel 1. Servicio de atención y soporte a usuarios general.....	22
6.1.2.	Nivel 2. Servicio de Atención y soporte a usuarios especializado.....	23
6.1.3.	Nivel 3. Servicio de Mantenimiento	23
6.1.4.	Nivel 4. Servicio de Administración de Sistemas, Seguridad y Comunicaciones	23
6.1.5.	Nivel 5. Servicio de escalado a socios del proveedor	24
6.1.6.	Ejemplo de niveles de servicio	24
6.2.	Procedimientos de Gestión del Servicio.....	24
6.3.	Herramientas.....	25
6.4.	Canales de soporte	25
6.5.	Otras consideraciones de soporte	26
7.	MODELO Y ALCANCE DE FORMACIÓN	27
7.1.	Colectivos.....	27
7.2.	Estrategia de formación.....	27
7.2.1.	Otras consideraciones de la estrategia formativa	28
7.3.	Ciclos del proceso formativo.....	28

7.4. Infraestructura de formación	29
8. CONSIDERACIONES DE ADMINISTRACIÓN DEL SISTEMA.....	30
8.1. Administración del sistema	30
8.1.1.Administración centralizada	30
8.1.2.Administración delegada.....	30
8.2. Administración de la infraestructura.....	31
8.2.1.Gestión de la capacidad	31
8.2.2.Gestión de la continuidad del servicio / disponibilidad	32
8.2.3.Gestión de la entrega.....	32
9. RESPONSABILIDAD Y BUEN USO	33
9.1. Régimen de supervisión y penalizaciones	34
10. SEGURIDAD	35
10.1. Confidencialidad y protección de datos	36
10.1.1. Protección de la Información.....	37
10.1.2. Datos de carácter personal	37
10.1.3. Conservación de los datos	39
10.1.4. Transferencias internacionales de datos	39
10.2. Control de Acceso	40
10.3. Trazabilidad.....	41
10.4. Continuidad del Servicio	42
10.5. Auditoría	42
11. EVOLUCIÓN DEL SERVICIO	43
11.1. Hoja de ruta de evolución de la aplicación en modo servicio	43
12. CONTRAPRESTACIÓN ECONÓMICA	45
12.1. Modelo de costes	45
12.2. Modelos de contraprestación.....	45
12.3. Penalizaciones	46
13. FINALIZACIÓN DEL SERVICIO	47
13.1. Finalización por fin del acuerdo de prestación	47
13.2. Finalización anticipada del acuerdo de servicio	47
14. REFERENCIAS	49
14.1. Legislación	49
14.2. Estándares y buenas prácticas.....	49
14.3. Documentos de trabajo y referencias	49

ANEXO I. CHECK LIST APLICACIONES EN MODO SERVICIO	51
--	-----------

ANEXO II. EQUIPO RESPONSABLE DEL PROYECTO	52
--	-----------

ÍNDICE DE FIGURAS

Figura 1. Actores intervinientes en la prestación de aplicaciones en modo servicio	16
Figura 2. Roles en Plataforma ADUJAVA.....	17
Figura 3. Roles en Sistema de Interconexión de Registros (SIR)	17
Figura 4. Roles en Sistema @Firma.....	18
Figura 5. Roles en Sistema CI@ve.....	18
Figura 6. Modelo de niveles de soporte de servicios TI	22
Figura 7. Niveles de Servicios Plataforma de Intermediación del MINHAP.....	24
Figura 8. Procedimiento de gestión de cambios	43



ÍNDICE DE TABLAS

Tabla 1. Ejemplos de indicadores de disponibilidad del servicio.....	20
Tabla 2. Ejemplos de tiempo de resolución de incidencias por prioridad	21
Tabla 3. Ejemplos de indicadores de tiempos de resolución de incidencias	21
Tabla 4. Ejemplos de indicadores de transacciones por segundo	21

Histórico de versiones del documento			
Versión	Nombre del documento	Fecha	Descripción
01.00	20160404-Guía para la prestación de aplicaciones en modo servicio	Abril de 2016	Versión 1

0. CONSIDERACIONES PREVIAS

1. Este documento constituye una guía de aplicación para la prestación de aplicaciones en modo servicio, y como tal, su objetivo es servir como herramienta de apoyo a las administraciones públicas que quieran ofrecer aplicaciones, plataformas, infraestructuras o procesos en modo servicio a otros organismos. Para la realización del documento, se han utilizado como apoyo otras guías relacionadas con este tipo de aplicaciones en modo servicio y contenidos complementarios.
2. Para facilitar su manejo y comprensión, esta guía incluye diferentes recursos gráficos cuya leyenda se muestra a continuación:

	Indicador de contenido considerado de especial importancia o relevancia.
	Advertencia o aclaración para la correcta interpretación del contenido.

3. A lo largo del desarrollo de esta guía, se referencia a leyes y decretos de protección de datos y otra normativa relacionada que es necesario conocer para abordar de manera global estos aspectos. Estas normas están referenciadas en el apartado correspondiente a referencias al final de este documento.

1. INTRODUCCIÓN

4. La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, **Ley 40/2015**)¹, al igual que previamente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (en adelante, **Ley 11/2007**), dedica su artículo 157 a la reutilización de aplicaciones y transferencia de tecnologías entre Administraciones públicas. De especial interés es el apartado 1, que establece lo siguiente:

Artículo 157. Reutilización de sistemas y aplicaciones de propiedad de la Administración

1. Las Administraciones pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

5. En este marco, se puede evidenciar el potencial de los modelos de reutilización basados en el ofrecimiento de aplicaciones en modo servicio para el desarrollo de la Ley citada anteriormente. Con ella se busca impulsar el acceso a los ciudadanos a más servicios, contenidos y trámites de administración electrónica, en condiciones de mayor rendimiento y disponibilidad gracias a la escalabilidad y flexibilidad que aportan los modelos de prestación en modo servicio para el despliegue de nuevos servicios de forma ágil y efectiva.
6. Con el fin de crear un escenario de eficiencia y un funcionamiento óptimo de la Administración, se establece en la Ley 40/2015 como una obligación de las Administraciones públicas la de utilizar aquellas soluciones disponibles que puedan satisfacer total o parcialmente las necesidades de los nuevos sistemas y servicios o la mejora y actualización de los ya implantados.

Artículo 157. Reutilización de sistemas y aplicaciones de propiedad de la Administración

3. Las Administraciones Públicas, con carácter previo a la adquisición, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, deberán consultar en el directorio general de aplicaciones, dependiente de la Administración General del Estado, si existen soluciones disponibles para su reutilización, que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

En este directorio constarán tanto las aplicaciones disponibles de la Administración General del Estado como las disponibles en los directorios integrados de aplicaciones del resto de Administraciones.

En el caso de existir una solución disponible para su reutilización total o parcial, las Administraciones Públicas estarán obligadas a su uso, salvo que la decisión de no

¹ La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público entrará en vigor el 2 de octubre de 2016 (un año desde su publicación en el Boletín Oficial del Estado).

reutilizarla se justifique en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera...


7. Una de las preocupaciones comunes en la prestación de aplicaciones en modo servicio es la seguridad y confidencialidad de los datos de carácter personal. En esta materia, España también cuenta con un marco normativo que da apoyo y ampara el desarrollo del mercado de aplicaciones en modo servicio:
 - i. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD) o norma que la sustituya.
 - ii. El reglamento de desarrollo de la LOPD, el Real Decreto 1720/2007, de 21 de diciembre (en adelante RLOPD) o norma que la sustituya.
8. Esta normativa establece las condiciones básicas que regulan la seguridad y protección de datos de carácter personal necesarias para considerar a España como un entorno jurídico seguro para el despliegue de aplicaciones en modo servicio.
9. Por otra parte, existe también normativa que regula los procedimientos de contratación de las Administraciones públicas y que soporta la contratación de aplicaciones en modo servicio. Tal es el caso del Real Decreto Legislativo 3/2011 por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público. Los servicios en red se encuentran tipificados como contratos de servicio, de acuerdo con el artículo 10 de dicho Real Decreto.
10. En este contexto jurídico se desarrolla la presente guía de prestación de aplicaciones en modo servicio, que pretende ser un apoyo a las Administraciones públicas que desean prestar estos servicios en cuanto a las particularidades a tener en cuenta para ponerlos en marcha, desde la adaptación de los modelos contractuales y acuerdos de prestación de servicios, consideraciones de confidencialidad, seguridad y protección de datos personales, establecimiento de condiciones de prestación del servicio y los modelos de relación y operativa comunes de este tipo de servicios en los ámbitos de soporte, estrategia formativa, administración del servicio, buen uso y finalización del servicio.

2. OBJETIVO Y ALCANCE DE LA GUÍA

11. Atendiendo a la necesidad de conocer los distintos aspectos a tener en cuenta para la prestación de aplicaciones en modo servicio, y con el objetivo de impulsar esta modalidad de servicio que supone importantes ahorros de costes para el sector público, esta guía desarrolla recomendaciones sobre:
- iii. Tipos de posibles acuerdos en los que se puede articular la prestación de aplicaciones en modo servicio.
 - iv. Condiciones de prestación que pueden afectar a estos servicios.
 - v. Modelo de soporte y formación oportunos para aplicaciones en modo servicio.
 - vi. Modelos de administración y mantenimiento de este tipo de servicios.
 - vii. Consideraciones de confidencialidad, protección de datos y seguridad.
 - viii. Gestión de la evolución y la demanda en este tipo de servicios.
 - ix. Posibles contraprestaciones económicas, teniendo en cuenta que la facturación no podrá suponer un lucro para la administración proveedora de la aplicación en modo servicio.
 - x. Aspectos a tener en cuenta en la devolución del servicio prestado.

2.1. Qué NO incluye la Guía

12. Esta guía pretende aportar recomendaciones o aspectos a considerar por las administraciones que tengan el propósito de involucrarse en la prestación de aplicaciones en modo servicio, bien sea como proveedores directos o como cualquiera de los agentes intervinientes en la prestación de este tipo de servicios.

13.  Por esta razón, la guía no pretende ser un manual de pasos a seguir para iniciar la prestación de este tipo de servicios, ya que las decisiones a tomar para cada uno de los contenidos presentados dependerá de muchos factores, entre ellos: el tipo de servicio a prestar, el contexto y negocio de la aplicación en modo servicio, las partes intervinientes, entre otros.

3. ÁMBITO DE APLICACIÓN Y DESTINATARIOS

14. El ámbito de esta guía es la prestación de aplicaciones en modo servicio en red por parte de organismos públicos, bien sea para ofrecer servicios como proveedores directos, como usuarios o en cualquier modelo de intermediación que pueda plantearse.
15. Por tanto, las indicaciones contenidas en esta guía pretenden dar orientación en todos los aspectos a tener en cuenta para la prestación de estos servicios, desde la definición del catálogo de servicios, pasando por la articulación del acuerdo de prestación entre las partes e incluyendo recomendaciones en cuanto al modelo y alcance del soporte y formación, administración del servicio, soportes, protección de datos, seguridad y tipos de contraprestación del servicio.
16. Dentro del ámbito de aplicación definido anteriormente, los destinatarios del contenido de esta guía práctica, son los siguientes:
 - i. Responsables de la prestación de la aplicación en modo servicio, bien sea como proveedores directos, intermediarios, habilitadores o cualquier otro tipo de modalidad de prestación que se defina en función del tipo de servicio a prestar.
 - ii. Responsables de actividades de administración relacionadas con el servicio prestado, bien sea en modo centralizado, delegado o mixto.
 - iii. Equipo encargado de impartir formación y preparar material formativo relacionado con este tipo de servicios.
 - iv. Miembros de departamentos de seguridad informática, cumplimiento de LOPD o norma que la sustituya y confidencialidad.
 - v. Responsables de auditoría de este tipo de servicios.
 - vi. Suscriptores de aplicaciones en modo servicio, tanto reales como potenciales.

4. ACUERDOS DE PRESTACIÓN DE APLICACIONES EN MODO SERVICIO

17. La naturaleza innovadora de la prestación de aplicaciones en modo servicio hace que la configuración de acuerdos de prestación presente ciertas complejidades adicionales. Resulta necesario definir los derechos y obligaciones de todas las partes intervinientes en la prestación del servicio con el máximo detalle posible. Algunos aspectos cruciales en los acuerdos de prestación de aplicaciones en modo servicio son:
- i. Las condiciones de prestación del servicio.
 - ii. La seguridad de la información.
 - iii. Los procedimientos de soporte y de administración del sistema.
 - iv. La localización de los datos y las posibles transferencias internacionales de los mismos.
 - v. La cobertura de los riesgos específicos asociados a servicios en red.
 - vi. Las condiciones y procedimientos de finalización del servicio.
18. En definitiva, resulta conveniente tener en cuenta que las aplicaciones en modo servicio no deberán articularse con contratos estándares de servicios IT, ya que existen muchos términos y condiciones de la contratación regular que en este tipo de prestaciones deben ser negociados entre las partes.



4.1. Regulación y formas jurídicas

19. La prestación de una aplicación en modo servicio requiere contemplar los aspectos fundamentales del servicio, seguridad y confidencialidad de la información, procedimientos de soporte, administración del sistema y condiciones del servicio. Cuando la Administración actúa como proveedor de servicios en red resulta necesario regular con claridad los derechos y obligaciones de cada una de las partes, así como las responsabilidades a asumir. Tal regulación podría articularse a través principalmente de cuatro figuras jurídicas: i) la firma de un Memorándum de Entendimiento; ii) la suscripción del correspondiente convenio; iii) la suscripción del correspondiente contrato; iv) la formalización de una encomienda de gestión.
20. Estos acuerdos se podrán formalizar a través de los siguientes mecanismos:

- i. **Memorándum de Entendimiento:** normalmente no tiene contenido obligacional, limitándose a señalar las intenciones de las partes en relación con una línea de acción común.

El carácter vinculante del instrumento a través del que se formalice el acuerdo para la prestación de una aplicación en modo servicio dependerá del grado de concreción de sus elementos básicos, así como de la concurrencia en el mismo de determinados requisitos legales y de previsiones expresas acerca de su cumplimiento forzoso por las partes firmantes.

Por tanto, este mecanismo, podría resultar apropiado para poner a disposición de otras Administraciones las aplicaciones a las que se refiere tanto el artículo 45 de la Ley 11/2007 como el artículo 157 de la Ley 40/2015, siendo necesario que en él se fijen los términos de uso de la aplicación y, sobre todo, los presupuestos esenciales de la relación jurídica.

Asimismo, en caso de que se optara por este mecanismo, resultaría conveniente incluir en el Memorándum las recomendaciones contempladas en la presente Guía relativas a la finalización del servicio.

- ii. **Convenio:** los convenios de colaboración son uno de los instrumentos de cooperación más frecuentes entre Administraciones. Son acuerdos vinculantes entre Administraciones Públicas (Administración General del Estado, Comunidades Autónomas y Entidades Locales), o bien entre dos o más organismos públicos o entidades de derecho público vinculados o dependientes de distintas Administraciones públicas. El contenido mínimo de los mismos debería abarcar: a) sujetos que celebran el convenio y la capacidad jurídica con la que actúa cada una de las partes; b) competencia en la que se fundamenta la actuación de las partes; c) objeto del convenio y las actuaciones que se acuerde desarrollar por cada sujeto para su cumplimiento; d) obligaciones y compromisos económicos de las partes; e) consecuencias en caso de incumplimiento; f) mecanismos de vigilancia y control de su ejecución y de los compromisos asumidos, que resolverán también los problemas de interpretación y

cumplimiento; g) régimen de modificación; h) plazo de vigencia, lo que no impedirá su prórroga si así lo acuerdan las partes firmantes.

Es conveniente tener en cuenta que la Ley 40/2015, sistematiza por primera vez los requisitos de validez y eficacia de los convenios, regulando asimismo las causas de extinción y los efectos de la resolución de los mismos. Una vez celebrados tienen que ser publicados en Diario oficial que corresponda.

- iii. **Contrato de servicios:** cuando la prestación de la aplicación en modo servicio vaya más allá de la mera puesta a disposición de aplicaciones, software, infraestructuras o plataformas, incorporando, entre otras, actuaciones tales como el soporte de servicio, formación y definición de distintos entornos, podría resultar más adecuado recurrir al uso de un contrato de servicios. Son contratos de servicios aquellos cuyo objeto son prestaciones de hacer consistentes en el desarrollo de una actividad o dirigidas a la obtención de un resultado distinto de una obra o un suministro, en los términos señalados por el Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público (en adelante, **TRLCSP**).

En todo caso, debe tenerse en cuenta que los contratos de servicios celebrados por entes, organismos y entidades pertenecientes al sector público deben ajustarse, en cuanto a su preparación y adjudicación, así como en relación con sus efectos y extinción a las disposiciones de la legislación pública de contratos que les resulten en cada caso de aplicación o normas a las que estas remitan. Por tanto, a la hora de acordar su formalización, es recomendable determinar su viabilidad jurídica y garantizar que no van a generarse distorsiones de la libre competencia.

En los casos en los que, por su naturaleza las prestaciones no tenga la consideración de contrato sujeto al TRLCSP, podría resultar más apropiada la figura del convenio de colaboración, siempre que se cumplan.

- iv. **Encomienda de Gestión:** permite a los organismos administrativos o de las Entidades de Derecho público encomendar a otros órganos o Entidades de la misma o distinta Administración la realización de actividades de carácter material o técnico, siempre que entre sus competencias estén estas actividades, por razones de eficacia, o cuando no se posean los medios técnicos idóneos para su desempeño. Es decir, se transfiere el ejercicio material de una potestad.

No supone cesión de la titularidad de la competencia encomendada, de forma que el encomendante sigue siendo responsable de dictar las resoluciones o actos jurídicos que den soporte o en los que se integre la concreta actividad material objeto de encomienda.

La formalización y resolución de la encomienda debe ser publicada en el Diario oficial correspondiente para garantizar su eficacia.

Es de advertir que la Ley 40/2015 señala las reglas a las que debe someterse la formalización de la encomienda de gestión.

Así, cuando se realice entre órganos administrativos o Entidades de derecho público pertenecientes a la misma Administración deberá formalizarse en los términos que

establezca su normativa propia y, en su defecto, por acuerdo expreso de los órganos o Entidades intervinientes. Cuando la encomienda se realice entre órganos y Entidades de distintas Administraciones, la encomienda se formalizará mediante convenio, salvo en el supuesto de la gestión ordinaria de los servicios de las Comunidades Autónomas por las Diputaciones Provinciales o en su caso Cabildos o Consejos insulares.

4.2. Definición y alcance del servicio

21. Para definir este tipo de servicios, es necesario primero entender el paradigma del “*cloud computing*” cuya filosofía da forma a la prestación de aplicaciones en modo servicio. En el estudio de la ONTSI, *Cloud Computing, Retos y Oportunidades de Mayo de 2012*, se presenta el siguiente concepto de este paradigma, haciendo a su vez referencia a la definición dada por el NIST (National Institute of Standards and Technology):

El cloud computing es un modelo tecnológico que permite el acceso ubicuo, adaptado y bajo demanda en red a un conjunto compartido de recursos de computación configurables compartidos (por ejemplo: redes, servidores, equipos de almacenamiento, aplicaciones y servicios), que pueden ser rápidamente aprovisionados y liberados con un esfuerzo de gestión reducido o interacción mínima con el proveedor del servicio

22. De este modo, la prestación de aplicaciones en modo servicio supone la compartición de recursos proporcionados por un proveedor y que pueden ser utilizados por distintos suscriptores en forma de servicios. Este modelo de prestación supone importantes beneficios de ahorro en costes y esfuerzos a las Administraciones pero implican también la necesidad de definir de forma precisa el servicio a prestar y el valor que aporta en su conjunto:

- v. **Tipo de servicio:** es conveniente definir la modalidad del servicio que se va a prestar. La *Guía para clientes que contraten servicios de Cloud Computing elaborada por la Agencia Española de Protección de Datos* plantea tres tipos de modalidades:
- **Software como servicio** (modelo de servicio Software as a Service o SaaS) en el que se ofrecen en red las herramientas con las que el usuario puede implementar directamente los procesos de su empresa.
 - **Infraestructura como servicio:** en este caso el proveedor proporciona capacidades de hardware, almacenamiento y proceso en bruto sobre las que el usuario puede construir sus aplicaciones.
 - **Plataforma como servicio:** aproximación intermedia entre las dos anteriores en la que, además de hardware, se ofrecen utilidades para construir aplicaciones.

Asimismo, existe una cuarta categoría que no se plantea en la guía mencionada anteriormente pero que es de uso común y se conoce como el modelo de prestación de **procesos como servicio**. Este modelo constituye la extensión lógica del software como servicio para el suministro total de un proceso, como la gestión de cobros, en modo servicio o en la nube.

- vi. **Funcionalidades:** la definición del servicio debe incluir el listado de funcionalidades a ofrecer por el servicio en cuestión indicando además si existirán módulos de administración y configuración que permitan delegar parte de estas tareas en el suscriptor del servicio. Al igual que en el resto de ámbitos, es fundamental indicar también las funcionalidades que no están incluidas en el servicio.
 - vii. **Actividades de administración:** supone detallar el modelo de administración que se utilizará, pudiendo ser centralizado o delegado (ver apartado 8.1 de este documento). En cualquiera de los casos, es recomendable describir cada una de las actividades de administración a realizar y los indicadores de servicio que asegurarán la calidad en la ejecución de las mismas.
 - viii. **Soporte del servicio:** es oportuno definir si se dará o no soporte al servicio prestado. En caso afirmativo, será conveniente definir los niveles de servicio que se contemplarán y la estrategia de soporte según se especifica en el apartado 6 de este documento.
 - ix. **Formación:** se recomienda concretar si el servicio incluye o no formación y en qué casos se prestará dicha formación. Además, dependiendo del tipo de servicio, podrá implementarse una estrategia u otra (véase apartado 7 de este documento).
 - x. **Entornos del servicio:** es conveniente incluir en la definición los entornos tecnológicos que tendrá el servicio. Dependiendo del tipo de servicio y la modalidad de prestación, podrían ofrecerse entornos de desarrollo, pruebas e integración, certificación, formación y producción según el caso.
23. La definición del servicio y el objeto finalista del mismo es la tarea inicial de cualquier modelo de prestación de servicios en red. Es fundamental detallar, de forma explícita y lo más detallada posible, el alcance del servicio a prestar, indicando qué incluye y, en especial y explícitamente, qué no incluye.
24. Además del servicio principal, dependiendo de la naturaleza del servicio podrán existir servicios anexos, ofrecidos por el proveedor o socios del mismo, a los que aplicará el principio comentado anteriormente y para los que es importante detallar también el alcance en cada caso.
25. La definición y alcance de cada uno de los servicios permitirá al proveedor poner a disposición de potenciales suscriptores un catálogo de aplicaciones en modo servicio. Es recomendable que este catálogo incluya el máximo nivel de detalle en cada uno de los ámbitos mencionados anteriormente, con el objetivo de que los posibles suscriptores puedan valorar si los servicios ofrecidos encajan o no con sus necesidades.

4.3. Actores intervinientes

26. La prestación de aplicaciones en modo servicio supone la participación de una serie de actores adicionales a los tradicionales clientes y proveedores. Entre ellos, destacan los socios de los proveedores del servicio, que ofrecen servicios y soportes adicionales comercializados al usuario final como licencias de uso, por ejemplo.
27. De acuerdo con lo establecido en el estudio de la *ONTSI, Cloud Computing Retos y Oportunidades* y en la *Guía* para clientes que contraten servicios de Cloud Computing de la Agencia española de protección de datos, la prestación de aplicaciones en modo servicio supone la posibilidad de intervención de los siguientes actores:

- i. **Suscriptor:** también conocido como cliente o usuario final, se corresponde con el contratante de los servicios, por lo que se identifica a esta figura como cliente de proveedores, intermediarios y auditores. Es importante destacar que el cliente es el responsable de los datos personales.
- ii. **Proveedor:** agente que presta el servicio al cliente, ya sea de forma directa o a través de un intermediario. De conformidad con la Ley de Protección de Datos, el prestador del servicio es el encargado del tratamiento de los datos personales, propiedad del suscriptor.
- iii. **Socios del Proveedor:** organismos que ofrecen servicios de soporte al usuario final que son complementarios a aquellos prestados por el proveedor principal. Entre estos servicios destacan las licencias de uso y cualquier herramienta o servicio transversal que contribuya a la mejora del servicio.
- iv. **Intermediario:** el dinamismo del mercado de aplicaciones en modo servicio permite la aparición de este agente que actúa entre el proveedor y los usuarios finales ofreciendo servicios adicionales o de soporte. La aplicación de estos modelos de prestación en la administración pública supondría la prestación de servicios por parte de un organismo a otro(s), mediante la intermediación de otras entidades del ámbito autonómico o local, por ejemplo.
- v. **Habilitador:** son entidades u organismos que proveen otros servicios dirigidos a proveedores de servicios en red, como es el caso de software y hardware, para que éstos desarrollen y ofrezcan al usuario sus servicios.
- vi. **Auditor:** la prestación de aplicaciones en modo servicio supone la implementación de importantes medidas de seguridad, protección de datos y rendimiento cuya evaluación es realizada por este agente.

28. En el siguiente diagrama se ilustran los actores intervinientes mencionados anteriormente y la relación entre ellos:

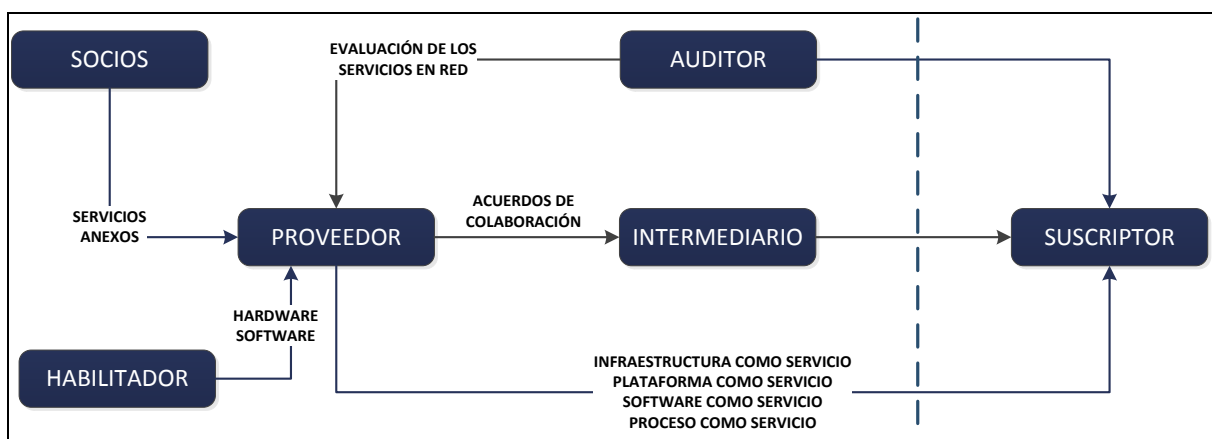


Figura 1. Actores intervinientes en la prestación de aplicaciones en modo servicio

29. Se recomienda que el proveedor identifique los distintos actores intervinientes en la prestación del servicio con el objetivo de articular los derechos y obligaciones de cada uno de ellos en el acuerdo de prestación de servicio o en los acuerdos bilaterales que se puedan establecer (por ejemplo, entre el proveedor y sus socios). La definición de los actores siempre se deberá por tanto realizar una vez definido de forma precisa el servicio a prestar.

30. A continuación se muestran una serie de ejemplos que ilustran cada uno de los roles indicados anteriormente así como sus responsabilidades y ámbitos de actuación:

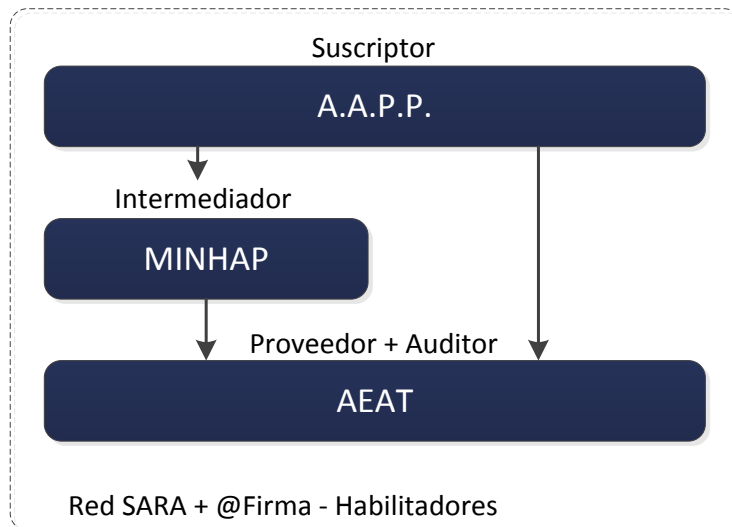


Figura 2. Roles en Plataforma ADUJAVA

31. El primer ejemplo corresponde a los roles participantes en la prestación de la aplicación en modo servicio de la plataforma de interoperabilidad ADUJAVA de la AEAT. En este caso, el suscriptor del servicio será cualquier administración pública, que podrá acceder el servicio a través de la plataforma de intermediación del MINHAP (intermediador) o por el contrario, directamente con la AEAT.
32. Este ejemplo, además de ilustrar cómo un mismo servicio puede prestarse de forma distinta, pone de relieve la figura del intermediario. En este caso, el MINHAP es el encargado de facilitar la relación con los distintos proveedores y de prestar una serie de servicios de valor añadido para el suscriptor (soporte técnico y funcional, soporte a la habilitación de procedimientos, etc.) y el proveedor (soporte a las auditorías, soporte a la habilitación de procedimientos, etc.).
33. Asimismo, en este ejemplo también aparecerían roles habilitadores, como puede ser el MINHAP a través de los servicios de red SARA y @firma.
34. A continuación se muestra otro ejemplo correspondiente al Sistema de Interconexión de Registros (SIR):



Figura 3. Roles en Sistema de Interconexión de Registros (SIR)

35. En el segundo ejemplo se puede observar un caso en el que existen dos tipos de suscriptores distintos (origen y destino) y no hay rol de intermediación del servicio. Tanto la Administración pública origen como la de destino utilizan el componente CIR del MINHAP que permite la interconexión de sus registros.

36. El habilitador del servicio, al igual que en el caso anterior, sería el MINHAP a través de la red SARA y @firma.
37. A continuación se presenta otro posible modelo de interacción de roles, es el caso del servicio de validación de certificados de @firma:

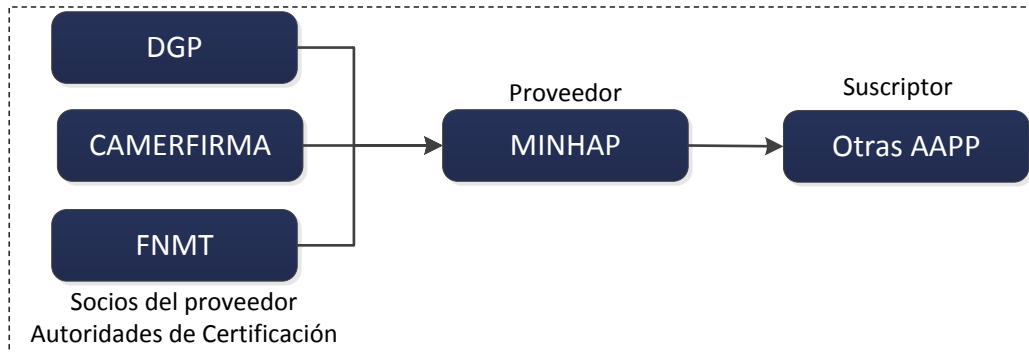


Figura 4. Roles en Sistema @Firma

En este caso, el proveedor del servicio es el MINHAP, que cuenta a su vez con una serie de socios, correspondientes a las autoridades de certificación (DGP, CAMERFIRMA, FNMT, etc.), que le permiten prestar el servicio.

Finalmente, se presenta la plataforma CI@ve para ilustrar un modelo de prestación de servicio en el que varias Administraciones actúan como un único proveedor.

En este caso, el proveedor del servicio CI@ve es la AEAT / GISS, aportando cada uno de ellos distintas funcionalidades a la plataforma:

- CI@ve ocasional - AEAT.
- CI@ve permanente - Seguridad Social.

Esta funcionalidad de clave permanente permitirá asimismo el acceso al ciudadano a la firma en la nube utilizando CI@veFirma (Certificado Centralizado de Firma) que ofrece la Dirección General de la Policía y que actúa como socio del proveedor.

Con independencia de cómo y quién desarrolle cada funcionalidad de la aplicación en red, ésta funciona como una única plataforma desde el punto de vista del suscriptor.

Asimismo, este ejemplo permite ilustrar el rol del intermediador. En este caso, el MINHAP actúa como árbitro o bróker de la identificación del ciudadano remitiendo la petición bien a CI@ve o bien a la plataforma @firma / Stork dependiendo del mecanismo de identificación utilizado.

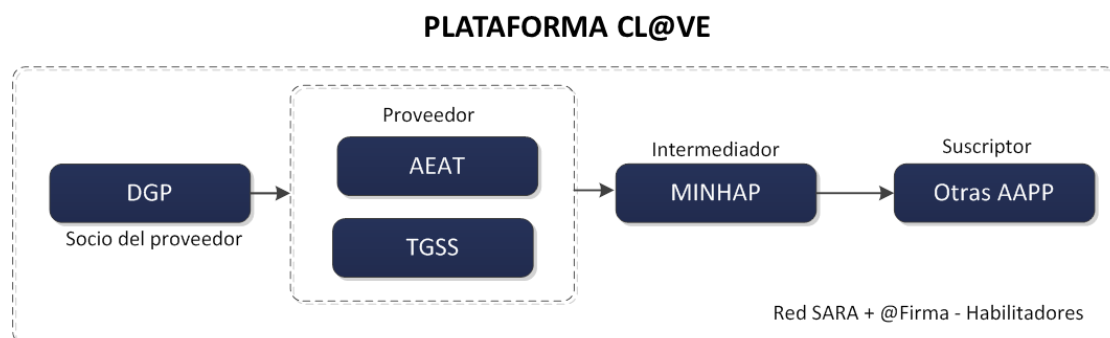


Figura 5. Roles en Sistema CI@ve

5. CONDICIONES DE PRESTACIÓN DE SERVICIO

38. Las condiciones de prestación de servicio son acordadas entre el proveedor y el suscriptor del servicio al inicio de la prestación y permiten establecer unos mínimos aceptados de calidad del servicio sobre los que el proveedor podrá focalizar sus esfuerzos de mantenimiento y soporte del servicio. Dependiendo de los organismos participantes y el tipo de servicio, podrán establecerse compromisos flexibles de calidad del servicio o mecanismos más formales tales como acuerdos de nivel de servicio.

5.1. Acuerdos de Nivel de Servicio

39. Con el objetivo de articular las condiciones y términos que regularán la prestación del servicio, se recomienda que el proveedor acuerde con el cliente unos niveles de servicio (*Acuerdos de Nivel de Servicio – ANS*). Estas condiciones se definirán a través de indicadores que permitirán cuantificar la calidad del servicio en términos de capacidad, disponibilidad, continuidad, gestión de incidentes y cualquier otro ámbito que afecte al servicio prestado.

40. Para una correcta definición de los indicadores se recomienda incluir los siguientes atributos para cada acuerdo:

- i. **Descripción del Indicador:** detalle del indicador, qué mide, cómo y con qué fuente de datos y la finalidad del indicador definido.
- ii. **Responsabilidades:** quién recoge y facilita los datos necesarios para realizar los cálculos.

En el contexto de la prestación de aplicaciones en modo servicio en red, puede ser necesaria la participación de un tercero independiente que verifique la calidad del servicio a través de la mediación de los indicadores definidos (rol de auditor).

- iii. **Fórmula:** para el cálculo y obtención del nivel de servicio periódico de cara a poder identificar si se ha cumplido o no el acuerdo.
- iv. **Umbrales:** valores mínimos en la prestación de la aplicación en modo servicio que disparan situación de aviso (monitorizar) y de alarma (corregir). Estos umbrales deben ser consensuados entre ambas partes aunque el proveedor podría definir otros umbrales de cara al aseguramiento de la calidad en el servicio. En caso de que el servicio se preste por debajo de los umbrales mínimos establecidos, se podrán establecer penalizaciones (ver apartado 13.3).
- v. **Periodicidad de la captura de datos,** cálculo de las métricas derivadas y de la verificación de umbrales de aviso. Se debe determinar además la periodicidad de los informes de cumplimiento de los ANS.

41. Es importante tener en cuenta que en algunos casos, y en función del tipo de servicio, el suscriptor del servicio puede reservarse el derecho de auditar los datos y el proceso de recogida de información y elaboración de los indicadores acordados.



5.2. Ejemplos de Indicadores de Nivel de Servicio

42. A continuación se describen los indicadores de nivel de calidad más comunes. En cualquier caso, el prestador del servicio deberá identificar aquellos que se adapten mejor a la aplicación en modo servicio en cuestión o incluir aquellos que considere necesario para controlar la calidad del servicio.

5.2.1. Horario de prestación del servicio

43. El prestador del servicio debe asegurar que la aplicación en modo servicio está disponible dentro de la franja horaria acordada con el cliente con la posibilidad de definir distintas franjas horarias para módulos o procesos críticos que así lo requieran.
44. Además, es importante indicar los casos en los que el horario podría ser ampliado debido a incidencias o momentos críticos. Asimismo, deberán establecerse los horarios de paradas y no disponibilidad del sistema, teniendo en cuenta que estas paradas deben ser en horario no-laboral, planificadas, comunicadas y aceptadas por el cliente que consume el servicio.
45. El establecimiento del horario de prestación del servicio será fundamental para el cálculo de indicadores de tiempos de resolución de incidencias especificados en el apartado 5.2.3. ya que sólo contabilizarán las horas en las que el servicio está operativo.

5.2.2. Disponibilidad del servicio

46. En función de la criticidad de la aplicación en modo servicio prestada, deberán acordarse porcentajes de disponibilidad, identificándose si hubiera períodos críticos en los que se requieren mayores niveles de disponibilidad.
47. Asimismo, es importante tener en cuenta la necesidad de procesos de mantenimiento, actualización y mejora de tecnológica del servicio, para lo que deberán pactarse las franjas horarias sobre las que realizar dichas actividades con el menor impacto posible de cara a cliente.
48. A continuación se presenta un ejemplo de posibles indicadores de disponibilidad:

Definición del Indicador
% de disponibilidad mensual del servicio en condiciones normales
% de disponibilidad del servicio en períodos críticos

Tabla 1. Ejemplos de indicadores de disponibilidad del servicio

49. En el caso de que el servicio incluya entornos tecnológicos de desarrollo, integración o pruebas, se recomienda establecer umbrales específicos para cada entorno.

5.2.3. Tiempos de respuesta por prioridad e impacto

50. La concurrencia de múltiples incidencias de la aplicación en modo servicio es una situación que puede producirse con regularidad, por lo que es necesario asignar niveles de prioridad para resolución de las mismas. Como norma general, se recomienda especificar la prioridad de la incidencia conforme a dos parámetros:
- Impacto:** cómo afecta a otros procesos y/o número de usuarios.
 - Urgencia:** tiempo determinado por el cliente de resolución conforme a prioridades del negocio o cumplimiento de Acuerdos de Nivel de Servicio.

51. Existen otros factores que podrían afectar la prioridad asignada a una incidencia:
- iii. Tiempo esperado de resolución.
 - iv. Número de recursos asignados para su resolución.
 - v. Cambio de prioridad conforme evoluciona la resolución de la incidencia.
52. A partir de los factores comentados anteriormente, se recomienda definir niveles de prioridad. Para cada nivel, se acordarán entre el cliente y proveedor distintos tiempos de resolución. A continuación se muestra un ejemplo de tiempos de resolución de incidencias con tres niveles de prioridad:

Prioridad	Tiempo de Resolución
1	Inferior a 4 horas
2	Inferior a 24 horas
3	Inferior a 4 días

Tabla 2. Ejemplos de tiempo de resolución de incidencias por prioridad

53. Posteriormente, se podrán definir distintos indicadores relacionados con los tiempos de resolución de incidencias en el servicio, repetición de incidencias del mismo tipo y calidad de la resolución, tal como se muestra en el siguiente ejemplo orientativo.

Definición
% mensual de incidencias resueltas en plazo y aceptadas por el suscriptor.
% de incidencias repetidas, en un período posterior a la resolución inicial, respecto a la cantidad de incidencias resueltas en dicho período.
% de resolución de incidencias aprobadas en primera instancia.

Tabla 3. Ejemplos de indicadores de tiempos de resolución de incidencias

5.2.4. Transacciones por segundo

54. Dependiendo del tipo de servicio prestado, podrán definirse indicadores de velocidad que pueden definirse por el número de transacciones o datos transferidos por segundo. Al inicio de la prestación se acordará este indicador dependiendo del tipo de servicio y se definirán los umbrales de alerta y acuerdos de nivel de servicio relacionados.
55. Algunos ejemplos de estos indicadores se muestran a continuación:

Definición
Número de transacciones soportadas por segundo
Volumen de datos transferidos por segundo

Tabla 4. Ejemplos de indicadores de transacciones por segundo

6. MODELO Y ALCANCE DE SOPORTE

56. En aquellas aplicaciones en modo servicio en las que se incluyan actividades de soporte, se recomienda establecer un modelo y alcance del soporte en el que se determinen:
- Niveles y actividades de soporte.
 - Procedimientos de Gestión del soporte al Servicio.
 - Herramientas.
 - Canales de soporte.
 - Estrategia de los períodos no intensivos.

6.1. Niveles de Soporte

57. Resulta conveniente definir los niveles de soporte del servicio que prestará el proveedor del detallando fases, actividades, entregables y equipo de soporte en cada uno de los niveles. Los procesos y niveles definidos tendrán que integrarse de manera efectiva con las herramientas de soporte, con el resto de niveles y con las normativas de gestión, seguridad y calidad del proveedor.
58. A continuación se establece una propuesta de niveles de soporte que pueden ser tomados como referencia para el diseño de aplicaciones en modo servicio:



Figura 6. Modelo de niveles de soporte de servicios TI

6.1.1. Nivel 1. Servicio de atención y soporte a usuarios general

59. Este nivel es el punto de contacto con el usuario final de la aplicación en red, destinado a proporcionarle ayuda básica en el uso de la misma o derivar la solicitud a otros niveles en caso de que sea necesario un tratamiento más especializado. Se recomienda establecer qué cuestiones o tipos de incidencia se deberán resolver en este nivel y cuáles podrán escalar al soporte especializado.
60. Con carácter general, el soporte de nivel 1 para las aplicaciones en red es siempre prestado por el suscriptor del servicio que definirá los canales a poner a disposición para interacción con el usuario final.



6.1.2. Nivel 2. Servicio de Atención y soporte a usuarios especializado

61. Al inicio de la prestación del servicio se recomienda acordar entre el proveedor y el suscriptor el alcance de este nivel de soporte. En general, se diferencian dos grupos de trabajo:
- i. Soporte especializado presencial: acompañamiento in-situ al usuario que hace la solicitud.
 - ii. Soporte especializado remoto: soporte por otros canales de comunicación no presenciales: herramientas de gestión de soporte, correo electrónico, teléfono, entre otros.
62. Dependiendo del tipo y complejidad del servicio prestado, el soporte de nivel 2 puede ser realizado por el suscriptor o centralizado en el proveedor.

6.1.3. Nivel 3. Servicio de Mantenimiento

63. A este nivel serán derivadas todas las solicitudes que requieran una intervención sobre el servicio para su resolución. Dentro de este nivel podrán entrar los mantenimientos adaptativos, preventivos, perfectivos, intervenciones por modificaciones en normativas legales y evolutivos.
64. Por lo general, se recomienda que todas las intervenciones derivadas de este nivel sean planificadas, siguiendo el procedimiento de publicación de nuevas versiones del servicio del apartado 8.2.3 de este documento. No obstante, puede darse el caso de que ciertas intervenciones no puedan ser planificadas por su naturaleza, en cuyo caso tendrán que definirse procedimientos de contingencia.
65. La calidad del servicio de mantenimiento será controlada mediante la definición de indicadores de servicio y tiempos de respuesta, tal como se detalla en el apartado 5.2.
66. El servicio de mantenimiento por lo general podrá incluir dos tipos de servicios:
- i. **Servicios No-planificables:** agrupa las líneas de servicio que, por su naturaleza, no pueden planificarse en el tiempo, como por ejemplo mantenimiento correctivo, consultas y otras peticiones o acciones.
 - ii. **Servicios planificables:** tales como mantenimiento adaptativo, mantenimiento perfectivo, cambios en el servicio por normativas legales y mantenimiento evolutivo.

Los servicios de mantenimiento de nivel 3 son generalmente ejecutados por el proveedor del servicio.

6.1.4. Nivel 4. Servicio de Administración de Sistemas, Seguridad y Comunicaciones

67. Se encargará del alta y baja de usuarios en el servicio, configuración de políticas de seguridad, roles y perfiles y posibles incidencias de comunicaciones reportadas por los usuarios que puedan estar relacionadas con la infraestructura.
68. En la mayoría de los casos el soporte avanzado de nivel 4 es también proporcionado por el proveedor del servicio. No obstante, es posible que parte de este soporte pueda ser ofrecido

por el suscriptor, como ocurre en el caso de altas y bajas de usuarios de modelos delegados, que se proporcionarían como parte del nivel 1 de soporte.

6.1.5. Nivel 5. Servicio de escalado a socios del proveedor

- 69. En caso de que se presente una incidencia o solicitud de soporte que no pueda ser resuelta por el proveedor del servicio, se escalará el asunto a sus socios (proveedores de hardware o licencias de software) para proceder a su subsanación.
- 70. Este nivel de servicio sólo aplica a aquellos servicios en los que participan socios del proveedor o incluso proveedores de software y hardware habilitador del servicio.

6.1.6. Ejemplo de niveles de servicio

- 71. En el diagrama a continuación se muestra un ejemplo de los niveles de servicio implementados para la Plataforma de Intermediación de MINHAP.

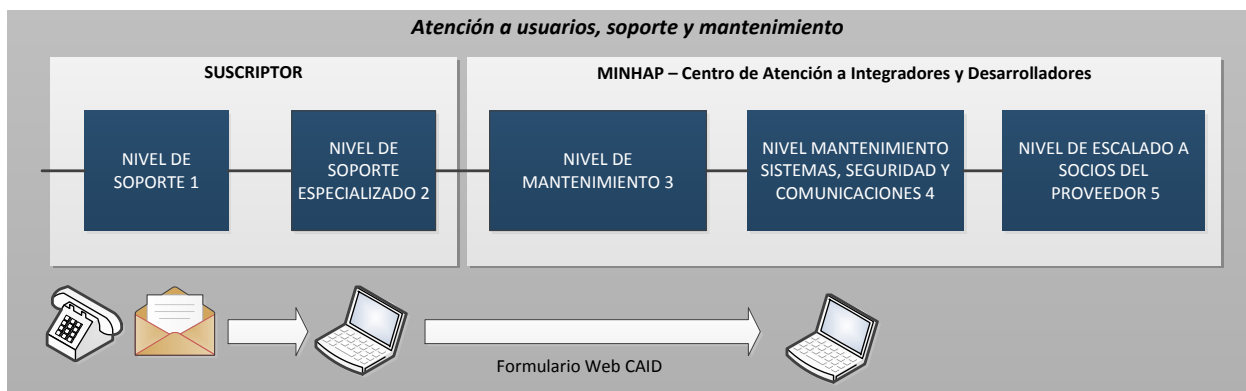


Figura 7. Niveles de Servicios Plataforma de Intermediación del MINHAP

- 72. Con carácter general, el suscriptor del servicio (CC.AA. o EE.LL.) dispondrá de un portal de consulta de los certificados que estará integrado con la plataforma de intermediación a través de servicios web.
- 73. En estos casos, el soporte de primer nivel a los usuarios del suscriptor será su propio CAU o grupos de soporte específicos. Este servicio cubrirá las incidencias asociadas a dicho portal, así como cuestiones referidas a los errores más comunes remitidos por la plataforma de intermediación.
- 74. En el caso de que la incidencia reportada sea de carácter técnico, el suscriptor la escalará al Centro de Atención a Integradores y Desarrolladores (CAID) del MINHAP (proveedor del servicio) a través del formulario web habilitado para su resolución. En función del tipo de incidencia, podrá derivarse dentro del CAID a otros niveles especializados de mantenimiento de sistemas, seguridad y comunicaciones o a los proveedores del servicio final.

6.2. Procedimientos de Gestión del Servicio

- 75. Resulta conveniente establecer mecanismos de seguimiento y gestión de incidencias y peticiones sobre las herramientas que se implementen para este fin. Las incidencias y peticiones deberán identificarse y priorizarse, para lo que pueden utilizarse reconocidas metodologías de gestión de servicios IT como es el caso de ITIL. De especial importancia es

la gestión de incidencias repetitivas en el servicio, que deben dar lugar a una actuación de mantenimiento perfectivo que elimine el problema base. Además, es necesario tener en cuenta el plan de comunicación a seguir en el caso de incidencias globales que puedan afectar a varios servicios y, por lo tanto, a distintos suscriptores.

76. Los procedimientos definidos para el soporte del servicio podrán estar encaminados a asegurar aspectos tales como:
- i. Gestión de Recursos: asegurar que el esfuerzo dedicado a cada petición y/o actividad de ajusta a las necesidades del servicio, de manera que se pueda distribuir y ajustar la dedicación y esfuerzo asociado a cada tarea.
 - ii. Gestión de entrega: de cara a asegurar la calidad de los entregables relacionados con tareas de soporte del servicio.
 - iii. Gestión del conocimiento: mantener actualizada la documentación relacionada con el servicio, cuestiones o dudas frecuentes, incidencias o problemas comunes, etc. La gestión del conocimiento incluye actualizar la documentación de la aplicación en modo servicio en el caso de nuevas versiones.
 - iv. Gestión de riesgos: con el objetivo de anticipar acciones necesarias e involucrar perfiles adecuados para la resolución de solicitudes.
 - v. Gestión de las relaciones: que permita coordinar interlocutores clave, gestión de expectativas y comunicación interna entre niveles de soporte.
77. Una vez definidos los procesos de soporte, se recomienda a la administración prestadora del servicio realizar revisiones periódicas del cumplimiento, planificando las actividades a realizar por los recursos de soporte durante el próximo período.

6.3. Herramientas

78. Se recomienda que los procesos de soporte del servicio estén apoyados en herramientas de gestión específicas, flujos de trabajo y niveles de servicio. La infraestructura, recursos y licencias necesarias para la implantación de estas herramientas suele ser responsabilidad del proveedor del servicio. En el caso de modelos de soporte y administración delegada, se deberá tener en cuenta la posibilidad de integrar herramientas de gestión del servicio del suscriptor y del prestador del servicio.
79. Asimismo, se deberá contemplar la posibilidad de que el cliente solicite acceso a los datos históricos de las herramientas de gestión que se encuentran en uso, lo que supone que el proveedor deberá disponer de mecanismos ágiles para la explotación efectiva por parte de un tercero en casos de auditorías externas o como parte de la portabilidad de cara al traspaso del servicio a un nuevo proveedor.



6.4. Canales de soporte

80. Además de los niveles de servicio, procesos y herramientas, es recomendable al inicio del servicio definir los canales de asistencia que podrá utilizar el suscriptor para comunicar nuevas solicitudes: teléfono o herramientas de soporte electrónico (formularios web o herramientas de “ticketing”) fundamentalmente.

81. Asimismo, se deben definir y habilitar mecanismos de comunicación entre los distintos niveles de soporte, de cara a simplificar el traspaso de solicitudes y agilizar la ejecución de los procedimientos definidos anteriormente.

6.5. Otras consideraciones de soporte

82. Dependiendo del tipo de aplicación en modo servicio ofrecida, es posible que existan períodos intensivos y menos intensivos para los que es oportuno definir una estrategia particularizada de soporte.
83. Es aconsejable tener en cuenta la estructura y dimensionamiento del equipo de soporte durante estos períodos.
84. Resulta conveniente además reforzar los procedimientos de gestión del conocimiento durante períodos intensivos, con el objetivo de que el soporte regular pueda heredar la experiencia adquirida en dichos periodos.

7. MODELO Y ALCANCE DE FORMACIÓN

85. En el caso de que el servicio incluya formación, se recomienda establecer una estrategia de formación donde se definan:
- i. Colectivos a formar.
 - ii. Estrategia de formación.
 - iii. Ciclos del proceso formativo.
 - iv. Infraestructura de formación.

7.1. Colectivos

86. Es recomendable como aspecto inicial a la definición del modelo de formación, identificar los distintos perfiles de usuarios y colectivos que tendrán acceso al servicio. Algunos colectivos que pueden requerir formación son los siguientes:
- i. Usuarios finales con acceso a funcionalidades operativas.
 - ii. Usuarios directivos.
 - iii. Usuarios funcionales TIC y futuros formadores.
 - iv. Administradores del servicio.
 - v. Integradores.

7.2. Estrategia de formación

87. La estrategia de formación a implementar debe proporcionar conocimientos a los colectivos incluidos en el alcance de la formación, de las capacidades y conocimientos en función de su categoría y responsabilidades que deberán ser definidas por el suscriptor del servicio.
88. El alcance de la formación a seguir no necesariamente será igual para distintos colectivos. Por ejemplo, es posible que el tipo de servicio a prestar permita dar una formación de tipo e learning a usuarios finales y formación no reglada con manuales a usuarios TIC. En cualquier caso, es oportuno que se identifiquen todas las posibles casuísticas al inicio del servicio.
89. La estrategia de formación a seguir dependerá de distintos factores que deben ser valorados al inicio de la prestación del servicio:
- i. **Tipos de perfiles de usuarios:** la formación tendrá que ser personalizada para distintos tipos de usuarios, según las funcionalidades a las que tendrán acceso dentro del sistema.
 - ii. **Dispersión geográfica:** este aspecto es fundamental a la hora de tomar la decisión de adoptar una estrategia de formación. Las aplicaciones en modo servicio se caracterizan por un nivel de dispersión muy alto.
 - iii. **Dispersión en el tiempo:** la formación podrá realizarse en distintos momentos de la prestación del servicio, por lo que se recomienda prever la existencia de varios ciclos formativos (ver apartado 7.3. Ciclos del proceso formativo).

- iv. **Dispersión en la incorporación del servicio:** es importante tener en cuenta el tiempo que va a transcurrir entre la formación y el inicio de la prestación del servicio a los distintos usuarios, puesto que en algunos casos puede ser necesario planificar distintos ciclos formativos para nuevas incorporaciones de usuarios.



90. Habitualmente, la estrategia formativa a seguir en modelos de aplicaciones en modo servicio en red está enfocada en formación reglada a formadores y otros mecanismos de formación no presencial. En este sentido, suelen ser de amplio uso las siguientes vías de formación:

- i. **Formación a formadores:** se podrán plantear sesiones formativas a formadores en función del tipo de servicio. Estos formadores serán luego los responsables de formar a usuarios finales de las administraciones a las que correspondan.
- ii. **E-Learning:** basada en el desarrollo de tutoriales interactivos sobre diferentes procesos y procedimientos del sistema. Este tipo de formación puede utilizarse como complemento a la formación a formadores o para formaciones masivas introductorias.
- iii. **Formación no reglada:** manuales de usuarios, diseños funcionales, técnicos y cualquier otra documentación de apoyo para el uso, administración e integración con la aplicación en modo servicio, en función del tipo de aplicación ofrecida.

91. Como ejemplo ilustrativo de una estrategia de formación de una aplicación en modo servicio en red, cabe destacar la aplicación ORVE. En este caso, se ha seleccionado una estrategia de formación a formadores de forma virtual que se ha combinado con vídeos explicativos y un entorno de formación sobre el que probar las funcionalidades de la aplicación.

92. Otro ejemplo de estrategia de formación se puede observar en la plataforma de interoperabilidad. En este caso, la estrategia consiste en formación a personal TIC de carácter no presencial, con manuales del estándar SCSP, guías de consumo de servicios y otra documentación de integración y técnica.

7.2.1. Otras consideraciones de la estrategia formativa

93. Aunque de menor uso en la prestación de servicios, es importante tener en cuenta que existen otros modelos posibles de formación que podrían adoptarse en casos particulares o un reducido tipo de servicios en red.

94. Una estrategia que podría aplicarse, aunque no comúnmente en este modelo de prestación, es la formación presencial a usuarios finalistas. Este tipo de formación solo se recomienda en aquellos casos en los que el número de usuarios del servicio es limitado y el uso de la aplicación puede suponer una complejidad importante.

7.3. Ciclos del proceso formativo

95. En función de la naturaleza del servicio prestado, podrán definirse distintos ciclos formativos para los que se podrán abordar distintas estrategias de las planteadas anteriormente. En cualquier caso, es importante que los ciclos formativos definidos estén alineados con las previsiones de evolución del servicio y planificación de inclusión de nuevos colectivos por parte del suscriptor. Del mismo modo, en algunos casos es posible prever necesidades extraordinarias de formación por cambios normativos o de plataformas, en cuyo caso también se recomienda adoptar una estrategia diferenciada.

96. En general, es recomendable abordar una estrategia en tres ciclos formativos:

- i. **Ciclo formativo inicial:** corresponde al inicio de la prestación del servicio. Este ciclo corresponde a la formación a usuarios finales, previa al comienzo de prestación del servicio pudiendo contemplarse además la formación conceptual al equipo directivo del cliente dirigido a la toma de decisiones.
- ii. **Ciclo formativo de mejora y perfeccionamiento:** estos ciclos formativos pueden surgir a demanda, aunque se recomienda acordar el número máximo de ciclos de este tipo que pueden surgir durante la prestación del servicio.
- iii. **Ciclo formativo extraordinario:** los ciclos formativos extraordinarios son acciones de formación no previstas que pueden deberse a actividades planificadas (nuevas versiones, incorporación de nuevos componentes, actualización de infraestructura) o no planificadas (cambio en la normativa, incorporación de nuevo personal, nueva directiva,..).

7.4. Infraestructura de formación

97. Un aspecto importante a tener en cuenta para el desarrollo de la estrategia formativa desarrollada es la infraestructura en la que se realizará dicha formación. En este ámbito, se pueden distinguir dos tipos de infraestructura:
- i. **Infraestructura física:** relacionada con el espacio físico o virtual en el que se realizarán las formaciones: plataforma de e-learning, salas de videoconferencias y material relacionado con el espacio formativo.
 - ii. **Infraestructura tecnológica:** es recomendable la creación de un entorno de formación específico para la realización de las actividades de formación.

8. CONSIDERACIONES DE ADMINISTRACIÓN DEL SISTEMA

8.1. Administración del sistema



98. Un cambio fundamental en la prestación de aplicaciones en modo servicio es que las operaciones de administración del sistema no siempre son tarea exclusiva del cliente que consume el servicio sino que es posible delegar algunas tareas en el proveedor.
99. Dependiendo del modelo de administración adoptado, se plantean a continuación los principales aspectos a considerar.

8.1.1. Administración centralizada

100. Muchos clientes de aplicaciones en modo servicio prefieren delegar la administración en el proveedor. De esta forma, el consumidor del servicio no tiene que preocuparse por realizar tareas de administración, aspecto que en algunos casos puede ser condicionante para posibles ampliaciones de colectivos o evolución del servicio contratado.
101. En el modelo de administración central, el cliente autoriza al proveedor a administrar el servicio. Es importante definir, al principio del documento de formalización de la prestación del servicio, el alcance de las tareas de administración a realizar por parte del proveedor.
102. Asimismo, se tendrán que definir los procedimientos, herramientas y canales de soporte y gestión para solicitud de nuevos usuarios, modificación de tablas maestras, ejecución de scripts y cualquier otro tipo de operaciones de administración a realizar por el organismo prestador del servicio.
103. A pesar de que las operaciones de administración serán realizadas por el prestador del servicio, la relación actualizada de usuarios y perfiles de usuarios es responsabilidad del consumidor del servicio, que tendrá que tener disponible esta información para que el proveedor pueda realizar las actividades correspondientes, tal como se plantea en el RLOPD:

El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

8.1.2. Administración delegada


104. En este modelo, el cliente mantiene las responsabilidades de administración del servicio prestado. En este caso el prestador del servicio simplemente proporciona los medios para mantener la disponibilidad acordada del servicio contratado. Salvo que se acuerde lo contrario, el proveedor no tendrá la responsabilidad de definir procesos, canales y herramientas de gestión ya que los mismos serán implementados por el cliente en sus instalaciones. No obstante, es una buena práctica por parte del prestador, el hecho de recomendar al cliente la implementación de mecanismos de gestión de la administración del servicio:

- i. Políticas de control y gestión de actualizaciones de la información.
 - ii. Periodicidad y procesos de revisión sobre obsolescencia de registros y usuarios.
 - iii. Otras políticas particulares al tipo de servicio prestado.
105. Este modelo de Administración es ampliamente utilizada en aplicaciones en modo servicio gracias a su versatilidad y a las múltiples ventajas que aporta tanto para el suscriptor como para el proveedor. En este sentido, cabe citar como ejemplo el portal de Entidades locales (<https://ssweb.seap.minhap.es/portaleELL/>).
- A través de este portal, las Entidades locales pueden acceder a diversas aplicaciones en modo servicio que el MINHAP pone a su disposición y entre las que destacan ORVE, IRIA o la gestión de documentación para su remisión a la AGE.
- Cada Administración local adherida al portal, cuenta con un Administrador delegado con capacidad para gestionar los usuarios y permisos de su Administración de forma ágil y totalmente autónoma para todas las aplicaciones.
- Asimismo, cada vez que la Entidad solicita utilizar una nueva aplicación o servicio, el Administrador del MINHAP habilita al Administrador delegado para que éste pueda gestionar la nueva aplicación en su entidad.
- Este modelo por tanto facilita la autogestión de la Entidad local permitiendo asimismo al MINHAP concentrarse en tareas de más valor añadido para las EELL como el desarrollo de nuevos servicios o la evolución de los existentes.

8.2. Administración de la infraestructura

106. En la prestación de aplicaciones en modo servicio, existen algunos procesos de administración del servicio en los que se pueden dar particularidades derivadas del propio modelo. En especial, es importante abordar estas posibles particularidades en la gestión de la capacidad, gestión de la continuidad del servicio y gestión de la disponibilidad.

8.2.1. Gestión de la capacidad

107. La gestión de la capacidad es muy recomendable para planificar la capacidad de proceso y almacenamiento necesaria para la prestación de aplicaciones en modo servicio. A través la gestión de la capacidad, el proveedor podrá dimensionar adecuadamente la infraestructura tecnológica para la prestación del servicio.
108.  En este contexto, se considera positivo solicitar a los suscriptores del servicio una planificación del consumo de capacidad del servicio (almacenamiento, proceso, etc.) con suficiente antelación y periodicidad como para permitir al prestador del servicio la adecuación de la infraestructura existente a las necesidades de capacidad previsibles.
109. Como ejemplo ilustrativo, cabe destacar el servicio INSIDE del MINHAP a través del cual las AA.PP. pueden suscribir un servicio de almacenamiento de expedientes y documentos electrónicos alineado con el Esquema Nacional de Interoperabilidad (en adelante ENS). Con el objetivo de dimensionar la capacidad del almacenamiento, el MINHAP solicita anualmente a los suscriptores del servicio una previsión de almacenamiento para los próximos años.

8.2.2. Gestión de la continuidad del servicio / disponibilidad

110. La continuidad y disponibilidad de las aplicaciones en modo servicio constituye una de las principales barreras a la hora de contratar este tipo de servicios.
111. Por ello, resulta conveniente que el proveedor del servicio defina y establezca un Plan de Continuidad del Servicio en el que se determinen todas las acciones para volver a prestar el servicio tras un incidente de fuerza mayor.
112. Para elaborar el Plan de Continuidad del Servicio resulta clave evaluar en primer término el impacto para el suscriptor en términos de negocio de una indisponibilidad del servicio temporal o prolongado en el tiempo. Así, por ejemplo no supone el mismo impacto en el suscriptor la indisponibilidad de un servicio de generación de nóminas en red que el servicio de consulta de certificados electrónicos a través de la plataforma de intermediación.
113. A partir de esta reflexión, el proveedor del servicio podrá identificar las acciones, procesos y elementos mitigadores en caso de indisponibilidad temporal o prolongada del servicio.

8.2.3. Gestión de la entrega

114. La gestión de la entrega incluye todos procesos asociados a la publicación de nuevas versiones de la aplicación en red o su plataforma base en los distintos entornos tecnológicos.
115. Con carácter general, estas intervenciones deberán realizarse en horarios que supongan un menor impacto en el servicio prestado a los suscriptores. Asimismo, se recomienda establecer procedimientos reglados de comunicación de dichas intervenciones con suficiente antelación entre el prestador y el suscriptor.
116. En el caso de la publicación de nuevas versiones, se recomienda establecer protocolos y procedimientos específicos en función del entorno afectado:
 - i. **Publicación en entorno de Integración:** este entorno puede ser crítico para la prestación de determinadas aplicaciones en modo servicio ya que permitirá realizar las pruebas de integración de los distintos componentes del servicio.

Al ser un entorno de pruebas, los horarios de publicación en este entorno pueden contar con cierta flexibilidad aunque es importante una correcta coordinación con los distintos equipos involucrados.
 - ii. **Publicación en preproducción:** resulta conveniente para determinados servicios requerir la participación del cliente para validar nuevas funcionalidades (por ejemplo, en el caso de que la aplicación y servicio prestado incluya cierta configuración o funcionalidad a medida del cliente).

Al igual que en el caso anterior, los horarios de estas publicaciones cuentan con cierta flexibilidad.
 - iii. **Publicación en producción:** en este caso el horario y tiempo de publicación resulta crítico por lo que es importante definir ventanas de actualización con suficiente antelación y comunicándolo a través de procesos previamente establecidos.

9. RESPONSABILIDAD Y BUEN USO

117. Es una buena práctica para la prestación de aplicaciones en modo servicio, acordar con los suscriptores las condiciones de los servicios a prestar. Estas condiciones pueden incorporarse como cláusulas formales en el documento de acuerdo de prestación del servicio o pueden ser proporcionadas en un documento de políticas generales de buen uso de servicios IT en red y podrán incorporar responsabilidades por el no cumplimiento de alguna de las condiciones de buen uso. A continuación se presentan un conjunto de posibles recomendaciones a incorporar:

i. Gestión de Usuarios

- No se deben realizar altas de usuarios incorrectos en el servicio y debe existir una política de limpieza de usuarios obsoletos. En el caso de un modelo de administración central, estas tareas serán realizadas por el proveedor pero será el suscriptor del servicio quién mantendrá un catálogo de usuarios actualizados e informará sobre modificaciones en el mismo para su actualización en el servicio.
- Si el alta de nuevos usuarios es delegada en el suscriptor o un tercero, es una buena práctica notificar al proveedor antes de realizar altas masivas de usuarios en producción, de cara a gestionar la capacidad de los recursos.

ii. Desarrollos y pruebas

- Se deberá notificar al proveedor antes de realizar pruebas de carga y estrés. Además, estas pruebas deberán realizarse en los entornos habilitados para ello y nunca en producción.
- En el caso de que el modelo de prestación del servicio permita al suscriptor el desarrollo de nuevos módulos o integraciones, se recomienda seguir los estándares del servicio, que deberán ser proporcionados previamente por el proveedor del servicio.
- Del mismo modo, en caso de que el suscriptor o terceros tengan posibilidad de ejecutar scripts en base de datos, se recomienda que los mismos requieran autorización del proveedor del servicio antes de su ejecución en producción. Además, se deberá tener especial cuidado de que los scripts ejecutados no comprometan la integridad de las bases de datos.

iii. Operativa del servicio

- Se podrá estudiar la posibilidad de incluir en el acuerdo contractual la obligación de notificar cualquier incremento planificado en la demanda del servicio por parte del suscriptor. De cualquier forma, es una buena práctica avisar sobre posibles picos para gestionar la capacidad del servicio.
- El suscriptor es responsable de no incluir datos o ficheros con código malicioso o virus que puedan afectar la operativa del servicio. En caso de que esto ocurra, se podrán estudiar distintos modelos de penalización como los planteados en el siguiente apartado.

9.1. Régimen de supervisión y penalizaciones

118. Como proveedor del servicio, se podrán establecer revisiones periódicas del uso de los servicios con el fin de supervisar que se está dando cumplimiento a las políticas de buen uso definidas y distribuidas a los suscriptores del servicio. De igual forma, es posible definir posibles penalizaciones por incumplimiento de alguna de las condiciones consideradas como buenas prácticas en la utilización de los servicios. Estas penalizaciones pueden articularse de distintas formas:
- Penalizaciones económicas sobre la facturación del servicio: se podrán plantear porcentajes máximos de penalización en función del número de incumplimientos en las condiciones.
 - Disminución o corte del servicio: en algunos casos podrá plantearse la reducción de las prestaciones del servicio (capacidad, disponibilidad, etc.) o incluso el corte del servicio al suscriptor durante un período temporal o definitivo.
119. En cualquier caso, las posibles penalizaciones en las que se puede incurrir deben estar claramente especificadas en el acuerdo de prestación del servicio que se adopte.

10. SEGURIDAD

120. El organismo que ofrezca aplicaciones en modo servicio en el ámbito de las administraciones públicas, debe asegurar que cumple con las garantías de seguridad establecidas en el Esquema Nacional de Seguridad. Resulta conveniente que el prestador del servicio evalúe dichas garantías y, en función de ello, articule las medidas de protección correspondientes. Esta información debería ser conocida por el suscriptor para evaluar la conveniencia de utilizar el servicio según las características del uso. Las principales garantías a considerar son:
- Seguridad integral, coordinando todos los elementos técnicos, humanos, materiales y organizativos relacionados con el servicio.
 - Gestión de riesgos, de vital importancia en servicios en red porque permitirá el mantenimiento de un entorno controlado.
 - Prevención, reacción y recuperación, para reducir la posibilidad de amenazas, atajando los incidentes de seguridad a tiempo.
 - Líneas de defensa, que se materializa en estrategias de protección constituidas por múltiples capas de seguridad.
 - Reevaluación periódica, de cara a adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.
 - Función diferenciada, distinguiendo entre el responsable de la información, responsable del servicio y responsable de la seguridad.
121. Es necesario que el proveedor valore la sensibilidad del servicio prestado a los suscriptores y la conveniencia de acreditar la conformidad con el ENS. Esto podría incluir, por ejemplo, una auditoría independiente de las medidas implantadas en el servicio, incluidos los registros que permiten conocer quién ha accedido a los datos de los que es responsable y el cifrado de los mismos, o que al inicio de la prestación del servicio un tercero independiente audite la seguridad del servicio.
122. Por otra parte, el proveedor informará diligentemente al suscriptor sobre la ocurrencia de incidentes de seguridad que afecten los datos de los que es responsable, así como de las medidas que deban ser adoptadas por ambas partes para resolución del incidente y evitar daños que puedan producirse. Del mismo modo el suscriptor ha de establecer las medidas de seguridad cuya aplicación es su responsabilidad, como puede ser el caso de la comunicación de bajas de usuarios del sistema cuando ya no requieran acceso al mismo y acciones de concienciación y formación a usuarios en materias de seguridad, entre otras.
123. Otro aspecto de seguridad de especial importancia en la prestación de aplicaciones en modo servicio es la protección de las comunicaciones. Se deberán configurar los mecanismos necesarios para que el sistema pueda proteger el perímetro de comunicaciones y permita la detección de intrusiones en el servicio, en particular, si dicho servicio requiere conexión a redes públicas. Con este fin, se recomienda que las comunicaciones se realicen a través de la Red SARA, que conecta las redes de las administraciones públicas españolas facilitando el intercambio seguro de información.
124. En los apartados que siguen se desarrollan aspectos especialmente significativos para la prestación de aplicaciones en modo servicios como los relativos a la confidencialidad y



protección de los datos, el control de acceso, la trazabilidad, la continuidad del servicio y la auditoría. No obstante, para poder profundizar más sobre estos aspectos véase la guía CCN-STIC 823 'Utilización de servicios en la nube'.

10.1. Confidencialidad y protección de datos

125. Al contratar el uso de una aplicación en modo servicio, los datos residen en sistemas tecnológicos que son gestionados por el proveedor del servicio. Por este motivo, la confidencialidad y protección de la información es uno de los aspectos más importantes para los suscriptores de estos servicios.
126. Las aplicaciones en modo servicio, implican un determinado nivel de confianza por parte de los suscriptores en la administración proveedora del servicio. Una de las preocupaciones habituales de los suscriptores es la seguridad de la información que se proporcionará o gestionará en la aplicación. En este sentido, es muy importante que el proveedor establezca los mecanismos de protección de la seguridad que velen por la confidencialidad, autenticidad, integridad, trazabilidad y disponibilidad de la información del sistema y que dichos niveles se ajusten a lo exigido por la normativa en vigor en cada momento y en función del tipo de datos y su grado de protección. Resulta imprescindible que los suscriptores conozcan estos mecanismos y que se determine con claridad: i) la posición que asume cada una de las partes en relación con los datos –responsable de fichero, encargado de tratamiento, etc.; ii) las responsabilidades asumidas por cada una de las partes, en coherencia con la posición, nivel de acceso a los datos y demás circunstancias; iii) la responsabilidad de cada una de las partes en los procesos relativos a la seguridad.
127. Es necesario que se defina en el documento de prestación del servicio el modelo de responsabilidades en relación con los datos a alojar en el servicio prestado y su manejo y/o tratamiento, a los efectos de seguridad de la información. Por ello, es recomendable acordar para todos los ficheros de carácter personal o con información sensible que se consideren como medios y servicios compartidos, quien va a ser el propietario de los mismos (responsable de fichero), lo cual determinará las obligaciones legales del suscriptor y el proveedor. Los temas más importantes que deberá incluir el modelo mencionado anteriormente son:
- Responsable de creación publicación y registro de los ficheros.
 - Quién debe aprobar la documentación normativa del sistema de gestión de la seguridad.
 - Deberes y obligaciones de las partes en cuanto a aplicación de medidas de seguridad de la información.
 - Tratamiento de las cesiones de datos, en su caso.
 - Documentos regulatorios de la adscripción al servicio que recojan esos deberes y obligaciones.



Habitualmente, el propietario de los datos y el responsable de los ficheros será el suscriptor del servicio correspondiendo al mismo las responsabilidades inherentes a su condición de propietario/responsable del fichero incluyendo las de publicación y registro de ficheros de carácter personal serán responsabilidad del suscriptor, tal como se ha venido comentando a lo largo del documento. Asimismo, el suscriptor tendrá la responsabilidad de definir la normativa del sistema de gestión de seguridad de los datos de los que es responsable. En

cuanto a los deberes y obligaciones de las partes, suele ser responsabilidad del proveedor la realización de las actuaciones necesarias para que el sistema permita la adecuada protección de los datos incorporados al mismo o necesarios para la prestación del servicio, al estar la misma íntimamente relacionada a la definición del servicio prestado. El proveedor deberá a su vez trasladar a socios y habilitadores la obligatoriedad del cumplimiento de las condiciones de seguridad que deban ser de su consideración.

10.1.1. Protección de la Información

128. Con carácter general, la legislación de protección de datos que resulta más relevante en la prestación de servicios en red es la siguiente:
- Protección de Datos de Carácter Personal, LOPD [Ley 15/1999] y su Reglamento de desarrollo [RD 1720/2007].
 - Legislación de cumplimiento obligatorio por Administraciones Públicas en el ámbito TIC [Ley 11/2007, Ley 40/2015] y los correspondientes reglamentos de desarrollo [RD 1671, RD 3/2010 ENS y RD 4/2010 ENI].
 - Legislación referente a Servicios de la Sociedad de la Información (LSSI) [Ley 56/2007].
129. No obstante, habrá que tener en cuenta que: i) la normativa en la materia de protección de datos se encuentra en constante evolución por lo que habrá de verificarse en cada caso la normativa en vigor en cada momento y cumplir con las obligaciones establecidas en la misma; ii) en función del tipo de servicio a prestar o datos deberá de tenerse en cuenta la existencia de legislación específica que podría resultar de aplicación y que deberá ser satisfecha y tomada en consideración por el proveedor del servicio.
130. Un escenario que puede presentarse en la prestación de aplicaciones en modo servicio es el de almacenamiento de datos sin tratamiento de los mismos. En estos casos, es altamente recomendable adoptar ciertas precauciones como el cifrado de los datos antes de salir del organismo del cliente, de forma que los requisitos de seguridad sobre el proveedor se reducen a la dimensión de disponibilidad o el establecimiento de cláusulas de confidencialidad. En este ejemplo, el cliente que consume el servicio será el único en poder de las claves de cifrado.
131. Las garantías de protección de datos deben ser también proporcionadas por otros agentes que actúan en la prestación del servicio, en cualquiera de las figuras de habilitador, intermediario o socio, en aquellos casos en que aplique.

10.1.2. Datos de carácter personal

132. El tratamiento de los datos de carácter personal debe ajustarse en todo caso a los principios y obligaciones establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, *de Protección de Datos de Carácter Personal*, su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre y a cualquier otra normativa que esté en vigor en cada momento y regule la materia.
133. Tal como se indica en la CCN-STIC 823 'Utilización de servicios en la nube', en su apartado 3 de Requisitos derivados de la existencia de datos de carácter personal, el suscriptor de la aplicación en modo servicio, normalmente, sigue siendo responsable del tratamiento de los datos de carácter personal, sin que esta responsabilidad se desplace al proveedor del

servicio, ni siquiera incorporando una cláusula con esta finalidad en el documento de formalización de la prestación del servicio. El artículo 16 del ENI no establece la obligación de celebrar un convenio para la reutilización de aplicaciones en el ámbito de las Administraciones Públicas. Debe valorarse en estos casos la necesidad de regular las obligaciones derivadas de la legislación sobre protección de datos para cumplir con las obligaciones establecidas por el artículo 12 de la LOPD mencionado a continuación.

134. En el caso en que el proveedor del servicio tenga acceso al tratamiento de los datos, debe comprometerse en el documento de formalización de la prestación del servicio a mantener la confidencialidad de la información del cliente, tal como se indica en el artículo 12 de la LOPD que establece que:

La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.

135. Además, el proveedor deberá asegurarse que los datos personales en tránsito estén cifrados, evitando que se realice la comunicación a través de entornos inseguros en los que puedan existir accesos no autorizados y conforme a lo establecido en la normativa aplicable. Los datos pueden ser recuperados mediante una pasarela de cifrado para su tratamiento en servidores seguros.
136. Por otra parte, si la prestación del servicio supone acceso por parte del proveedor a datos personales, el mismo, con carácter general, cumplirá el papel encargado del tratamiento. Como se indica en el artículo 12 de la LOPD, en el caso de que el encargado utilice los datos para otra finalidad que incumpla lo acordado en el documento de formalización de la prestación del servicio, será considerado también responsable del tratamiento, respondiendo a las infracciones en que hubiera incurrido personalmente.
137. Además de la LOPD, el prestador del servicio deberá cumplir los requisitos de protección de datos personales expuestos por el ENS y el RLOPD, proporcionando las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, garantizando un nivel de seguridad equivalente al correspondiente a los accesos en modo local, teniendo en cuenta la mayor o menor sensibilidad de los datos.
138. La gestión de soportes que puedan contener datos de carácter personal puede suponer un procedimiento de seguridad mucho más complejo de garantizar en la prestación de este tipo de servicios, por la deslocalización de los usuarios que puedan acceder a la información y la dificultad de controlar la creación de estos soportes. Por este motivo, la estrategia de protección de datos personales y limitación de creación de soportes de datos personales debe estar alineada con acciones de concienciación de los usuarios finales.
139. En aquellos casos en los que la prestación del servicio no suponga acceso a datos personales, no se aplicarán las normas y obligaciones establecidas en la LOPD y el RLOPD y serán, en su caso, las estipulaciones convencionales relativas a la confidencialidad de la información las que deberán atenderse. No obstante, conviene tener en cuenta que la interpretación que hace la LOPD de dato de carácter personal es bastante amplia, cubriendo cualquier dato que permita identificar a su titular sin un esfuerzo desproporcionado, así

como que con carácter general las personas jurídicas no están incluidas dentro del ámbito de aplicación de la LOPD.

140. Tal como se ha comentado al inicio de este apartado, el cliente que contrata aplicaciones en modo servicio con carácter general seguirá siendo el responsable de los datos personales, estando obligado a facilitar el ejercicio de los derechos ARCO (derecho de acceso, rectificación, cancelación y oposición sobre los datos de carácter personal) a los interesados en los plazos legales.
141. Para ello, es posible que se precise de la colaboración del prestador del servicio para proporcionar información actualizada. A tal efecto, el proveedor debe prever que puede existir esta necesidad y tendrá que tener disponibilidad para proporcionar información al respecto y, cuando se solicite, hacerla efectiva diligentemente.

10.1.3. Conservación de los datos

142. Durante la prestación del servicio, el proveedor debe garantizar la conservación de los datos mediante técnicas habituales de realización de copias de seguridad periódicas y dotando su infraestructura de los mayores niveles de seguridad física y lógica y en todo caso apta para garantizar el cumplimiento de los niveles de protección exigidos por la normativa aplicable. Además, se recomienda establecer procedimientos de recuperación y migración de datos que deben ser del conocimiento del cliente de cara a la futura devolución del servicio.
143. Al finalizar el acuerdo de prestación del servicio, los datos y copias de respaldo del proveedor deben ser destinados y tratados en los términos exigidos por la normativa aplicable en cada momento y a lo pactado (con carácter general los propios deberán de ser devueltos al responsable del tratamiento o destruidos, emitiéndose el correspondiente certificado, no obstante podrá pactarse la conservación de una copia bloqueada durante el plazo de prescripción de las acciones que pudieren ejercitarse). A sensu contrario no procederá la destrucción de los datos o su devolución en el caso en que exista una previsión legal que exija su conservación o se haya estipulado así en el documento de formalización de la prestación del servicio.
144. La obligación de destrucción o devolución de los datos está indicada en el artículo 22 del RD 1720/2007:

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento

145. Por otra parte, es importante tener en cuenta que hay casos en los que no se almacena en ningún momento la información del suscriptor en el sistema en red, como podría ser la plataforma de intermediación de datos y por lo tanto no aplicaría tampoco la conservación de los datos. Asimismo, podría darse el caso de que la información se conserve con carácter temporal, durante el proceso de intercambio y una vez confirmada la finalización del intercambio se procede a la eliminación de los datos almacenados.

10.1.4. Transferencias internacionales de datos

146. La localización de los datos es un elemento fundamental a tener en cuenta para garantizar la confidencialidad y protección de los datos. En este aspecto, es necesario tener en cuenta

que la ubicación geográfica de los datos puede suponer necesidades adicionales para garantizar que la información sea segura.

147. Si los datos del servicio proporcionado residen en cualquier otro país, hay que tener presente que la normativa del país donde se ubiquen puede influir jurídicamente en cuanto a la regulación del acceso y la protección de datos y habrá que conocer si existen entidades de inspección homologables a las españolas. En caso de que la autoridad del país en cuestión solicite datos personales, el cliente deberá ser informado por el prestador del servicio de esta circunstancia (salvo que lo prohíba la ley del país tercero).
148. Como mecanismo para asegurar la protección de datos en transferencias internacionales de datos, se podrá estudiar la posibilidad de obtener certificaciones estándares para prestadores de servicios en la nube, como es el caso de la norma ISO/IEC 27018. El objetivo de este tipo de certificaciones es permitir a proveedores de servicios un cumplimiento de las obligaciones establecidas en la normativa de protección de datos de carácter personal, ofreciendo transparencia al suscriptor sobre dónde, cuándo y quién ha almacenado o procesado sus datos personales y en qué condiciones se ha producido, incorporando las garantías contractuales adecuadas y, de manera especial, estar a disposición de poder acreditar que se dispone de certificados de seguridad adecuados y auditables por un tercero independiente.
149. En aquellos escenarios en los que se produzca transferencia internacional de datos personales, se considera una garantía adecuada que el país de destino ofrezca un nivel de protección equivalente al 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 hacer constar la transferencia a la Agencia Española de Protección de Datos para su inscripción en el Registro General de Protección de Datos.
150. En relación con las entidades que ofrecen garantías adecuadas para la protección de datos (Puerto Seguro), téngase en cuenta que el Tribunal de Justicia de la Unión Europea declaró inválida la Decisión de la Comisión 2000/520/CE que establece el nivel adecuado de protección de las garantías para las transferencias internacionales de datos a EE.UU. ofrecidas por el acuerdo de Puerto Seguro publicado por su Departamento de Estado; y que la Comisión Europea y los EE.UU. han anunciado, el 2 de febrero de 2016, un acuerdo de un nuevo marco para la transferencia internacional de datos que se deberá desarrollarse próximamente. En cualquier caso, téngase presente la información más actualizada que pueda aportar la Agencia de Protección de Datos en materia de transferencias internacionales de datos.

10.2. Control de Acceso

151. En la prestación de aplicaciones en modo servicio, se deberá ser especialmente riguroso aplicando el control de los derechos de acceso a usuarios (mínimo privilegio, necesidad de conocer y capacidad de autorizar). Es importante tener especial cuidado en controlar estos accesos por parte del personal del proveedor a los datos del suscriptor.
152. El proveedor de una aplicación en modo servicio deberá asegurar el cumplimiento de los requisitos de control de acceso establecidos en el Anexo II del ENS a medidas de seguridad:

- | |
|---|
| <ol style="list-style-type: none">a) Que todo acceso esté prohibido, salvo concesión expresab) Que la entidad quede identificada singularmente |
|---|

- c) Que la utilización de recursos esté protegida
- d) Que se definan para cada usuario o entidad del servicio los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización
- e) Serán diferentes las personas que autorizan, usan y controlan el uso
- f) Que la identidad de la entidad quede suficientemente autenticada
- g) Que se controle tanto el acceso local como el acceso remoto cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento

153. El proveedor del servicio además de asegurar el control de accesos deberá de asegurarse de que los trabajadores del mismo respeten las obligaciones que en materia de seguridad y confidencialidad se establezcan.
154. Dependiendo del nivel de seguridad que haya determinado el proveedor para el servicio prestado, el sistema de control de acceso que se implante podrá primar la comodidad de uso sobre la protección de la información (servicios de nivel de seguridad bajo) o viceversa, si se trata de servicios que requieran seguridad crítica.
155. Por otra parte, debido a la naturaleza de las aplicaciones en modo servicio, es habitual que el servicio se interconecte con otros sistemas del suscriptor o de cualquiera de los otros roles participantes, dándose el caso en que los sistemas de identificación, autenticación y autorización tengan lugar en diferentes dominios y bajo distintas responsabilidades. Si este es el caso, se recomienda establecer acuerdos de colaboración entre las partes para homogeneizar los procedimientos que permitan controlar aspectos como la identificación de los accesos, requisitos de acceso en el servicio y el resto de sistemas integrados, proceso de gestión de derechos de acceso, mecanismos aceptados de autenticación y políticas de acceso local y remoto.

10.3. Trazabilidad

156. El proveedor de aplicaciones en modo servicio deberá disponer de registros de acceso que permitan monitorizar, analizar, investigar y documentar acciones no autorizadas, tanto a nivel operativo como de administración, en aquellos casos en los que esta última tarea esté delegada en el proveedor. Disponiendo de medidas de trazabilidad del sistema, el prestador podrá dar cumplimiento a las obligaciones legales del ENS y el RD 1720/2007 en su artículo 103 de Registro de accesos, en caso de que se trate de datos de carácter personal.
157. Para poder realizar un correcto registro de actividad sobre el servicio, el documento de formalización de la prestación del servicio debe especificar las obligaciones del proveedor, teniendo especial cuidado a los plazos de retención de los registros, teniendo en cuenta la naturaleza de la información de los servicios y políticas acordadas con el suscriptor.
158. Las responsabilidades del proveedor en relación con el registro de actividad estarán íntimamente ligadas al modelo de administración implementado. Si el servicio es delegado en el suscriptor, el proveedor del servicio tendrá responsabilidad limitada en cuanto a la trazabilidad de las operaciones sobre los datos. En cualquier caso, en el documento de

acuerdo de prestación del servicio tendrán que estar claramente definidos los datos sobre los que el proveedor debe mantener una trazabilidad y los plazos para entregar esta información al suscriptor en caso de que sea demandada por el mismo. Es importante tener en cuenta que podrían contemplarse modelos de registro de acceso compartidos, en los que los accesos a información sensible pueden ser hospedados y custodiados en los sistemas del suscriptor, mientras que el registro rutinario de operación de los sistemas puede quedar como responsabilidad del proveedor.

10.4. Continuidad del Servicio

159. Otro de los aspectos que el proveedor debe tener en cuenta en su modelo de seguridad es la necesidad de continuidad del servicio. Para determinados servicios, podría requerirse garantizar la continuidad del servicio en caso de catástrofe o incidente grave, por lo que el proveedor debería cumplir con los requisitos previstos en el Anexo II del ENS, relativos a la continuidad del servicio y medios alternativos, considerando además los siguientes aspectos en función del nivel de disponibilidad requerido:
- Existencia del plan de continuidad de negocio, definiendo un procedimiento de coordinación ante incidencias y desastres que puedan afectar al servicio, contemplando los flujos de información y las interacciones entre cliente y proveedor.
 - Evidencia satisfactoria de la ejecución periódica de pruebas de continuidad.
 - Análisis de impacto del servicio proporcionado, alineado con los criterios definidos en los Acuerdos de Nivel de Servicio.
160. Por último, en caso de que el servicio prestado sea realmente crítico para los suscriptores, se podría considerar realizar pruebas periódicas que involucren al suscriptor y a otros participantes en la prestación del servicio (habilitantes, socios, intermediarios), con el fin de validar el correcto funcionamiento de los planes y el cumplimiento de los plazos y servicios mínimos previstos.

10.5. Auditoría

161. El suscriptor, en su condición de responsable de los datos, deberá disponer de un determinado nivel de control sobre el servicio que trata estos datos. Con este fin, es habitual que disponga del derecho de auditoría, con la profundidad correspondiente, sobre el proveedor de servicios o solicite a éste la siguiente documentación:
- Declaración de aplicabilidad de las medidas de seguridad acordadas en el documento de formalización de la prestación del servicio.
 - Auditoría que evidencia el cumplimiento de las medidas de seguridad del Anexo II del ENS y que estén acordes con el nivel del sistema, o las que se determine según las particularidades del servicio.
 - Auditorías de cumplimiento de normativa, por ejemplo: LOPD, SAS70, PCI-DSS, etc.
162. En definitiva, el cliente podrá requerir al proveedor que cumpla los principios y los requisitos mínimos establecidos por el ENS. El prestador del servicio 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.

11. EVOLUCIÓN DEL SERVICIO

163. La evolución de las aplicaciones en modo servicio es un aspecto a tener en cuenta en el modelo de prestación de este tipo de servicios de cara a no incurrir en sobrecostes y optimizar el aprovechamiento de los recursos que se comparten en red.
164. Las previsiones de evolución de un servicio por lo general será una decisión del proveedor del servicio y resulta recomendable tener una planificación de evolución del servicio que será comunicada a los suscriptores del servicio de cara a coordinar esfuerzos de nuevos desarrollos, incorporación de nuevos colectivos al servicio y cualquier otra acción que pueda estar condicionada por la publicación de nuevos cambios en el servicio ofrecido.

11.1. Hoja de ruta de evolución de la aplicación en modo servicio

165. En aplicaciones en modo servicio, las solicitudes de cambio pueden provenir de distintos suscriptores con necesidades y negocios diversos, que en muchos casos pueden solaparse o incluso no estar alineadas. Por este motivo, es importante realizar un análisis de las solicitudes de cambio recibidas (RFC) para decidir qué cambios pueden ser implementados en función de una serie de criterios.
166. Siguiendo la filosofía del estándar ITIL, es recomendable que el análisis de estas peticiones de cambio y su viabilidad sea realizado internamente por el proveedor, a través de un Comité de Cambios que pueden ser formalizado o no y que podrá apoyarse en socios y habilitadores del servicio. A continuación se muestra el modelo propuesto para evolución de este tipo de servicios:

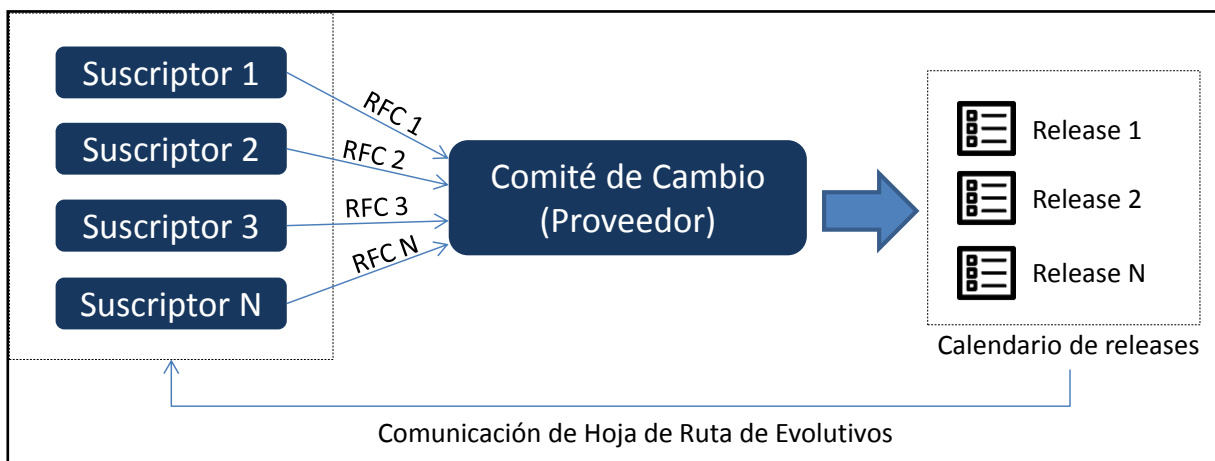


Figura 8. Procedimiento de gestión de cambios

167. Los suscriptores envían sus solicitudes de cambio al proveedor que las centraliza en un comité de cambios interno. En este comité se evaluarán y priorizarán las peticiones siguiendo distintos criterios, como pueden ser:
- Costes de implementación del cambio.
 - Demanda del cambio por parte de otros suscriptores.
 - Visión estratégica del servicio.
 - Viabilidad técnica y funcional.

168. El análisis de cambios realizado por el comité resultará en la aceptación o no de cada una de las solicitudes recibidas. Los cambios aceptados se priorizarán según los criterios comentados anteriormente y se podrán agrupar en *releases*, cuya implementación podrá ser planificada en un calendario u hoja de ruta de evolutivos.
169. Es recomendable la comunicación de esta hoja de ruta a los distintos suscriptores, de cara a que puedan conocer los cambios que finalmente se abordarán y las fechas estimativas de su liberación.

12. CONTRAPRESTACIÓN ECONÓMICA

170. La prestación de aplicaciones en modo servicio en la administración pública puede suponer o no una contraprestación por parte del organismo que consume los servicios. En cualquier caso la posible contraprestación económica asociada será únicamente a efectos de repercutir el coste de la administración del servicio y nunca con fines de lucro.
171. En el sector privado existen distintos modelos de contraprestación que pueden ser adaptados al sector público. Entre estos modelos, los que pueden tener mayor aplicación al son el pago por consumo, pudiéndose articular mediante el cobro de un importe fijo hasta un límite y coste unitario por exceso y el pago por suscripción.



12.1. Modelo de costes

172. Para poder repercutir los costes de las aplicaciones en modo servicio, se recomienda que el prestador del servicio disponga de un modelo de imputación de costes TI al servicio que permita cuantificar de forma más o menos precisa los costes totales incurridos en la prestación del servicio.
173. Para ello y en primer lugar, el proveedor del servicio deberá proceder a la identificación de las principales partidas de gasto e inversiones y caracterizarlas de acuerdo a las posibilidades y limitaciones de reparto del coste. (Fijos vs Variables, directos; indirectos, posibilidades de distribución,...).
174. Esta caracterización de los costes permitirá cuantificar de forma aproximada el coste del servicio. Para una cuantificación más precisa, se recomienda establecer un Modelo de costes en el que se establezca el modelo de imputación y reparto de los mismos al servicio en cuestión.

12.2. Modelos de contraprestación

175. A partir del modelo de costes definido, se podrán proponer distintos tipos de contraprestación para alinearlos con la tipología de los costes del servicio. Por ejemplo, si en el servicio prestado predominan los costes fijos, el modelo más adecuado para su repercusión es de pago por suscripción (tarifa plana), mientras que en servicios con más costes variables resultará conveniente aplicar el pago por consumo. A continuación se desarrollan en más detalle ambas contraprestaciones:
- i. **Pago por consumo:** este es el modelo por excelencia de los servicios en la nube ya que se deriva del concepto de escalabilidad, en el que el coste del servicio asociado se modifica en función de las necesidades puntuales de uso de la solución. Las métricas más utilizadas para establecer el consumo son:
 - Número de usuarios
 - Número de usuarios concurrentes
 - Número de operaciones procesadas (nominas, documentos almacenados, etc.)
 - Volumen de almacenamiento

En algunos casos es posible variar el modelo aplicando un importe fijo hasta un límite de consumo y un coste unitario o por tramo por recurso adicional consumido.

Asimismo, dentro del pago por consumo se pueden establecer distintos precios dependiendo de las funcionalidades utilizadas por el suscriptor.

- ii. **Pago por Suscripción:** el cliente paga por utilizar el servicio durante un periodo de tiempo, por lo general mensual. Por lo general este modelo permite el uso ilimitado durante el tiempo de vigencia de la suscripción permitiendo al cliente pagar el mismo importe independientemente de los recursos que se consuman.
176. En todo caso los mecanismos de pago deben de permitir acreditar que las cantidades recibidas en concepto de pago no superan los costes soportados².
177. Con independencia del modelo de contraprestación seleccionado, el prestador del servicio deberá acordar la forma de facturación y pago: periodo de facturación y plazo de pago fundamentalmente.

12.3. Penalizaciones


178. Las penalizaciones a aplicar pueden afectar tanto al cliente como al prestador del servicio y, en su caso, deberán estar formalizadas por las partes.
179. Las penalizaciones sobre el prestador del servicio se aplicarán con carácter general por incumplimiento de los acuerdos de nivel de servicio definidos en el apartado 5.1 del documento. Algunas causas comunes de penalizaciones que podrían afectar a la administración prestadora del servicio son:
- i. Retrasos en la resolución de incidencias.
 - ii. Reclamaciones por disconformidad en la calidad del soporte a usuarios.
 - iii. Indisponibilidad del servicio o alguno de sus módulos durante el horario de prestación.
 - iv. Retrasos en gestión de usuarios (alta, baja, modificación).
180. El cálculo de posibles penalizaciones se realiza de forma periódica, por lo general mensualmente y antes de la facturación del período en cuestión. Se debe acordar entre el prestador y el cliente quién realizará la medición de los indicadores y calculará las penalizaciones, pudiéndose delegar esta tarea a un auditor si se considera oportuno.
181. Por otro lado, las penalizaciones también se pueden aplicar al cliente por diversos motivos entre los que destacan
- i. Incumplimiento de cualquiera de los términos de capacidad acordados (número de usuarios, transacciones, documentos, etc.).
 - ii. Solicitud de finalización anticipada del servicio.
 - iii. Uso inadecuado de la plataforma (pruebas en entornos productivos o sin aviso previo, inclusión de código o archivos maliciosos, etc.).
 - iv. Cualquier otra obligación que se establezca para el servicio.
182. En cuanto a las posibles penalizaciones a aplicar sobre el cliente, es necesario acordar, al inicio del documento de derechos y obligaciones de las partes, si dichas penalizaciones supondrán acciones sobre la prestación del servicio, por ejemplo un corte del servicio, o se traducirán en un sobrecoste en la facturación periódica.

² Sólo en el caso de que la prestación de servicios se configurase como un auténtico contrato de servicios podría plantearse la posibilidad de que la remuneración excediera los costes.

13. FINALIZACIÓN DEL SERVICIO

183. La finalización del servicio deberá estar recogida expresamente en el documento que regule el servicio con independencia de la fórmula jurídica seleccionada. Para ello, se deberá contemplar:
- La duración del servicio y, por tanto, la finalización planificada del mismo.
 - La posibilidad de finalización anticipada del servicio por deseo de cualquiera de las partes.

13.1. Finalización por fin del acuerdo de prestación

184. La finalización del servicio por fin del período formalizado de prestación de servicio, supone poner en marcha los procedimientos pautados antes del inicio del servicio de cara a transferir el conocimiento y los datos relacionados con el servicio. Para ello, se recomienda que el proveedor del servicio presente y valide un plan de retorno del servicio en el que se recojan, entre otros, los aspectos siguientes:
- i. Planificación e hitos de devolución.
 - ii. Procedimientos y documentación para el traspaso del conocimiento.
 - iii. Cualquier otro aspecto que se considere relevante para un proceso de traspaso del servicio.
185. Habitualmente se establece un periodo de transición que permita ordenar la finalización del servicio y permitir al suscriptor la transición al nuevo escenario de servicio. Entre las actividades a realizar durante dicho periodo destaca la migración de los usuarios y de la información que podrá ser parcial con los datos vivos o total incluyendo el histórico.
186. La portabilidad de los datos es un aspecto clave en la devolución del servicio. Independientemente del formato en que se traten los datos por parte del proveedor, se recomienda cerrar con el suscriptor el formato y mecanismo en el que se hará entrega de los datos devueltos durante la fase de finalización.
- 
187. Adicionalmente, se podrán establecer 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.
188. Finalmente, podrán incluirse en las cláusulas mecanismos para garantizar la destrucción efectiva de los datos, por ejemplo a través de auditorías.

13.2. Finalización anticipada del acuerdo de servicio

189. Existe la posibilidad de que el acuerdo de prestación del servicio finalice antes del período acordado. Esta finalización puede tener distintos motivos.
- i. Que el suscriptor considere inadecuado el servicio recibido.
 - ii. Modificación unilateral de las condiciones del servicio por parte del proveedor.

- iii. Fin de la prestación de este tipo de servicio por parte del proveedor o de intermediarios cuya fuerte dependencia tecnológica suponga la necesidad de una parada prolongada del servicio.
 - iv. Fin de la necesidad del consumo del servicio por parte del suscriptor.
190. Habitualmente este tipo de finalización suele llevar aparejada una penalización económica para compensar a la contraparte de los perjuicios ocasionados.
191. Se recomienda en este sentido disponer de un plan de retorno del servicio de forma anticipada en se aborden todos los aspectos de devolución del servicio supuestos en una finalización regular del mismo, teniendo en cuenta la reversibilidad y portabilidad.

14. REFERENCIAS

14.1. Legislación

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
[BOE-A-2015-10566](#)
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
[BOE-A-2015-10565](#)
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
[BOE-A-1999-23750](#)
- 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-A-2008-979](#)
- 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-A-2010-1330](#)
- 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-A-2010-1331](#)

14.2. Estándares y buenas prácticas

- Guía/Norma seguridad de las TIC (CNN-STIC-823). Esquema Nacional de Seguridad. Diciembre 2014. Utilización de Servicios en la Nube
<https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud/file.html>

14.3. Documentos de trabajo y referencias

- Orientaciones para prestadores de servicios de Cloud Computing. Agencia española de protección de datos. 2013
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/ORIENTACIONES_Cloud.pdf
- Guía para clientes que contraten servicios de Cloud Computing. Agencia española de protección de datos. 2013

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

- Estudio sobre el *cloud computing* en el sector público en España. Instituto Nacional de Tecnologías de la Comunicación. 2012

<https://www.incibe.es/file/a6Cywl9gxru5f1Ez5MwRMA>

- Cloud Computing Retos y Oportunidades. ONTSI. 2012

http://www.ontsi.red.es/ontsi/sites/default/files/1_estudio_cloud_computing_retos_y_oportunidades_vdef.pdf

ANEXO I. CHECK LIST APLICACIONES EN MODO SERVICIO

1. Acordar la forma jurídica para la prestación del servicio
2. Definir el servicio a prestar y su alcance
3. Condiciones de prestación del servicio.
 - a. Indicadores y acuerdos de nivel de servicio (ANS)
 - b. Horario de prestación
4. Definir el modelo y alcance de soporte
 - a. Niveles de soporte que ha de proveer el suscriptor
 - b. Niveles de soporte del proveedor
 - c. Procedimientos y herramientas de Gestión del Servicio: OPCIONAL
 - d. Canales de Soporte
5. Definir estrategia de formación: OPCIONAL
6. Acordar políticas de confidencialidad, protección de datos y seguridad
7. Procedimiento de evolución y Gestión de la demanda: OPCIONAL
8. Modelo de Contraprestación económica del servicio³
9. Establecer condiciones de finalización del servicio

³ En caso de que no se aplique un modelo de contraprestación económica, será necesario incorporar en el acuerdo de prestación del servicio una cláusula en la que se explicita la no contraprestación del servicio.

ANEXO II. EQUIPO RESPONSABLE DEL PROYECTO

Coordinador del proyecto

Amutio Gómez, Miguel A.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Responsable de edición

Alcaide García, Aleida

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Grupo de expertos:

Administración General del Estado

Agurruza Mutuberría, Jokin

Alburquerque Pernías, Francisco

Alberto Martín, Félix

Alcaide García, Aleida

Alcolea Muñoz, Antonio

de Alfonso López, Ricardo

de Amil Villarrubia, Pablo

Amores Molero, Felipe

Aragonés Arribas, Félix Jesús

Arranz, Candelas

Ballesteros Arjona, Juan Jesús

Barba Lobatón, Jesús

Barrón Basterrechea, José Luis

Beltrán, Ana

Berral López Alfonso

Blanco Arribas, Miguel Ángel

Bustos Pretel, Gerardo

Cabezas Manso, Laura

Candau, Javier

Caruana De las Cagigas, Elisa

Del Caño Gil, Cristina

Casado Robledo, M^a Jesús

Cívicos Villa, Noemí

Conejo Fernández, Carmen

Corral Guinea, Myriam

Crespo Sánchez, Juan

Criado Gómez, Isabel

Cubo Contreras, Aitor

Cueva Calabia, José Luis

Desantes Fernández, Blanca

De la Calle Vian, Elena

Delgado Casanova, Ricardo

De Miguel de Santos, María

Díez Pérez, Esther

Eguíluz Gauna, Jesús

Escapa Castro, Lucía

Eusamio Mazagatos, José Antonio

Fernández Crespo, María Esther

Fernández Lombardía, Oscar

Fradua García-Soto, Idoia

Fuentes Bajo, Ricardo

Franco Espino, Beatriz

Galindo Alonso, Olga

Gamarra, Juan Carlos

Garcés, Juan Carlos

García Celada, Joseba

García Gómez, Eugenio

García Martín, M^a Jesús

García Martínez, José Luis

Gijón Romero, Francisco

Gil Navalón, Roberto

Gómez Muñoz, Carlos Francisco

Gómez Plaza, Carlos

INSTITUTO NACIONAL DE ESTADÍSTICA

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL DE LA POLICÍA

MINISTERIO DE JUSTICIA

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

FÁBRICA NACIONAL DE MONEDA Y TIMBRE

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA

MINISTERIO DE FOMENTO

MINISTERIO DE JUSTICIA

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL DE TRÁFICO

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CENTRO CRIPTOLÓGICO NACIONAL

MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE LA PRESIDENCIA

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DEL INTERIOR – DIRECCIÓN GENERAL DE LA POLICIA

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

MINISTERIO DE LA PRESIDENCIA

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DEL INTERIOR - DIRECCIÓN GENERAL DE LA POLICÍA

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

MINISTERIO DE AGRICULTURA, ALIMENTACIÓN Y MEDIO AMBIENTE

MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

GERENCIA DE INFORMÁTICA Y SEGURIDAD SOCIAL

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

CONSEJO GENERAL DEL PODEL JUDICIAL

MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL - SEPE

MINISTERIO DE INDUSTRIA, ENERGIA Y TURISMO

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE FOMENTO

MINISTERIO DE DEFENSA

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

Gómez Raya, José Ignacio
Gómez Vaz, Manuel
González Rufo, M^a Ángeles
Gonzalo Ramírez, Alberto
Graña Domínguez, Santiago
Hernández Vicente, Severiano
Hernández Gallardo, Diego
Hernández Jiménez, Francisco
Hernández Maroto, M^a Dolores
Hernández Vigliano, Julián
Herrero García, Carlos
Horganero Gómez, Sara
Hortigüela Hortigüela, Concha
Iniesta Sánchez, Fernando
Jaqueti, Francisco Javier
Jara González, Francisco José
Jiménez Muñoz, Luis
Lago Bagues, Ramiro José
Lapuente Perea, José Luis
López Crespo, Francisco
López Herrero, Miguel Ángel
Lorenzo Fernández, Laura
Lucas Vegas, M^a José
Llorens González, Juan de Dios
Mañes Guerras, Santos
Martín García, Raúl
Martín Lázaro, Francisco José
Martín Marcos, Miguel
Martín Rey, Rosa M^a
Martínez Muñoz, David
Martínez Vidal, Miguel Ángel
Maza Frechín, Carlos
Merchán Arribas, Montaña
De Miguel Santiago, María Luz
Millaruelo Gómez, Alejandro
Molina Moscoso, Domingo
Montes Antona, Javier
Muñoz Montalvo, Juan Fernando
Muñoz Salinero, Elena
Ochando Perales, Javier
Ortiz Tovar, Eva María
Otheo de Tejada, Josefina
De la Paz Rincón, Antonio
Pardo, Jesús
Pastor Bermúdez, Andrés
Pérez Alcázar, Ricard
Pérez Galindo, Rafael
Pérez de Lema Sáenz de Viguera, Andoni
Rada Muruaga, Begoña
Ramos Curto, Juan Francisco
Requejo Zalama, Javier
Rincón Mirón, Jorge Antonio
del Río Molini, Mario
Robledo Pascual, Óscar
Rodríguez Hervás, Francisco Javier
Rodríguez Escolar, Nimia
Rodríguez Ramos, Miguel Ángel
Román Cortés, Juan Carlos
Rubio Martínez, Javier
Ruiz del Corral, Manuel
Ruiz de Garibay Cubillo, Andrea
Salom, Juan
San Atanasio, Pinar
Sánchez Abad, M^a Pilar
Sánchez Agulló, Pablo
Sanz Pulido, Antonio

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE FOMENTO
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL - SEPE
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
FÁBRICA NACIONAL DE MONEDA Y TIMBRE
INSTITUTO NACIONAL DE ESTADÍSTICA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE LA PRESIDENCIA
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL - GISS
MINISTERIO DE LA PRESIDENCIA
INSTITUTO NACIONAL DE ESTADÍSTICA
MINISTERIO DEL INTERIOR – DIRECCIÓN GENERAL DE LA POLICIA
CENTRO CRIPTOLÓGICO NACIONAL
MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN
MINISTERIO DE FOMENTO
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL - SEPE
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE DEFENSA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN
INSTITUTO NACIONAL DE ESTADÍSTICA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE AGRICULTURA, ALIMENTACIÓN Y MEDIO AMBIENTE
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
FÁBRICA NACIONAL DE MONEDA Y TIMBRE
MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE DEFENSA
MINISTERIO DE JUSTICIA
AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
FÁBRICA NACIONAL DE MONEDA Y TIMBRE
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL - GISS
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
MINISTERIO DE DEFENSA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DEL INTERIOR
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE INDUSTRIA, ENERGIA Y TURISMO
AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA
GUARDIA CIVIL
AGENCIA ESTATAL DE METEOROLOGÍA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

Sobrino Moreno, José María
Tapias Sancho, Álvaro
Triguero Garrido, Mario
Valcárcel Lucas, Pedro-Castor
Vallejo Echevarría, Maite
Vega Fidalgo, Luis Miguel
Vélez Fraga, Santiago
Villafranca Ramos, Alberto
Viñado Villuendas, Pilar
Villalba Tomás
Zapardiel, Juan Antonio
Zapico, Alberto

Comunidades Autónomas

Andrés Sevillano, Albert
Báez Rodríguez, Luis Alberto
Barras, Juan Antonio
Del Barrio Morón, Antonio
Berjano Tartiere, Bárbara
Cantabrana González, Ricardo
Cañal Villanueva, M^a José
Castellano, Enrique
Cortés Domingo, Rubén
Chapado Gregorio, Susana
Esparza Ruiz, Catalina
Fernández Requejo, Antonio
Font Bibiloni, Andreu
Galán Huertos, Pilar
Gallego Español, Rosa María
Garay, Raquel
García Carrera, Diego
García Sexto, María José
González Rodríguez, Manuel de los Reyes
Izco García, Fernando
López González, M^a del Rosario
Lozano Cantín, M^a Ángel
Marín Cruz, Pepa
Martínez Pelayo, Paula
Moreno, Ángel
Ojeda Pérez, Juan Sebastián
Olivares Sánchez, Pedro
Perera Domínguez, Manuel
Rodríguez Parraga, José María
Rodríguez Rodríguez, Juan Carlos
Rosat Jorge, José Luis
Ruíz Benítez, M^a del Carmen
Sánchez Melero, Arturo
Saro, Javier
Sáez de Vicuña, Asier
Zorita Pacheco, Antonio

Corporaciones Locales

Bárceñas Gutiérrez, Pablo

Universidades

Sánchez Martínez, Daniel

Otras Instituciones

de Ocaña Lacal, Daniel

Medio Propio – Red.es

Polo Sanz, Pilar

De la Barreda Manso, Ana

Apoyo - PriceWaterhouseCoopers

Bautista Ortega, Luis María

Morales Ríos, Christian

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
MINISTERIO DE JUSTICIA
GERENCIA DE INFORMÁTICA DE LA SEGURIDAD SOCIAL
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DE LA PRESIDENCIA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
MINISTERIO DEL INTERIOR
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS
AGENCIA ESTATAL DE LA ADMINISTRACIÓN TRIBUTARIA

ARAGÓN
CANARIAS
CASTILLA Y LEÓN
CASTILLA-LA MANCHA
ASTURIAS
ARAGÓN
CASTILLA Y LEÓN
CANARIAS
CATALUÑA
COMUNITAT VALENCIANA
REGIÓN DE MURCIA
EXTREMADURA
ILLES BALEARS
CASTILLA Y LEÓN
CATALUÑA
PAÍS VASCO
CASTILLA Y LEÓN
JUNTA DE GALICIA
CANARIAS
NAVARRA
ASTURIAS
ARAGÓN
COMUNIDAD DE MADRID
ASTURIAS
LA RIOJA
ANDALUCIA
REGIÓN DE MURCIA
ANDALUCIA
CASTILLA Y LEÓN
PRINCIPADO DE ASTURIAS
CASTILLA Y LEÓN
CANARIAS
COMUNIDAD DE MADRID
CANTABRIA
PAÍS VASCO
EXTREMADURA

FEDERACIÓN ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

CONFERENCIA DE RECTORES DE LAS UNIVERSIDADES ESPAÑOLAS

TRIBUNAL CONSTITUCIONAL