III. OTRAS DISPOSICIONES

MINISTERIO DE LA PRESIDENCIA

17147 *Resolución de 15 de octubre de 2010, de la Secretaría de Estado para la Función Pública, por la que se publica el Acuerdo de colaboración con el Tribunal Constitucional para la prestación mutua de servicios de administración electrónica.*

La Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos establece, entre sus principios generales, el de cooperación en la utilización de medios electrónicos por las Administraciones Públicas al objeto de garantizar la interoperabilidad de los sistemas y soluciones adoptados por cada una de ellas así como, en su caso, la prestación conjunta de servicios a los ciudadanos. Este principio es igualmente aplicable a la cooperación entre las Administraciones y otros poderes públicos.

En aplicación de este principio de cooperación interadministrativa, diversos preceptos de la Ley especifican los aspectos en que dicho principio puede manifestarse en las materias objeto de regulación por la Ley, cerrándose ésta con un título dedicado a la cooperación entre administraciones para el impulso de la administración electrónica, lo que constituye una prueba de la importancia de la cooperación para implantar la administración electrónica al servicio del ciudadano y coadyuvar al desarrollo de la sociedad de la información.

Con fecha 17 de septiembre de 2010 se formalizó un Acuerdo de colaboración entre el Ministerio de la Presidencia y el Tribunal Constitucional para la prestación mutua de servicios de administración electrónica, en el que se establecen los términos y condiciones para un aprovechamiento común de los servicios electrónicos que prestan ambas partes.

Mediante este Acuerdo, ambas partes impulsarán la prestación de servicios en línea al ciudadano que permita la interoperabilidad de los servicios, trámites y procedimientos. En este sentido, en sus respectivos ámbitos de competencia, consideran necesario promover la coordinación de los proyectos de administración electrónica, tomando como objetivo conseguir la máxima utilidad de los mismos a través de la utilización de servicios.

En concreto, podrán acceder recíprocamente a las funcionalidades de los servicios proporcionados por la conexión a la red SARA (sistemas, aplicaciones y redes para las administraciones), que facilita el intercambio seguro de información, a través de un enlace común para todas las necesidades de intercomunicación. Asimismo, el Tribunal Constitucional podrá acceder a los servicios ofrecidos por el Ministerio de la Presidencia para la verificación por vía electrónica de los datos de identidad y residencia de los ciudadanos que expresamente lo autoricen, a fin de evitar que tengan que aportar la fotocopia de documentos de identidad o el certificado de empadronamiento como documento probatorio del domicilio y residencia cuando dichos documentos obran en poder de las administraciones.

Igualmente, el Tribunal Constitucional podrá disponer del servicio prestado por el Ministerio de la Presidencia a través de la plataforma de validación y firma electrónica @firma para la identificación, validación o generación de firma electrónica por medio de certificados digitales, y del servicio que facilita la práctica de notificaciones telemáticas seguras mediante la utilización de la dirección electrónica habilitada.

Debe destacarse que el intercambio de estos servicios no comporta obligaciones económicas para ninguna de las partes firmantes del Convenio.

En cumplimiento de lo dispuesto en el artículo 8.2 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, esta Secretaría de Estado para la Función Pública dispone su publicación en el «Boletín Oficial del Estado».

Madrid, 15 de octubre de 2010.–La Secretaria de Estado para la Función Pública, Consuelo Rumí Ibáñez.

cve: BOE-A-2010-17147

ANEXO

Acuerdo de colaboración entre el Ministerio de la Presidencia y el Tribunal Constitucional para la prestación mutua de servicios de administración electrónica

En Madrid, a 17 de septiembre de 2010,

REUNIDOS

De una parte, doña María Emilia Casas Baamonde, Presidenta del Tribunal Constitucional, nombrada por Real Decreto 1470/2004, de 15 de junio (BOE de 16 de junio), en ejercicio de las facultades que le atribuye el artículo 15 de la Ley Orgánica del Tribunal Constitucional, 2/1979, de 3 de octubre (BOE de 5 de octubre).

De otra parte, doña María Teresa Fernández de la Vega, en su calidad de Ministra de la Presidencia, y en representación del Departamento, en el ejercicio de las competencias que le confiere el artículo 13.3 de la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado.

Ambas partes se reconocen la capacidad jurídica necesaria para suscribir el presente Acuerdo y en su virtud

EXPONEN

1.º Que tanto el Ministerio de la Presidencia (MPR) como el Tribunal Constitucional tienen entre sus funciones, el ofrecimiento de unos servicios de interés a los ciudadanos, la búsqueda de la eficiencia en el uso de los recursos públicos y la simplificación en la tramitación administrativa y jurisdiccional.

2.º Que asimismo, tienen entre sus cometidos la aplicación de las tecnologías de la información para el impulso, desarrollo e implantación de servicios electrónicos en línea, con objeto de hacer realidad la administración electrónica en beneficio de los ciudadanos.

3.º Que las partes están de acuerdo en impulsar la prestación de servicios en línea al ciudadano que permita la interoperabilidad de los servicios, trámites y procedimientos. En este sentido, los firmantes, en sus ámbitos de competencia, consideran necesario promover la coordinación de los proyectos de administración electrónica, tomando como objetivo conseguir la máxima utilidad de los mismos a través de la utilización de servicios puestos a disposición por las partes, buscando así la satisfacción de necesidades de las Administraciones y otros poderes públicos y el interés público.

4.º Que para lograr una mayor eficacia en la consecución de estos fines y conforme a los principios de cooperación y coordinación en la actuación entre los poderes públicos, el presente acuerdo resulta de especial utilidad para las dos instituciones.

Por todo ello, las partes firmantes suscriben este Acuerdo de colaboración con arreglo a las siguientes

CLÁUSULAS

Primera. *Objeto.*–El presente Acuerdo tiene por objeto establecer los términos y condiciones generales para un aprovechamiento común de los servicios electrónicos que prestan las partes firmantes.

Esto se traduce en la disponibilidad de determinados servicios facilitando el acceso y uso común de servicios prestados por cualquiera de las partes. Dicha prestación de servicios se llevará a cabo en los términos que establece el presente Acuerdo y en las cláusulas particulares recogidas en el anexo que le sea de aplicación a cada servicio.

Segunda. *Ámbito de aplicación.*–Las partes que suscriben el presente Acuerdo podrán acceder a las funcionalidades proporcionadas por los servicios relacionados en los anexos al presente Acuerdo que a continuación se especifican:

1. Conexión a la Red SARA.
2. Servicios ofrecidos por el Ministerio de la Presidencia para la verificación de datos de identidad y de residencia de un ciudadano (SVDI, SVDR).

cve: BOE-A-2010-17147

3. Servicios ofrecidos por el Ministerio de la Presidencia a través de la plataforma de validación y firma electrónica @firma.

4. Servicios ofrecidos por el Ministerio de la Presidencia de Dirección Electrónica Única y Catálogo de Procedimientos del Servicio de Notificaciones Telemáticas Seguras.

De igual forma las partes podrán acceder a nuevas funcionalidades mediante la suscripción, por las partes firmantes de este Acuerdo, de nuevas adendas para servicios no incluidos en el mismo.

Tercera. *Reciprocidad.*–Los servicios sujetos al presente Acuerdo pueden ser puestos a disposición por cualquiera de los firmantes y accesibles por el otro. Se atiende así al concepto de reciprocidad entre las partes, tanto en su calidad de oferentes de servicios como de consumidores de éstos. Esta circunstancia se plasmará expresamente en el clausulado de cada uno de los anexos.

Cuarta. *Comisión Técnica de Seguimiento.*–Para la gestión, seguimiento y control de lo acordado en el presente Acuerdo y de las actividades asociadas a los anexos, se constituirá una Comisión Técnica de Seguimiento que estará compuesta por dos miembros designados por el titular de la Secretaría de Estado para la Función Pública del Ministerio y dos miembros designados por el titular de la Secretaría General del Tribunal Constitucional, ajustándose el funcionamiento de la citada Comisión a las normas contenidas en el capítulo II del título II de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común.

La Comisión Técnica de Seguimiento se reunirá, de manera ordinaria, una vez al año y de forma extraordinaria, a petición de cualquiera de sus miembros. La Comisión mantendrá permanentemente actualizados los datos de referencia y los responsables que figuran en los anexos del Acuerdo.

Corresponde a la Comisión Técnica de Seguimiento resolver los problemas de interpretación y cumplimiento que se deriven del presente Acuerdo, así como proponer la formalización de las mejoras del mismo que considere oportunas o la suscripción de nuevas adendas para servicios no incluidos en el presente Acuerdo.

Quinta. *Régimen económico.*–Este Acuerdo de colaboración no comporta obligaciones económicas entre las partes firmantes.

Sexta. *Plazo de duración del Acuerdo.*–El presente Acuerdo surtirá efectos a partir del día de su firma y tendrá una duración de tres años. El Acuerdo se prorrogará automáticamente por períodos anuales, salvo denuncia por alguna de las partes con una antelación mínima de tres meses antes de la fecha de vencimiento.

Séptima. *Revisión del Acuerdo.*–Cualquiera de las partes podrá proponer la revisión de este Acuerdo en cualquier momento para introducir las modificaciones que se estimen pertinentes. De producirse la revisión del clausulado del Acuerdo, los correspondientes cambios habrán de incorporarse al mismo y ser suscritos por las partes.

La incorporación de adendas de acceso a nuevos servicios no supondrá revisión de las cláusulas del presente Acuerdo.

Octava. *Régimen jurídico.*–El presente Acuerdo tiene naturaleza administrativa y se encuentra excluido del ámbito de aplicación de la Ley 30/2007, de 30 de octubre, de contratos del sector público, en virtud de lo establecido en su artículo 4.1 c). En todo caso, y de conformidad con el artículo 4.2 de la referida Ley, las dudas o lagunas que en la interpretación o ejecución de este Acuerdo pudieran suscitarse, se resolverán aplicando los principios contenidos en dicha Ley.

Novena. *Resolución de conflictos.*–Mediante la firma del presente Acuerdo, las partes se comprometen a resolver de mutuo acuerdo las incidencias que puedan surgir en su cumplimiento.

Las cuestiones litigiosas que surjan entre las partes durante el desarrollo y ejecución del presente Acuerdo y no puedan ser resueltas por la Comisión Técnica prevista en la cláusula cuarta, se someterán a la jurisdicción contencioso-administrativa, conforme a lo dispuesto en la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Y en prueba de cuanto antecede, las Partes suscriben el Acuerdo en dos ejemplares y a un solo efecto, en el lugar y fecha señalados en el encabezamiento.

cve: BOE-A-2010-17147

ANEXO I

Servicio de conexión a la Red SARA

I. *Condiciones Generales*

1. Objeto.–El Ministerio de la Presidencia (MPR) tiene entre sus competencias la Red SARA, integrada por un conjunto de infraestructuras tecnológicas que permiten conectar en red a todas las administraciones que lo deseen, y facilitar un sistema de intercambio de aplicaciones entre Administraciones.

En el ejercicio de estas competencias y en consonancia con lo establecido en el artículo 43 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos que promueve «crear una red de comunicaciones que interconecte los sistemas de información de las Administraciones Públicas españolas y permita el intercambio de información y servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros», está desarrollando SARA (Sistema de Aplicaciones y Redes para las Administraciones).

Teniendo en cuenta que los servicios que reciben los ciudadanos tienen, en muchas ocasiones, que ser prestados en cooperación entre las distintas Administraciones, el objeto de este anexo es determinar las condiciones de utilización de la red SARA por las Administraciones, como enlace común para todas las necesidades de intercomunicación entre las mismas.

2. Alcance.

(i) El servicio abarca la conexión a una plataforma básica de comunicaciones de ámbito privado, con unos servicios básicos y una política de seguridad común para facilitar el intercambio seguro de información entre las aplicaciones de las Administraciones Públicas conectadas a la red SARA, según las características y condiciones que se establecen en este documento.

(ii) La conexión se proporciona a través de un Área de Conexión (AC) que se ubica en dependencias del Tribunal Constitucional (TC) y que es instalada, administrada y mantenida por el MPR.

(iii) El AC comunica de manera segura la Red Corporativa del Tribunal Constitucional con las redes corporativas de otras Administraciones y entidades públicas conectadas a la red SARA y con la red sTESTA de la Comisión Europea.

(iv) Se habilita a cualquier aplicación informática del Tribunal Constitucional a utilizar cualquiera de los servicios que se presten a través de la Red SARA, previo acuerdo entre el prestador del servicio y el beneficiario del mismo, con posterior comunicación al Centro de Soporte de la Red SARA.

(v) Ambas partes acuerdan poner todos los medios a su alcance para adaptarse mutuamente a sus correspondientes planes de direccionamiento, de tal manera que una determinada clase de direcciones IP pueda ser reservada para preservar la compatibilidad.

3. Obligaciones del MPR.–El MPR, como responsable de la Red SARA asume las siguientes obligaciones:

(i) Instalar, administrar y mantener los enlaces para la comunicación y el AC del Tribunal Constitucional ubicado en las dependencias que éste determine y que mejor permitan la conexión con su correspondiente Red Corporativa.

(ii) Proporcionar la documentación técnica correspondiente de la arquitectura y configuración de los sistemas que componen el AC del Tribunal Constitucional.

(iii) Mantener un servicio de soporte 24 × 7 para garantizar la continuidad del servicio de la Red SARA en su conjunto, que sirva para realizar la notificación de incidencias, resolución de las mismas, cuando le corresponda, o gestión de la resolución cuando intervengan agentes externos (fabricantes, operadores, otros organismos con acceso al sistema), consultas técnicas relacionadas con el servicio, así como peticiones de nuevos accesos.

cve: BOE-A-2010-17147

(iv) Habilitar y gestionar un Portal de Administradores que sirva como espacio para facilitar información a los responsables técnicos del TC y de la Presidencia respecto del servicio proporcionado, notificación de incidencias, paradas programadas, publicación de nuevos servicios, etc.

(v) Adoptar las medidas de seguridad necesarias para proteger debidamente la información transmitida, mediante el cifrado de las comunicaciones

4. Obligaciones del Tribunal Constitucional.

(i) Realizar las labores de conectividad y despliegue pertinentes para poder acceder desde sus propias dependencias o instalaciones a la Red SARA a través del AC.

(ii) Gestionar y mantener los elementos activos que conectan su Red Corporativa a la Red SARA, así como las condiciones adecuadas en la ubicación, condiciones medioambientales, suministro eléctrico, cableado, etc, del AC con el fin de asegurar la continuidad del servicio

(iii) Mantener un servicio de soporte, a ser posible 24 × 7 para garantizar la continuidad del servicio en los elementos activos del Tribunal Constitucional, así como de los elementos ajenos al MPR. Para ello se facilitarán al MPR los contactos, tanto de los responsables de la conexión a SARA en el Tribunal Constitucional, como los del Centro de Soporte, CAU o equivalente.

(iv) Colaborar con el MPR en la detección, diagnóstico y resolución de las incidencias, incluso si ello lleva consigo pequeñas comprobaciones o actuaciones en el AC, dirigidas desde el Centro de Soporte de la Red SARA, con el fin de reducir los tiempos de resolución de las incidencias que pudieran ocurrir.

(v) Facilitar y promover las relaciones telemáticas entre el Tribunal Constitucional y el resto de Administraciones Públicas a través de la Red SARA, como vía preferente, en consonancia con lo establecido en el art. 43 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

(vi) Colaborar con el MPR en el mantenimiento del catálogo de servicios y conexiones participadas por ambas partes para, de esta manera, poder tener un mayor control sobre el servicio prestado y así poder reaccionar más rápidamente ante incidentes y problemas. Dicho catálogo permitirá la difusión de los servicios a los usuarios de SARA, facilitará la elaboración de estadísticas, cuadros de mando, etc, que el MPR publicará en el Portal de Administradores a disposición de todos los implicados.

Los prestadores de los servicios se comprometen a proporcionar la información básica indicada en el punto 7.3 para que sean incorporados al catálogo y se encargarán de efectuar las modificaciones para que dicho catálogo esté convenientemente actualizado.

5. Limitación de responsabilidad.–En ningún caso el MPR o sus proveedores están obligados a asumir cualquier daño y perjuicio indirecto que provengan del mal empleo o la no disponibilidad del servicio.

6. Referencias.–El Ministerio de la Presidencia podrá hacer públicas en cualquier lista de referencia o en cualquier boletín de prensa publicado y sin autorización previa, la relación de organismos usuarios de la red SARA.

El Tribunal Constitucional podrá referenciar la utilización de la red SARA sin autorización previa por parte del Ministerio de la Presidencia.

7. Elementos de identificación.

7.1 Identificación del Centro de Soporte de la Red SARA.

Identificación	Centro de Soporte de la red SARA
Responsable de la Unidad.	Montaña Merchán Arribas. Directora de la División de Proyectos de Administración Electrónica.
Responsable técnico.	Jorge Fabeiro Sanz. Jefe de Servicio - Responsable Red SARA.
Horario de servicio.	24 × 7.

cve: BOE-A-2010-17147

Identificación	Centro de Soporte de la red SARA	
Localización.	Ministerio de la Presidencia. María de Molina, 50.	
Gestión de incidencias.	9h a 17h30 de lunes a jueves. 9h a 14h30 los viernes.	912732032. 912732202 incidencias.ia@mpr.es.
	Fuera del horario laboral, sábados, domingos y festivos.	902013114. 618586324.
Observaciones.		

7.2 Identificación del Centro de Soporte del Tribunal Constitucional.

Identificación	Centro de Soporte del TC
Responsable de la Unidad.	Fernando Ruiz García. Subdirector de tecnologías de la información.
Responsable técnico.	Carlos Llorente Calle. Jefe del Área de seguridad, comunicaciones y gestión de calidad.
Horario de servicio.	24 × 7.
Localización.	Tribunal Constitucional. Calle Doménico Scarlatti, 6. 28003 Madrid.
Gestión de incidencias.	De 9 a 19:30 Horas de lunes a viernes. 915508231. 915508305.
Observaciones.	Fuera del horario laboral, sábados, domingos y festivos:. 618164416. 618164959.

7.3 Información a suministrar para cada servicio.

Denominación del servicio.	
Breve descripción.	
Usuarios del servicio.	
Nivel de criticidad.	
Tiempo de respuesta.	
Tiempo de resolución de incidencias.	
Horario del servicio.	
Responsable del servicio (nombre, teléfono y correo electrónico).	
Origen, destino, puerto.	
Funcionalidad.	
Atención de usuarios.	
Resolución de incidencias.	
Observaciones.	

cve: BOE-A-2010-17147

II. *Condiciones técnicas y funcionales*

1. Descripción del Sistema.

1.1. Descripción de la Red Sara y sus elementos de conexión.

La Red SARA es, en esencia, una infraestructura de comunicaciones y un conjunto de servicios básicos asociados a ella para garantizar continuidad, seguridad, y la disponibilidad de un conjunto de prestaciones, de utilidad para las Unidades que se sirvan de ella, de calidad, y en condiciones económicas competitivas, que resulten la primera alternativa a considerar cuando, para la prestación de un servicio en el que hayan de cooperar dos Unidades administrativas, sea necesario compartir e intercambiar información, o acceder a un procesador remoto.

La Red SARA alcanza a los siguientes ámbitos:

Los Centros de Procesos de Datos del MPR donde se alojan los servicios comunes de administración electrónica.

Los Ministerios de la Administración General del Estado y a través de ellos sus Organismos adscritos.

Las Comunidades Autónomas y demás Instituciones Públicas de su ámbito y, a través de aquellas, las Corporaciones Locales.

Las Instituciones y Organismos Públicos que no tienen adscripción a ningún Ministerio y/o Comunidad Autónoma, tales como los Órganos Constitucionales.

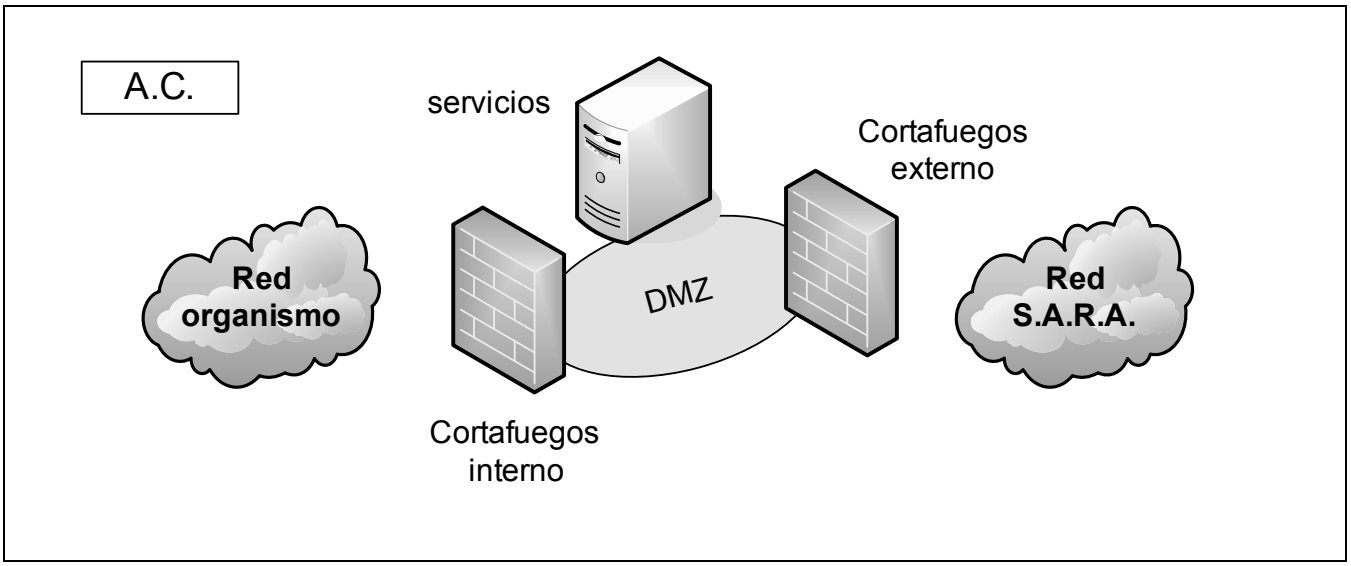
Las Ventanillas Únicas Empresariales.

La Comisión Europea y los Estados Miembros de la UE a tráves de la red sTESTA.

La interconexión a través de un único punto de acceso de cada uno de los Organismos referidos, con la red SARA, se realiza a través de lo que se denomina un Área de Conexión (AC). Este Área de Conexión responde básicamente al esquema de una zona desmilitarizada (DMZ) delimitada por un cortafuegos externo que, en este caso, conecta con el resto de la Red y un cortafuegos interno hacia el interior del organismo.

Los elementos del Área de Conexión, además de realizar funciones de cortafuegos, albergan también los servicios básicos (proxy, relay de correo, servicio DNS, NTP, etc.). En la zona intermedia (DMZ) es posible alojar cualquier equipo que el organismo considere conveniente utilizar para la comunicación con el resto de organismos que componen la Red.

El sistema que actúa como cortafuegos externo es también el encargado de cerrar una red privada virtual (VPN) contra el resto de sedes de la red SARA, con lo que todas las comunicaciones, a través del operador de servicios de telecomunicaciones, van cifradas mediante túneles IPSEC.



cve: BOE-A-2010-17147

1.2. Descripción de los elementos que componen el Área de conexión del Tribunal Constitucional.

La solución completa está formado por los siguientes elementos:

1. Routers externos: estos elementos son los que llevan a cabo la conexión con la red troncal de la red SARA. Cada sede dispone de dos routers cada uno con una línea de acceso a la red VPLS del operador de servicios de telecomunicación, de forma que dispone de una línea principal y otra de respaldo. De esta forma queda asegurada la alta disponibilidad de los enlaces de red.
2. Conmutadores LAN: para el conjunto de conexiones LAN de los elementos que componen la solución, así como para el acceso a los segmentos de conexión con los routers y con la Intranet del organismo, se utilizan dos switches apilados, lo que asegura la disponibilidad ante fallos de uno de ellos.

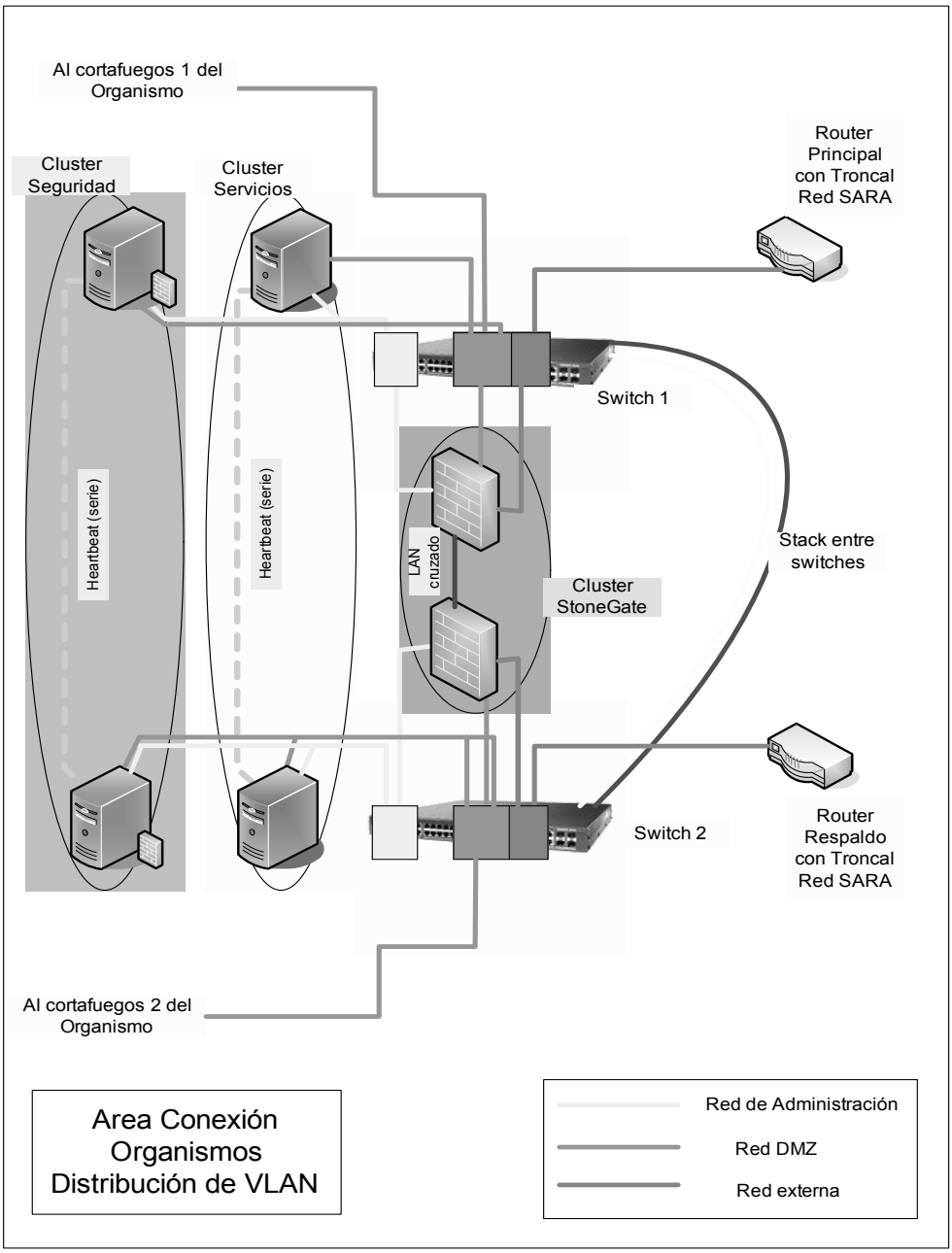
Se configuran tres redes virtuales (VLAN) para separar el tráfico correspondiente a tres zonas:

Tráfico entre los routers y los cortafuegos externos (VLAN externa).
Tráfico del propio AC (VLAN DMZ).
VLAN para el tráfico relacionado con el funcionamiento interno del AC. Este tráfico no es necesario que sea accesible por parte de los usuarios de los servicios de la DMZ, y por tanto se separa en una VLAN aparte. Incluye la comunicación entre los nodos de un racimo (cluster), el tráfico de sincronización de discos, acceso a consolas, gestión de SAI, etc. (VLAN gestión).

3. Cortafuegos externos: cumple las funciones de cortafuegos y cierre de VPN con otros organismos de la red SARA.
4. Racimo de servicios: se trata de un cluster formado por dos nodos en configuración activo-activo. En él se localizan los servicios básicos que proporciona el Área de Conexión: resolución de nombres (DNS), estafeta de correo (SMTP), antivirus, servidor de tiempo (NTP), servidor web y servidor proxy. Los servicios se reparten equitativamente entre los dos nodos. En caso de ocurrir alguna incidencia en un equipo, el otro pasaría a hacerse cargo de las funciones del elemento dañado.
5. Racimo de seguridad y monitorización: se trata de un cluster formado por dos nodos en configuración activo-activo. En él se localizan los servicios de seguridad y monitorización del Área de Conexión. Estos servicios están formados por: sistema de detección de intrusiones (IDS), servidor para gestión de registros del cortafuegos, agente de monitorización de eventos de seguridad en IDS y cortafuegos, monitor de tráfico de red y agente de recogida de datos estadísticos. Los servicios se reparten equitativamente entre los dos nodos. En caso de ocurrir alguna incidencia en un equipo, el otro pasaría a hacerse cargo de las funciones del elemento dañado.
6. Sistemas de alimentación ininterrumpida (SAI): sirve para mejorar la disponibilidad de los elementos en caso de cortes de alimentación. Se suministran dos unidades ya que se solicita a los organismos dos fuentes de potencia externa independientes. Cada una de ellas se debe hacer pasar por su correspondiente SAI. Cada SAI estará conectado a uno de los servidores que actúa como maestro y es capaz de controlar a agentes instalados en el resto de servidores, de forma que en caso de falta absoluta de corriente en las dos fases y agotamiento de ambas baterías proceda al cierre ordenado de aplicaciones y servidores.
7. Armario de altura completa (42U): todos los elementos de la solución se integran en un único armario. Además, todos los elementos de interconexión a la troncal de la red SARA (desde routers hasta posibles conversores de medio) se deberán instalar en este mismo rack. De esta manera, toda la infraestructura del Área de Conexión queda recogida en una única ubicación, con la excepción de los enlaces con el operador y de las conexiones LAN que conectan con la red interna del Tribunal Constitucional.

La siguiente figura muestra el esquema general de los elementos de la solución y sus conexiones:

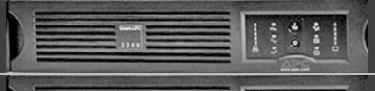
cve: BOE-A-2010-17147



cve: BOE-A-2010-17147

1.3 Características físicas de los elementos.

1.3.1 Subsistema eléctrico y de refrigeración.

U	RACK 42 U	Descripción	Peso (Kg)	Consumo máx. (W)	Refrigeración máx. (BTU)
42 . .					
34 33 32 31 30		RESERVADO PARA LOS ELEMENTOS DE COMUNICACIONES DE ACCESO A LA RED TRONCAL DE LA SARA	5	250	500
26					
25		PDU 2 *			
24		PDU 1 *			
23		VGA (Dell PowerEdge			
22		KVM (Dell PowerEdge	5	50	100
21 20		Dell PowerEdge 2950 (1 x Quad Core)	35	700	1600
19 18		Dell PowerEdge 2950 (1 x Quad Core)	35	700	1600
17					
16		Switch Cisco Catalyst	4	50	100
15		Switch Cisco Catalyst	4	50	100
14 13		Dell PowerEdge 2950 (1 x Quad Core)	35	700	1600
12 11		Dell PowerEdge 2950 (1 x Quad Core)	35	700	1600
10					
9 8		Dell PowerEdge 2950 (2 x Quad Core)	35	700	1600
7 6		Dell PowerEdge 2950 (2 x Quad Core)	35	700	1600
5					
4 3		APC Smart UPS	44	200	400
2 1		APC Smart UPS	44	200	400
	RACK	PowerEdge 4210	110	N/A	N/A
	TOTAL		526	5000	11200

cve: BOE-A-2010-17147

La tabla anterior muestra el peso, las necesidades eléctricas y de refrigeración de los elementos que constituyen el área de conexión.

Las conexiones eléctricas siguen un esquema de alta disponibilidad mediante duplicidad de elementos a los siguientes niveles:

Doble fuente externa de corriente desde fases diferentes. Este aspecto es un requisito que debe ser suministrado por el organismo donde se instala el área de conexión.

Doble sistema de alimentación ininterrumpida (UPS). Cada una de las fases externas proporciona corriente a un UPS distinto. Cada UPS está conectada por USB a uno de los servidores que controla su estado de forma que, en caso de pérdida de alimentación y agotamiento de baterías en ambas UPS, se proceda al apagado controlado por software de los servidores.

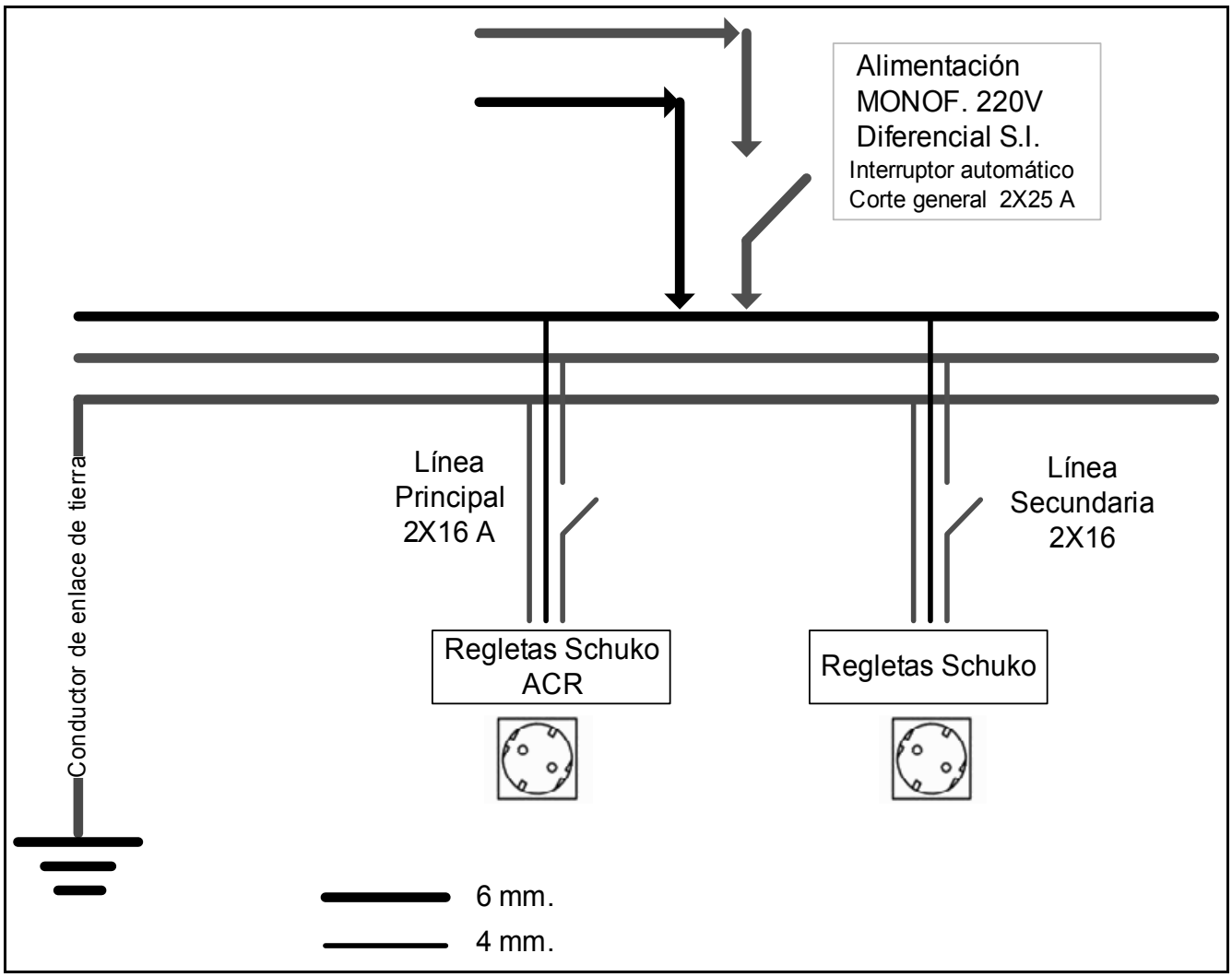
Doble sistema de distribuidores eléctricos para conexión de los elementos de la cabina.

Doble fuente de alimentación en los servidores. Cada una se conecta a un distribuidor distinto de los dos disponibles.

Duplicidad de conmutadores LAN y de los elementos de acceso a la red troncal, cada uno conectado a un distribuidor eléctrico diferente.

Este esquema asegura el suministro eléctrico para todos los elementos críticos del área de conexión.

La siguiente figura muestra el esquema eléctrico recomendado para la instalación:



cve: BOE-A-2010-17147

1.4 Definición de los servicios básicos.

Entendemos por servicios básicos aquellos primeros y fundamentales que soportan la interoperabilidad entre aplicaciones o los complementan. La infraestructura descrita se encargará de la interoperabilidad de estos servicios.

Son servicios básicos de la Red SARA: DNS, relay SMTP, WWW, PROXY y NTP, sincronizado este último con el Real Instituto y Observatorio de la Armada del Ministerio de Defensa que permite entregar al TC la hora oficial española.

ANEXO II

Servicios ofrecidos por el MPR para la intermediación de datos entre Administraciones Públicas

I. *Condiciones Generales*

1. Objeto.–El objeto del presente anexo es regular los derechos y obligaciones que se establecen para la prestación, por parte del MPR, del servicio de intermediación de datos a los órganos, comunidades autónomas o entidades locales que suscriben o se adhieran al Acuerdo.

En el ámbito de la Administración General del Estado, el pasado 22 de junio del 2007, se aprobó la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (LAECSP), cuyo artículo 6.2 b), recoge el derecho del ciudadano a no aportar datos y documentos que obren en poder de las Administraciones Públicas (AAPP). Con el objeto de facilitar la efectividad de esta previsión legal el MPR ha desarrollado una plataforma de intermediación de dichos datos.

Por medio de esta plataforma las AAPP interesadas podrán consultar automáticamente y por medios electrónicos los datos de ciudadanos, bien sea para eliminar la obligación de aportar los citados documentos, o bien para poder realizar comprobaciones de dichos datos siempre que una ley les habilite para ello o el ciudadano de su consentimiento.

Teniendo en cuenta la necesaria cooperación entre las distintas administraciones para proporcionar a los ciudadanos servicios integrados y el principio recogido en el artículo 4.e de la Ley 11/2007, de 22 de junio, el objeto de este anexo es determinar las condiciones de utilización del servicio de intermediación de datos entre Administraciones, para realizar las consultas de datos que sean necesarias en el cumplimiento de las funciones administrativas, cumpliendo las garantías de seguridad, integridad y confidencialidad exigidas por la ley.

2. Alcance.–La aplicación de este anexo habilita a cualquier aplicación informática o empleado del Tribunal Constitucional a utilizar el servicio de intermediación de datos en los términos que se desarrollan más adelante.

El servicio se presta a través de una plataforma básica de intercambio de datos.

3. Obligaciones del prestador del servicio.–El MPR, como prestador del servicio, asume las siguientes obligaciones:

(i) Poner a disposición del Tribunal Constitucional el servicio de intermediación de datos entre AAPP.

(ii) Disponer de entornos de prueba para la integración de los servicios con objeto de garantizar la correcta operación de éstos con carácter previo a su puesta a disposición de los usuarios finales.

(iii) Habilitar los mecanismos para ofrecer el soporte necesario a los equipos de integración y desarrollo del Tribunal Constitucional para la integración de sus aplicaciones con los servicios.

(iv) Disponer de los recursos necesarios para atender y resolver las consultas e incidencias derivadas del uso de los servicios.

(v) Proporcionar los elementos de auditoría en las operaciones realizadas que permitan certificar el no repudio de las transacciones.

cve: BOE-A-2010-17147

(vi) Adoptar todas las medidas de seguridad necesarias para proteger debidamente la información y los servicios de intermediación de ofrecidos.

(vii) Garantizar la escalabilidad, robustez, disponibilidad, integridad y confidencialidad de todos los datos relacionados con la prestación de los servicios de intermediación.

4. Obligaciones del usuario de los servicios.–El Tribunal Constitucional, como usuario del servicio de intermediación de datos, se compromete a:

(i) Realizar las labores de conectividad y despliegue pertinentes para poder acceder desde sus propias dependencias o instalaciones al servicio de intermediación de datos a través del Sistema de Aplicaciones y Redes para las Administraciones (S.A.R.A) desarrollado por el MPR.

(ii) Cumplir con las medidas de seguridad y requisitos de autenticidad, confidencialidad e integridad establecidos en el apartado II de este anexo.

(iii) Concertar con el MPR la realización de pruebas de rendimiento o monitorización de los servicios con el objeto de no comprometer la disponibilidad hacia otros de los servicios al resto de usuarios de estos sistemas de verificación de datos.

(iv) Recabar el consentimiento de los ciudadanos, si no existe una Ley que le habilita a solicitarlos.

(v) Hacer un uso correcto del servicio, utilizándolo para aquello casos para lo que está autorizado.

(vi) Facilitar, promover y habilitar el acceso y uso del servicio de intermediación de datos, a los órganos, o entidades dependientes y administraciones de su ámbito territorial, así como garantizar la calidad del servicio en la parte que le corresponda.

(vii) Seguir los procedimientos establecidos para armonizar los procesos de administración de aplicaciones y sistemas usuarios del Servicio.

5. Acuerdo de calidad de los servicios.–Los servicios objeto del presente anexo estarán sujetos las condiciones técnicas y funcionales recogidas en el apartado II de este anexo.

6. Limitación de responsabilidad.–En ningún caso el MPR o sus proveedores están obligados a asumir cualquier daño y perjuicio directo o indirecto que provengan del mal empleo o la no disponibilidad del servicio.

7. Referencias.–El MPR podrá hacer públicas en cualquier lista de referencia de usuarios o en cualquier boletín de prensa publicado, y sin autorización previa, la relación de comunidades autónomas o entidades locales usuarios de los servicios.

El Tribunal Constitucional podrá referenciar la utilización de dichos servicios sin autorización previa por parte del MPR.

8. Contactos de referencia.–La resolución de consultas técnicas relacionadas con la utilización de los servicios así como las de carácter administrativo relativas al alcance del presente anexo se ofrecerá a través de los siguientes contactos de referencia.

Servicio	SVDI y SVDR
Oferente del servicio.	Ministerio de Presidencia.
Responsable Técnico del Servicio.	Directora de la División de Proyectos para la Administración Electrónica. Teléfono: 91 2732461. Correo electrónico: sgprotec@mpr.es. Dirección postal: María de Molina, 50, 9.ª planta. 28071 – Madrid.
Responsable Administrativo del anexo.	José Luis Redondo Pérez. Vocal asesor de la Dirección General para el Impulso de la Administración Electrónica. Teléfono: 91 2732463. Correo electrónico: joseluis.redondo@mpr.es. Dirección postal: María de Molina, 50, 9.ª planta.

cve: BOE-A-2010-17147

II. *Condiciones técnicas y funcionales del sistema de intermediación de datos entre AAPP*

1. Descripción del sistema de intermediación de datos entre AAPP.–El sistema de intermediación de datos puesto a disposición de las Administraciones Públicas por parte del Ministerio de la Presidencia se establece como servicio horizontal para la consulta, comprobación y/o actualización de los datos de los ciudadanos custodiados por diversas AAPP, según sus competencias.

2. Adopción de medidas de seguridad, organizativas o técnicas del acceso al sistema de intermediación de datos entre AAPP.

2.1 Con carácter general, las comunidades autónomas o entidades locales que accedan al Sistema de Intermediación de datos cumplirán con las medidas de seguridad, conservación y normalización que se detallan en los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades aprobados por el Consejo Superior de Administración Electrónica mediante Resolución de 26 de mayo de 2003 y revisiones posteriores.

2.2 El alcance e intensidad de aplicación de las medidas de seguridad, conservación y normalización vendrán determinadas por el resultado del análisis y gestión de riesgos que se realice, recomendándose a estos efectos la utilización de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) del Consejo Superior de Administración Electrónica.

2.3 Lo dispuesto en este documento se aplicará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y demás normativa aplicable en esta materia como el Reglamento de medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

3. Acceso al sistema de intermediación de datos entre AAPP.–El acceso al sistema de intermediación de datos se realizará a través del Sistema de Aplicaciones y Redes para las Administraciones Públicas (SARA), siguiendo el esquema de conexión que éste tiene establecido para cualquier departamento u organismo público.

4. Requisitos de autenticidad para el acceso a los sistemas de verificación de datos de identidad y residencia.

4.1 El acceso al sistema de intermediación de datos se efectuarán utilizando certificados electrónicos reconocidos que cumplan la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 95948 de 1997).

4.2 El sistema admitirá los sistemas de identificación definidas en la Ley 11/2007, de 22 de junio, para la identificación de las AAPP.

4.3 No podrán utilizarse certificados electrónicos caducados o revocados para acceder al servicio.

5. Requisitos de confidencialidad del sistema.

5.1 El sistema de intermediación de datos ofrecerá consultas en las que, a partir de la identificación del ciudadano (nacional o extranjero) se devolverán los datos pertinentes.

Al tratarse de datos de carácter personal, el responsable del órgano administrativo deberá firmar una autorización, debidamente justificada, para cada usuario y aplicación que accedan al sistema.

5.2 En caso de que los datos introducidos no fueran suficientes para identificar de manera única a un ciudadano, el sistema no devolverá en la respuesta información sobre dicho ciudadano.

5.3 En el Tribunal Constitucional existirá un responsable del uso del servicio de intermediación de datos que velará por las condiciones y normas de buen uso del servicio

cve: BOE-A-2010-17147

entre los usuarios de su administración que tienen acceso a los mismos y los datos que pueden obtener.

5.4 Para realizar la consulta al sistema, será preciso el consentimiento del ciudadano cuyos datos se vayan a consultar, salvo que una norma de rango de ley autorice dicha consulta. Dicho consentimiento deberá constar en la solicitud de iniciación del procedimiento, o en cualquier otra comunicación posterior, siempre y cuando dicha comunicación sea previa a la consulta en el sistema, no pudiendo realizarse consulta alguna en caso de no contar con el consentimiento de forma fehaciente. Los impresos o formularios electrónicos de solicitudes de iniciación de procedimientos administrativos deberán adecuarse para recoger dicho consentimiento y deben informar del uso de la plataforma de intermediación.

En caso de realizar la consulta al amparo de una norma legal, deberá reflejarse en la solicitud de acceso al servicio, tanto la norma que les habilita como la finalidad de la misma.

5.5 Cada consulta y el acceso a la información proporcionada por el sistema de intermediación de datos deberá realizarse con una finalidad concreta, que quedará recogida en el momento de la consulta. La información obtenida sólo podrá utilizarse para dicha finalidad.

6. Requisitos de integridad de la información proporcionada por el sistema.–Todas las consultas que se realicen al sistema, así como las respuestas que devuelvan deberán haber sido firmadas electrónicamente. Esta firma electrónica tiene por objeto garantizar tanto la integridad de los datos intercambiados como la identidad de las partes que intervienen y el no repudio de la consulta.

De la misma forma, todas las consultas que el sistema de intermediación de datos deba realizar a los organismos cedentes de los datos, así como las correspondientes respuestas obtenidas resultado de las mismas, habrán de ser debidamente firmadas electrónicamente para garantizar tanto la integridad de la información como la identidad tanto del organismo cedente como del Tribunal Constitucional.

7. Requisitos de disponibilidad de la información proporcionada por el sistema.–El sistema de intermediación de datos estará disponible los 7 días de la semana las 24 horas del día. Los organismos cedentes deberán contar con la misma disponibilidad y niveles de servicio en sus sistemas.

8. Garantías jurídicas del sistema de intermediación de datos ante posibles recursos.

8.1 Los servicios web proporcionados por este sistema sigue el estándar de intercambio de datos definido por la iniciativa «Sustitución de Certificados en Soporte Papel» del Consejo Superior de Administración Electrónica, que reúne, en base a la normativa vigente, las garantías jurídicas aplicables al intercambio de datos entre Administraciones Públicas.

8.2 El sistema de intermediación de datos dispondrá de un módulo de auditoría, en el que quedarán registradas todas las consultas de datos realizadas, información de contexto asociada, la identidad del solicitante, la fecha y la finalidad de la consulta, y aquellos eventos relevantes desencadenados a partir de la propia consulta. Se garantizará la integridad y no repudio de la información registrada mediante técnicas de firma electrónica y sellado de tiempo, estableciéndose, asimismo, medidas técnicas para garantizar la disponibilidad y recuperación de aquella información que no se mantenga on-line por motivos de eficiencia técnica o seguridad.

8.3 Para certificar la fecha y tiempo de las actividades y sucesos registrados en el sistema de intermediación de datos se hará uso del Servicio de Sellado o marca de Tiempo del Ministerio de Presidencia, de acuerdo al artículo 47 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

8.4 Sólo personal de la Administración Pública debidamente autorizado y acreditado podrá acceder a las funcionalidades de auditoría del sistema.

cve: BOE-A-2010-17147

8.5 La calidad de los datos será responsabilidad del organismo que custodia el mismo.

9. Condiciones de la prestación del servicio.

9.1 La gestión del sistema de intermediación de datos corresponde al Ministerio de la Presidencia.

9.2 Los órganos que hagan uso de estos servicios estarán sujetos a las medidas de seguridad, los requisitos de autenticidad, integridad, confidencialidad, disponibilidad y criterios técnicos establecidos en este documento.

ANEXO III

Servicios ofrecidos por el MPR a través de plataforma de validación y firma electrónica @firma

I. *Condiciones generales*

1. Objeto.–En el ejercicio de sus competencias el Ministerio de la Presidencia (MPR) impulsa el uso de los servicios de certificación y firma electrónicos por ciudadanos y Administraciones Públicas. Para ello el MPR ha desarrollado una Plataforma de servicios de certificación y firma electrónica cuyos servicios pone a disposición de las diferentes administraciones y entidades de derecho público vinculadas o dependientes, para fomentar la puesta en marcha y el despliegue tanto de aplicaciones informáticas que empleen firma, autenticación, validación o generación de firma electrónica como de servicios de Administración Electrónica que requieran de firma electrónica en su relación con los ciudadanos, empresas y organismos.

El objeto del presente anexo es regular los derechos y obligaciones que se establecen para la prestación, por parte del MPR, de los servicios ofrecidos por su Plataforma de validación y firma electrónica.

2. Alcance.–El presente anexo abarca un conjunto de servicios electrónicos que el MPR pone a disposición del Tribunal Constitucional con fines de identificación, validación o generación de firma electrónica.

Entre los servicios ofrecidos por la Plataforma de validación y firma electrónica del MPR se encuentran los siguientes:

Validación de firmas y certificados electrónicas.
Firma electrónica de ficheros y formularios.
Sellos de tiempos.

A efectos del presente anexo se utilizará la referencia al servicio de Validación de Firma para referirse al conjunto de servicios prestados por la plataforma.

Habilita a cualquier aplicación informática del Tribunal Constitucional a validar certificados digitales en procesos de autenticación y firma electrónica de los certificados digitales admitidos por la plataforma. Esta circunstancia introduce, además, la no obligatoriedad por parte del Tribunal Constitucional a suscribir un acuerdo particular de colaboración con los Prestadores de Servicio de Certificación emisores de los correspondientes certificados digitales con los que el MPR tenga firmado un Convenio de colaboración que recoja estas circunstancias. A estos efectos, el MPR facilitará la lista de Prestadores que incorporen esta facilidad.

En el caso de aquellos Prestadores de Servicios de Certificación con los que el MPR no tenga firmado un Convenio al respecto, y mientras no concurra esta circunstancia, el Tribunal Constitucional deberá disponer de los preceptivos Acuerdos vigentes con cada Prestador.

3. Obligaciones del prestador del servicio.–El MPR, como prestador de los servicios ofrecidos por la Plataforma de validación y firma electrónica, asume las siguientes obligaciones:

a) Poner a disposición del Tribunal Constitucional los servicios de validación y firma electrónica ofrecidos por la Plataforma de servicios basada en @firma versión 5.0 o posteriores.

cve: BOE-A-2010-17147

b) Disponer de entornos de prueba de la integración de los servicios con objeto de garantizar la correcta operación de éstos con carácter previo a su puesta a disposición de los usuarios finales.

c) Habilitar los mecanismos para ofrecer el soporte necesario a los equipos de integración y desarrollo del Tribunal Constitucional para la integración de sus aplicaciones con el servicio.

d) Disponer de los recursos necesarios para atender y resolver las consultas e incidencias derivadas del uso del servicio.

e) Proporcionar los elementos de auditabilidad de las operaciones realizadas que permitan certificar el no repudio de las transacciones.

f) Mantener actualizado el software de aplicación de la Plataforma de validación y firma electrónica con las últimas versiones de @firma.

g) Adoptar todas las medidas de seguridad necesarias para proteger debidamente la información de los servicios ofrecidos a través de la Plataforma de validación y firma electrónica.

h) Garantizar la escalabilidad, robustez, disponibilidad, integridad y confidencialidad de todos los datos relacionados con la prestación del servicio de validación y firma electrónica.

4. Obligaciones del usuario de los servicios.–El Tribunal Constitucional, como usuario de los servicios ofrecidos por la Plataforma de validación y firma electrónica, asume las siguientes obligaciones:

a) Realizar las labores de conectividad y despliegue pertinentes para poder acceder desde sus propias dependencias o instalaciones a los servicios proporcionados por la Plataforma.

La accesibilidad a los servicios ofrecidos por la Plataforma se llevará a cabo a través del Sistema de Aplicaciones y Redes para las Administraciones (SARA) desarrollado por el MPR.

b) Cooperar con el MPR y otros organismos usuarios en la evolución de los servicios ofrecidos por la Plataforma de validación y firma electrónica de acuerdo con lo indicado en el punto 6 (Modificaciones y evolución de @firma)

c) Respetar la caracterización tecnológica definida por el MPR y el resto de organismos usuarios a partir de los requerimientos técnicos establecidos para la Plataforma de validación y firma electrónica para la integración de las aplicaciones informáticas usuarias de los servicios.

d) Concertar con el MPR la realización de pruebas de rendimiento o monitorización de los servicios con el objeto de no comprometer la disponibilidad hacia otros de los servicios al resto de usuarios de la Plataforma de validación y firma electrónica.

e) Seguir los procedimientos establecidos por el MPR para armonizar los procesos de administración de aplicaciones y sistemas usuarios de los servicios de la Plataforma.

A esos efectos, suministrará la información requerida por el MPR para dar de alta aplicaciones informáticas usuarias de los servicios, configurar la política de firma electrónica asociada, etc.

5. Acuerdo de calidad de los servicios.–Los servicios objeto de la presente Adenda estarán sujetos al Acuerdo de Nivel de Servicios ofrecido por el MPR que se adjunta en el apartado II de este anexo.

6. Modificaciones y evolución de @firma.–El Tribunal Constitucional se convierte en miembro del Programa de Evolución Continua (PEC) de @firma, que se regirá por el Marco de Evolución Continua (MEC) que se adjunta en el apartado III de este anexo. El periodo de pertenencia a dicho grupo de trabajo está sujeto al periodo de vigencia del presente Acuerdo y a sus posteriores prórrogas.

El Tribunal Constitucional podrá designar representantes en el PEC pertenecientes a otras entidades con las que colabore en el desarrollo de actividades ligadas a la firma e identificación electrónica

cve: BOE-A-2010-17147

La adaptación y progresión de los servicios a las nuevas exigencias del Tribunal Constitucional se realizarán preferentemente de manera coordinada en el seno del citado grupo de trabajo del PEC.

7. Referencias.–El MPR podrá incluir al Tribunal Constitucional, sin autorización previa, en cualquier boletín de prensa o lista de usuarios que haga referencia a los organismos usuarios de los servicios a los que hace referencia el presente anexo.

El Tribunal Constitucional podrá referenciar la utilización de dichos servicios sin autorización previa por parte del MPR.

8. Contactos de referencia.–La resolución de consultas técnicas relacionadas con la utilización de los servicios así como las de carácter administrativo relativas al alcance del presente anexo de servicios se ofrecerá a través de los siguientes contactos de referencia.

Servicio	Validación y firma electrónica @firma
Oferente del servicio.	Ministerio de la Presidencia.
Responsable Técnico del Servicio.	Directora de la División de Proyectos de Administración Electrónica Teléfono: 91 273 24 53. Correo electrónico: sgprotec@mpr.es. Dirección postal: María de Molina, 50, 3.ª Planta. 28071 – Madrid.
Responsable Administrativo del anexo.	José Luis Redondo Pérez. Vocal Asesor de la Dirección General para el impulso de la Administración Electrónica. Teléfono: 91 2732463. Correo electrónico: joseluis.redondo@mpr.es. Dirección postal: María de Molina, 50, 9.ª planta. 28071 – Madrid.

II. *Marco de evolución continua de @firma*

1. Objeto.–La Plataforma de validación y firma electrónica @firma del MPR se basa en el software @firma versión 4.0, que fue cedido por la Junta de Andalucía en el marco del Convenio de Colaboración firmado entre el Ministerio de Administraciones Públicas y la Junta de Andalucía para la cesión de aplicaciones informáticas de Administración Electrónica.

El citado Convenio establece las bases para la creación de un grupo de trabajo que tiene, entre otras misiones, las siguientes:

El seguimiento de la cesión de las aplicaciones informáticas acordadas.

La identificación y el desarrollo de las mejoras que puedan realizarse sobre las mismas.

Igualmente, en dicho Convenio ambas partes se comprometen a establecer mecanismos de cooperación y normalización en el seguimiento de la evolución de @firma, de manera que pueda trasladarse una imagen integrada y coherente de la situación en el conjunto del Estado y Comunidad Autónoma.

Con estas premisas, se ha acordado la creación de un Programa o escenario de trabajo, que se ha denominado Programa de Evolución Continua (PEC), que servirá para conciliar y materializar las necesidades de las administraciones públicas en materia de firma electrónica (firma-e) y certificación digital con los servicios de firma-e ofrecidos por el MPR y el producto para la validación y firma, @firma.

El objeto del Marco de Evolución Continua (MEC) es establecer las pautas de funcionamiento que seguirá el grupo de trabajo que participará en el desarrollo de dicho PEC.

cve: BOE-A-2010-17147

2. Definiciones.–A efectos de este MEC se entiende por:

@firma: Producto de firma y certificación electrónica que constituye la base tecnológica de los servicios de firma-e ofrecidos por el MPR.

DNI-e: Documento Nacional de Identidad electrónico.

Participante del PEC: Cualquier Administración, departamento ministerial u otra entidad de derecho público que haga constar su intención de asumir las estipulaciones de MEC. Se distinguen dos modalidades de participación:

Como miembro del PEC: Participantes que han firmado un Convenio de colaboración, ya sea para acceder a los servicios de la Plataforma de firma-e del MPR (modelo ASP o Aplication Service Provider), o bien para obtener una licencia del producto @firma (modelo federado).

Como observador: Participantes que asisten a las reuniones del grupo de trabajo objeto de este MEC porque están interesadas en la evolución de @firma y que no reúnen las condiciones para ser miembros del PEC.

Plataforma de firma-e: Plataforma física de servicios de certificación y firma basada en el producto @firma que el MPR pone a disposición de las administraciones y entidades públicas vinculadas o dependientes que suscriban el Convenio de uso de sus servicios.

PSC o «Prestador de Servicios de Certificación»: Entidades públicas o privadas que expiden certificados digitales y ofrecen servicios asociados conforme a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

3. Alcance.

Este MEC establece los términos generales de la relación entre los participantes en el grupo de trabajo para desarrollo de los servicios de firma-e que el MPR pone a disposición de las distintas administraciones y entidades públicas vinculadas o dependientes.

Más concretamente, los trabajos de este grupo darán como resultado las pautas de funcionamiento del Programa de Evolución Continua (PEC) de los servicios de firma-e ofrecidos por el MPR y del producto para la validación y firma @firma, con el fin de impulsar y ayudar a la implantación de la firma-e, catalizar el intercambio de conocimientos y experiencias entre las Administraciones, y rentabilizar las inversiones llevadas a cabo en este área.

El grupo de trabajo resultante de este MEC tiene entre sus objetivos principales:

Determinar los criterios que sirvan para la articulación del PEC: obligaciones, garantías, condiciones de uso del producto, etc.

Intercambiar y difundir aspectos relativos a la adecuación tecnológica de las infraestructuras de firma-e de los miembros en materias afines: DNI-e, formatos de firma, validación de certificados, etc.

Identificar y articular la implementación de mejoras correctivas y evolutivas de servicios y productos, adoptando, con la mayor prioridad, los estándares publicados a nivel nacional e internacional por las entidades de estandarización y normalización.

Asimismo, se pueden destacar entre sus objetivos secundarios los siguientes:

Coordinar la prestación de servicios comunes relacionados en el ámbito de competencia de los participantes: CAU, soporte a la integración, etc.

Difundir capacidades y evolución de la tecnología de a la firma-e, explotando y haciendo ampliamente accesible la información científica y técnica entre sus miembros.

Las decisiones relevantes adoptadas por el grupo de trabajo serán elevadas a la Comisión Permanente del Consejo Superior de Administración Electrónica de la Administración General del Estado y al Comité Sectorial de Administración Electrónica.

cve: BOE-A-2010-17147

4. Participantes.

Los participantes acuerdan actuar de buena fe y cooperar en el seno grupo de trabajo, compartiendo la información y soportes que sean requeridos.

La participación en este MEC está abierta a cualquier Administración, entidad pública o departamento ministerial ya sea como participante o, previa aprobación de solicitud, como observador.

Los participantes en condición de observadores:

Tienen acceso a toda la información y documentos generados en el seno del grupo de trabajo.

Participan a igualdad de condiciones que los miembros del PEC en todo lo referente a la articulación del PEC, evaluación de tecnología relativa a firma-e, participación en estudios, procesos de estandarización, etc.

Entre su principal propósito se encuentra el de analizar y evaluar los servicios ofrecidos por la Plataforma de firma-e y/o el producto @firma.

Los participantes en condición de miembros del PEC, además de los aspectos considerados para los observadores:

Deciden sobre aspectos evolutivos, operativos del servicio y producto.

Determinan la evolución del servicio prestado por la Plataforma @firma, en aspectos como:

Nuevas funcionalidades,
Interoperabilidad de los módulos del producto,
Portabilidad de plataforma hardware, software a nivel de cliente y servidores.
Determinación de elementos de confianza que sirvan de base para el modelo Federado.
Sistema de accounting y reporting, etc.

Aquellos miembros que hubieran elegido el modelo ASP colaborarán, junto con el Equipo de dirección de la Plataforma de firma-e del MPR, en la determinación de decisiones como:

Nivel de soporte a la integración.
Soporte a usuarios finales de aplicaciones.
Administración y parametrización de entornos.
Gestión de la explotación.
Integración con servicios externos de time-stamping.
Políticas de Firmas a registrar y PSCs a incorporar a la Plataforma.
Modelos de custodia de los documentos, etc.

Los participantes se comprometen a promocionar e impulsar las líneas actuación y servicios resultantes del grupo con diferentes órganos y entidades públicas vinculadas o dependientes de los que éstos representan.

5. Equipo de coordinación

Entre el conjunto de participantes en el MEC se designará un Equipo de coordinación para asegurar la planificación y desarrollo de los trabajos acordados en el seno del grupo. Este equipo, cuya composición podrá variar para adecuarse a las necesidades que se determinen, estará compuesto al menos por dos representantes del MPR y dos representantes del Tribunal Constitucional, que serán designados respectivamente por el Director General para el Impulso de la Administración Electrónica del MPR y por el Secretario General del Tribunal Constitucional.

cve: BOE-A-2010-17147

Los representantes del MPR en este grupo serán los responsables de dirigir las actuaciones que se lleven a cabo sobre la Plataforma de firma-e implementada por este Ministerio.

Otras tareas a desempeñar:

Custodiar los códigos fuentes y otros recursos reservados del producto @firma.

Mantener la estructura orgánica de los participantes, gestionando nuevas incorporaciones, bajas, etc.

Organizar y coordinar reuniones de grupo. El lugar de reuniones podrá ser variable en función de los ofrecimientos de los integrantes y la disponibilidad.

Promover encuentros con grupos o entidades públicas o privadas externas para profundizar o evaluar criterios técnicos y operativos.

Facilitar la intermediación entre el grupo y otros grupos y comités de carácter público que abordan materias afines al grupo como los grupos de trabajo derivados de la Comisión Técnica de Apoyo a la implantación del DNI-e o el Consejo Superior de Administración Electrónica.

Posibilitar la proyección de los trabajos desarrollados por el grupo a Comités o grupos de normalización especializados en materia de firma-e.

Trasladar las decisiones de los miembros del PEC a los equipos responsables del mantenimiento correctivo y evolutivo de @firma.

Evaluar propuestas de colaboración externa que se deriven del desarrollo de productos y servicios disponibles.

Elevar propuestas de actividades, gestiones u otras consideraciones de los participantes a las reuniones de grupo.

Evaluar la incorporación de nuevos PSC a la Plataforma de firma-e basándose para ello en el protocolo de adhesión habilitado al efecto y evaluando las Declaraciones de Prácticas de Certificación y estructura de los certificados digitales propuestos.

Aprobar las solicitudes recibidas de otros organismos para la participación como miembros observadores.

6. Inicio y duración.

La vigencia del presente Marco estará asociada a la propia vigencia de los convenios suscritos que habilitan a sus miembros a participar en el mismo.

7. Costes de funcionamiento.

Los participantes correrán con los costes de su participación en las actividades del grupo de trabajo, lo que incluye los implícitos de formular o transmitir informes, los gastos de viajes, y otros gastos, relacionados con su asistencia a las reuniones convocadas, y con otras funciones, eventos y actividades del grupo.

El MPR, dentro de sus gastos ordinarios de funcionamiento, asume los costes de gestión y administración de repositorio único de documentos, habilitación de salas de reunión, confección de fotocopias u otras actividades asociadas a la coordinación del grupo. Se emplearán herramientas de groupware y desarrollo colaborativo para la publicación, difusión y coordinación de la actividad del grupo, que será gestionada por participantes de MPR.

8. Confidencialidad

Los participantes podrán declarar que determinada información facilitada en el seno del grupo es propietaria y confidencial, a efectos de que sea tratada como tal por el resto de componentes. Se incluyen programas, documentación, datos técnicos, planes, tecnologías, etc.

Aquella información considerada como confidencial no podrá ser revelada a terceros, salvo autorización de los participantes propietarios o del equipo de coordinación.

cve: BOE-A-2010-17147

Sólo puede ser revelada a empleados y colaboradores de los diferentes organismos participantes para actividades relacionadas con el grupo de trabajo, siendo informados del carácter confidencial de la información tratada.

En el momento de dar por finalizada la participación en el grupo de trabajo del presente MEC, los participantes cesantes habrán de dejar de usar la información confidencial, pudiendo ser solicitada por el equipo de coordinación y quedando prohibida la realización de copias.

9. Propiedad intelectual.

Se intentará, en la medida que la normativa que resulte de aplicación lo permita, poner bajo dominio público el resultado de todos los trabajos encargados, creados o desarrollados directamente en el seno del grupo, respetando las condiciones establecidas por los proveedores externos de información al grupo.

Para hacer público en el grupo y/o fuera de él documentos pertenecientes a algunos de los participantes, se ha de obtener del propietario de la información un consentimiento expreso.

Los participantes promoverán la transferencia no exclusiva a otras entidades públicas de los recursos que sean producto del presente Marco de colaboración.

Las obligaciones anteriores se cumplirán, en todo caso, con pleno respeto a los derechos de propiedad intelectual regulados por el Real Decreto Legislativo 1/1996, de 12 de abril, modificado por la Ley 5/1998, de 6 de marzo, por el que se aprueba el texto refundido de la Ley de propiedad intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

III. *Acuerdo de nivel de servicio (ANS) de plataforma de Validación y firma electrónica @firma del MPR*

1. Objeto.–Según la Ley 59/2003, de 19 de diciembre, de firma electrónica, cualquier compañía constituida como Prestador de Servicios de Certificación (PSC) puede emitir certificados electrónicos, que cumpliendo una serie de requisitos, identifican en el ámbito telemático a una persona física.

En la actualidad existen multitud de empresas constituidas como PSCs y, consecuentemente, múltiples certificados electrónicos, todos ellos válidos como medio para acreditar la identificación personal en el ámbito electrónico.

Además, la progresiva implantación del DNI electrónico en el territorio nacional requiere de una modificación en los servicios de Administración Electrónica proporcionados por los organismos Públicos, para garantizar su aceptación como elemento de autenticación y firma en la tramitación telemática con los ciudadanos.

Esta multiplicidad de certificados, y las carencias de interoperabilidad de los mismos, obliga al Ministerio de la Presidencia (MPR), dentro de su misión impulsora de la Administración Electrónica, a desarrollar una plataforma para verificar la identidad electrónica de una persona física o jurídica, independientemente del tipo de certificado que ésta utilice en sus relaciones telemáticas con la Administración.

En este contexto nace la plataforma de validación del MPR denominada @firma que establece un ecosistema de seguridad, permitiendo verificar el estado y validez de los certificados electrónicos empleados por el ciudadano en cualquier procedimiento telemático, entre ellos, los del DNI-e.

La solución propuesta es no intrusiva con arquitecturas y soluciones ya existentes. Por ello, sus principales características son:

La plataforma se basa en Servicios Web que son utilizados por las distintas AAPP.

Es una plataforma de validación MultiAC (múltiples Autoridades de certificación), MultiPolítica, MultiCertificados, MultiFirma, MultiFormatos..., de tal manera que permite la utilización de múltiples tipos de Certificados y Autoridades de Validación a los ciudadanos, en su relación telemática con las distintas AAPP.

cve: BOE-A-2010-17147

Permite una evolución diseñada y articulada por los organismos usuarios, de una manera participativa y colaborativa.

Proporciona las máximas garantías de seguridad y robustez, garantizando en su funcionamiento: interoperabilidad, rendimiento óptimo, alta disponibilidad, portabilidad, etc.

El MPR, como prestador de los servicios de validación y firma electrónica a través de su plataforma de servicios basada en @firma, se regirá por un enfoque orientado a la gestión del servicio, donde la calidad del mismo se medirá mediante los parámetros del Acuerdo de Nivel de Servicio (en adelante ANS). Este ANS contemplará tanto los parámetros propios del servicio, como los de soporte a los interesados y organismos emisores, para la gestión y resolución de consultas e incidencias, durante todo el tiempo de duración de la prestación de los servicios por el MPR.

El MPR se compromete a cumplir los niveles indicados en este documento y a determinar la evolución de éstos a medida que van evolucionando nuevos servicios.

El enfoque del presente ANS, se realiza en múltiples ámbitos: desde el punto de vista de la disponibilidad de los servicios de validación y firma contemplados en la plataforma @firma del MPR, servicios de sistemas y comunicaciones, servicio de atención a usuarios, monitorización de sistemas, etc.

2. Calendario para la implantación del ANS.–El MPR se ajustará al siguiente calendario para la obtención de los niveles de servicio establecidos para cada parámetro:

Periodo transitorio:

Es el periodo inicial, desde el arranque del servicio hasta que este alcance el ajuste necesario para su estabilización.

Este periodo será de seis meses desde la fecha de publicación de este documento y el prestador deberá alcanzar el 90 % del objetivo marcado en cada parámetro.

Período de prestación del servicio:

El prestador deberá alcanzar como mínimo los objetivos establecidos y comprometerse a completar, perfeccionar y mejorar el ANS inicial.

3. Niveles de servicio genéricos de las infraestructuras de alojamiento y comunicaciones.

3.1 Infraestructuras básicas.

Se dispone de los siguientes servicios básicos de infraestructuras en el Centro de Proceso de Datos, con todos los sistemas en redundancia n+1 y sin punto único de fallo abajo descritos:

Alimentación eléctrica ininterrumpida:

Se dispone de un sistema de alimentación de corriente alterna, filtrada y balanceada a través de dos UPS en redundancia n+1, que permiten una potencia desde 500 hasta 2.000 W/m^2, y una capacidad de 1,6 a 2,5 MW sin punto único de fallo.

Los racks de servidores de la Plataforma disponen de dos tomas eléctricas, redundantes e independientes: UPS1 y UPS2. Adicionalmente existen generadores diesel en redundancia n+1 con una autonomía de 48 horas y un contrato con el distribuidor de gasoil que garantiza la recarga de los tanques en un tiempo inferior a 4 horas.

Suelo técnico:

Suelo técnico de 50 cm de altura compuesto por baldosas antideslizantes y antiestáticas reforzadas de 600 × 600 mm y 30 mm de espesor que permite una carga máxima por metro cuadrado de 1.000 kg. Distribuido sobre ese suelo existen diferentes sensores de temperatura y humedad gestionados por un sistema SCADA ("Supervisory Control and

cve: BOE-A-2010-17147

Data Acquisition») que permite la supervisión, monitorización y control desde una consola centralizada en el NOC («Network Operation Center»), mediante el sistema BMS («Building Management System») del edificio.

Sistemas de Control de Temperatura y Humedad (HVAC):

El sistema HVAC está basado en la gestión del ambiente mediante el enfriamiento de agua y permite un control constante de temperatura de 22 ºC +/- 5 ºC con una humedad relativa del 20 % al 70 %. Las bombas y los refrigeradores están situados en la planta superior con redundancia n+1 y sin ningún punto único de fallo. Del mismo modo, la distribución del mismo sobre el edificio mantiene la redundancia en anillos con sensores ante detección de fugas. En cada sala existe un sistema igualmente redundado de aire acondicionado y filtrado.

Protección de incendios:

El sistema de detección de incendios consta de múltiples sensores ópticos situados en techo y suelo de cada una de las salas técnicas. El sistema entra en funcionamiento en el momento que más de dos detectores de humo se activan y es completamente direccionable para el edificio entero, permitiendo la detección cruzada (en techo y en piso elevado) El sistema de extinción permite el disparo automático y manual y está basado en la inundación total de la sala con gas F-13, que es almacenado en cuartos separados en el edificio.

Iluminación:

Todas las salas están iluminadas con tubos de 4 × 18 W, con difusores en «V», y poseen luces de emergencia y señales que proporcionan la información precisa acerca del entorno y salidas.

Control de acceso seguro 24 × 7 (seguridad física):

Se dispone de un sistema con circuito cerrado de televisión que controla el acceso interior y exterior del edificio, así como el acceso a las diferentes salas. La entrada a las mismas se realiza con lectores de tarjeta de proximidad o de identificación biométrica que tienen programados los caminos de acceso permitidos al cliente. La entrada/salida es controlada por los policías del servicio de seguridad del edificio en 24 × 7 y mediante apertura remota. Las puertas de emergencia poseen unas células de apertura que activan una serie de alarmas en función de los intentos de acceso no autorizados. Este sistema permite un acceso 24 × 7 mediante una lista de personal autorizado, manteniendo un registro seguro según el Manual de Operación de:

Las personas que acceden al edificio.
Las personas que acceden a las salas.
Entrada y salida de material.

Doble ruta de acceso de cables:

El edificio dispone de doble ruta de entrada de cables para poder ofrecer redundancia de caminos disponiendo así de una mayor seguridad ante el eventual corte de una de las rutas.

Parámetros Generales del ANS	Niveles de servicio – Porcentaje
Suministro de energía eléctrica segura	99,999
Condiciones ambientales:	
Temperatura (22 ºC +/- 5 ºC)	99,90
Temperatura (22 ºC +/- 8 ºC)	99,99
Humedad (20 % a 70 %)	99,90

cve: BOE-A-2010-17147

3.2 Comunicaciones.

3.2.1 Punto neutro de interconexión a SARA.

El acceso a los servicios de la Plataforma se realiza a través de SARA, o Sistema de Aplicaciones y Redes para las Administraciones-, una infraestructura tecnológica que permite y garantiza la comunicación entre las distintas administraciones además de servir de plataforma de intercambio de aplicaciones. Constituye una extranet de comunicaciones que da soporte a la interoperabilidad entre aplicaciones de diferentes organismos públicos.

Incluido dentro de la infraestructura base proporcionada por SARA, se dispone de un punto neutro de comunicaciones (PNC) que posibilita la accesibilidad a los servicios de la plataforma desde múltiples operadores de comunicaciones, dentro de un esquema de direccionamiento IP privado y con las mayores garantías de monitorización.

Serán de aplicación las siguientes condiciones de implantación en el punto neutro:

Solo serán permitidos aquellos equipos de cliente o proveedor necesarios para la provisión de servicio de interconexión (equipos de transmisión y/o acceso).

En caso de que el servicio se pueda proveer sin necesidad de equipos activos, los cables podrán acceder directamente hasta la zona del Repartidor Principal del proveedor.

Los repartidores de cables de entrada al edificio se alojarán en el Área de Servicio del cliente o proveedor (pudiendo ser éste PNC si sólo se tiene presencia en la misma).

No serán permitidas interconexiones directas entre salas, jaulas o racks de clientes o proveedores; toda interconexión entre ellos deberá ser obligatoriamente realizada en el PNC.

La Intranet Administrativa (IA), como infraestructura básica de comunicaciones y servicios telemáticos de la AGE se conecta al punto neutro mediante dos enlaces GigabitEthernet (1 Gbps) en alta disponibilidad cada uno de ellos con un operador distinto.

La conexión de un nodo de la AGE con la red troncal de la IA cuenta con un enlace principal y otro de respaldo (backup) también con 2 operadores distintos lo que proporciona un aseguramiento en la fiabilidad y continuidad en el servicio prestado. Adicionalmente y como medida de seguridad la información transita a través de la red troncal cifrada mediante el establecimiento de túneles IPSec.

La IA cuenta con un servicio de soporte 24 × 7 en el que los tiempos de respuesta y de resolución dependen de la severidad de la incidencias en base a una categorización de los servicios que por ella transitan y de los agentes que participen extremo a extremo.

Parámetros Generales del ANS	Niveles de servicio
Tiempo de respuesta en 24 × 7	120 minutos

3.3 Intervenciones en sistemas físicos.

Se dispone del servicio de soporte básico (On Site Basic Support - OSBS) que consiste en la intervención de técnicos para ejecutar tareas básicas sobre los equipos bajo instrucciones directas.

Ejemplos de estas tareas básicas son:

Cambio de cableado en un repartidor.
Encendido y apagado de equipos.
Reset de tarjetas y sistemas.
Cambio de tarjetas (repuestos proporcionados por el cliente).
Verificación de conexiones.
Cambios de cinta para respaldos (back-ups).
Inspección visual e identificación de alarmas.

cve: BOE-A-2010-17147

Otras acciones básicas a definir.

Se dispone de técnicos con formación específica para este servicio y con amplia experiencia en la ejecución de este tipo de servicios, con disponibilidad 24 × 7 × 365.

Estos técnicos disponen de los procedimientos y configuraciones de los equipos para la correcta ejecución de las tareas.

En función de las necesidades del cliente, todas las intervenciones se catalogarán dentro de los siguientes tiempos de respuesta:

Parámetros Generales del ANS	Niveles de servicio*
Intervenciones no urgentes y programadas	Menor a 24 horas
Intervenciones urgentes	Menor a 4 horas
Intervenciones muy urgentes	Menor a 2 horas

* El tiempo de respuesta se considera desde la emisión del acuse de recibo del parte de solicitud de servicio hasta que el técnico llega a la sala del cliente y comunica que está a disposición para iniciar el servicio.

3.4 Monitorización y supervisión.

Se dispone de servicios de monitorización en 24 × 7 de los equipos de la Plataforma a través de la gestión de agentes SNMP.

Este servicio permite la monitorización de hardware, software, servicios de sistemas y aplicaciones; mediante una supervisión paramétrica con un tiempo de respuesta inferior a 15 minutos en 24 × 7 garantizado por ANS.

La monitorización se lleva a cabo desde un Centro de Operación y Soporte centralizado (COS).

El servicio de monitorización incluye cuatro (4) modalidades:

Parámetros Generales del ANS	Niveles de servicio
Monitorización básica/ICMP de sistemas y líneas de comunicaciones.	Período: 24 × 7. Avisos <= 15 minutos.
Monitorización preventiva.	Período: 24 × 7. Avisos <= 15 minutos.
Monitorización avanzada.	Período: 24 × 7. Actuación procedimentada tras aviso <= 15 minutos.
Monitorización Internet. De dominios, portales y aplicaciones en Internet desde varias redes.	Período: 24 × 7. Avisos <= 15 minutos.

3.5 Copias de seguridad.

Se realiza un respaldo (backup) a dos niveles:

Respaldo centralizado, consistente en la integración de los sistemas de la Plataforma en una red y plataforma de respaldo basada en HP Data Protector.

Respaldo remoto, consistente en la gestión de la plataforma de respaldo particular de los sistemas de la Plataforma.

La política aplicada es la siguiente:

Respaldo incremental diario de todos los módulos de información de los sistemas.

Respaldo completo semanal, con un periodo de retención de las cintas de cuatro (4) semanas. El último respaldo del mes tiene retención de 1 año y, el último del año, retención de 5 años. Se pueden establecer períodos más largos en función de la naturaleza de la información almacenada.

cve: BOE-A-2010-17147

En cumplimiento del marco legal en materia de protección de datos (LOPD), se realiza la encriptación de datos de respaldo desde de la salida de los sistemas de la Plataforma.

Parámetros Generales del ANS	Niveles de servicio
Disponibilidad de servicios de respaldo (backup) y restauración (restore)	99 %

4. Niveles de disponibilidad de los servicios y actuaciones de soporte a Organismos.

4.1 Niveles de urgencia e impacto y Tiempos de Respuestas.

Se categorizan los siguientes niveles de urgencia e impacto para el tratamiento de incidencias, que podrán evolucionar con el seguimiento de la explotación de los servicios.

Urgencia		
Categoría Petición	Tipo	Descripción
Incidencia	Alta	Impiden el acceso y/o el uso del servicio a todos los usuarios.
	Media	Afecta a un grupo importante de usuarios. Interrumpe la prestación normal del servicio pero tiene alternativa de funcionamiento
	Baja	Afectan a un número muy limitado de usuarios del servicio y no tienen trascendencia global. No interrumpe la prestación normal del servicio.

Impacto	
Nivel de Impacto	Descripción
Alto	Servidores principales para el Servicio. Afecta a más de 50 usuarios. Caída de Base de datos. Fallos de conectividad entre componentes. Infección masiva de virus informáticos. Violación de la seguridad. Afecta a los ciudadanos. Incidencias que provoquen incumplimientos legales.
Medio	Incidencias de 5 a 40 usuarios afectados por un problema. Incidencias de degradación de los servicios. Accesos remotos de usuarios de otra ubicación. Incidencias de software que residan en un servidor. Incidencias de un usuario individual.
Bajo/Sin impacto	Incidencias con poco impacto en el Servicio. Requerimientos de actualizaciones de software y/o hardware. Requerimientos de información. Labores de mantenimiento. Actualizaciones no críticas de sistemas operativos. Actualizaciones periódicas de aplicativos.

Por tanto, del cruce entre la Urgencia de una incidencia y el Impacto en el Servicio, se obtiene la siguiente matriz que reflejará los niveles de priorización de cada incidencia conforme a la metodología ITIL.

Urgencia	Descripción	Impacto		
		Alto	Medio	Bajo
Alta	El servicio está completamente caído.	P1	P2	P3
Media . .	El servicio está parcialmente caído, o existe degradación en los elementos	P2	P3	P4
Baja . . .	Afecta a un número reducido de usuarios	P3	P4	P5

cve: BOE-A-2010-17147

Los tiempos de respuesta y resolución para el servicio se configuran de la siguiente manera reflejados en la siguiente tabla:

Prioridad	Descripción	Tiempo Máximo Resolución
P1	Crítica	1 hora
P2	Importante	8 horas
P3	Moderado/Normal	24 horas
P4	Menor/Baja	48 horas
P5	Por planificar	Por planificar

Por tiempo de respuesta se entiende desde que el centro de operaciones hace suya la incidencia y comienza a gestionar los recursos para la resolución de la misma.

El horario de cobertura de los servicios contemplados en el presente apartado serán:

1. Incidencias graves y leves: Horas laborables de lunes a domingo de 9:00 a 19:00 h.
2. Incidencias críticas: servicio 24 × 7 con teléfono específico para la atención de este tipo de incidencias.

4.2 Informes de indicadores del cumplimiento del nivel de servicio (ANSs).

Mensualmente se dispondrá de un informe de incidencias cerradas, incidencias abiertas incidencias no resueltas dentro de los limites definidos por el ANS y grado de cumplimiento del Acuerdo de Nivel de Servicios comprometido.

Ejemplos de indicadores empleados para la evaluación de cada servicio:

Número de incidencias del servicio.
Número de incidencias atendidas dentro del tiempo de respuesta.
Número de incidencias resueltas dentro del tiempo de resolución.
Porcentaje de ANSs alcanzados dentro del tiempo de respuesta.
Porcentaje de ANSs alcanzados dentro del tiempo de resolución.

Ejemplo:

Servicio /Categoría	N.º Incidencias	N.º Incidencias OK en: Tiempo Respuesta Tiempo Resolución	% ANS alcanzado en: Tiempo Respuesta Tiempo Resolución
Hardware	1	1 1	100 100
Arquitectura y configuración	5	3 4	92 95
Plataforma base	31	29 28	94 92
Conectividad	21	21 21	100 100
Servicios externos:			
Conexión PSCs	3	3	100
TSA		3	100
Integración	4	4 4	100 100
Total	292	287 284	98 97

cve: BOE-A-2010-17147

4.3 Parámetros del soporte y Atención a usuarios.

El servicio de soporte y atención a usuarios de la plataforma, es parte inseparable del sistema global, especialmente dado que se trata de servicios donde los usuarios son ajenos al prestador del mismo.

El servicio de Soporte y Atención al Cliente abarca a los siguientes interlocutores:

Organismos que integran los servicios de la Plataforma.

CAU de nivel 2 para atender a agentes externos al servicio: organismos, otros CAUs de los organismos, PSCs, etc.

CAU de 3er nivel, que atiende a las peticiones de nivel de actuación en sistemas y desarrollos del CAU de 2.º nivel.

PSCs.

Gestores del proyecto del MPR.

Proveedores de servicios e infraestructura base para solicitar su asistencia ante incidencias o actuaciones preventivas en los sistemas.

4.3.1 Descripción de actuaciones de soporte y atención a usuarios.

Las principales funciones, desempeñadas por el Servicio de Soporte @firma, son las siguientes:

Recepción de solicitudes a través de todos los canales de entrada establecidos.

Por teléfono a través del número 902 93 44 05.

Por e-mail a la dirección soporte.afirma5@mpr.es

Registro y clasificación de incidencias y peticiones en función de su tipología y asignación de prioridades.

Evaluación, investigación y diagnóstico de las incidencias y peticiones.

Escalado funcional a los diferentes niveles de soporte.

Escalado jerárquico, de manera que los diferentes niveles de responsabilidad de las organizaciones implicadas posean visibilidad de los casos más relevantes y puedan tomar las acciones necesarias para minimizar el impacto de dichas incidencias.

Realizar el seguimiento de las incidencias y peticiones a lo largo de todo su ciclo de vida, hasta su cierre y verificación, manteniendo a los usuarios informados respecto del estado y el grado de progreso de sus incidencias/peticiones.

Generar informes de gestión:

Llamadas o peticiones recibidas, atendidas y abandonadas.

Incidencias y peticiones cerradas y abiertas.

Alcance de los niveles de servicio.

4.3.2 Disponibilidad.

El servicio de soporte debe estar acorde con el del sistema, y por tanto, ha de ser continuo, 24 × 7. Igualmente, al tratarse de un servicio electrónico, es fundamental que se habiliten los canales de interacción electrónicos, al menos a través de e-mail.

La atención por los canales electrónico y telefónico será la del sistema, 24 × 7, considerándose una funcionalidad crítica del sistema global. Se suministrará la información necesaria para facilitar la integración a los organismos requirentes de los servicios, y llevan a cabo las actuaciones de soporte y mantenimiento correctivo o evolutivo correspondiente.

Se presta el servicio por el canal telefónico con las siguientes características:

De 9:00 h a 19:00 h de lunes a viernes en días laborables, ininterrumpido con atención telefónica y vía e-mail personalizada. Se incluyen festivos no nacionales con este horario.

cve: BOE-A-2010-17147

De 19:00 a 9:00, fines de semana y festivos nacionales, manteniendo atención telefónica personalizada para la resolución de incidencias operativas de gran impacto que afecten a la disponibilidad de los servicios.

El parámetro de calidad del servicio será el grado de atención de cada canal, medido como porcentaje de mensajes y llamadas atendidas, consideradas así aquellas que entran en el sistema y alcanzan a un operador, independientemente de su resultado. El objetivo a alcanzar en cada canal es el siguiente:

Canales e-mail y web, la misma disponibilidad que el sistema, será el 98 %.
Canal telefónico, tanto en atención personal, como por buzón de voz (llamadas atendidas por el buzón), será:

Porcentaje mínimo de llamadas totales atendidas será superior al 95 %.
Tiempo de espera del 90 % de las llamadas atendidas no será superior a 30 segundos.
Tiempo de espera del 98 % de las llamadas atendidas no será superior a 60 segundos.

4.3.3 Solicitudes de soporte de los organismos.

Las solicitudes de soporte se clasificarán en función de su impacto en el servicio según el apartado 4.1 y se categorizarán de la forma siguiente:

Incidencias. El organismo solicitante identifica un defecto o fallo que afecta al sistema en general o a alguna funcionalidad. Los tipos de incidencias contemplados inicialmente serán:

Tipología de Incidencias		
Tipología Nivel 1	Tipología Nivel 2	Tipología Nivel 3
Incidencia	Acceso	Conectividad IP. Servicios Plataforma. Prestadores. Otros.
	Protocolos	OCSP. XMLSOAP. Servicios Web. ValidarCertificado. ObtenerInfoCertificado. Validar firma. Cliente firma. Errores y excepciones. Otros.
	Plataforma	HW. SW Base. Aplicaciones. Otros.

Peticiones de Servicio. El organismo emisor solicita información o ayuda para la integración, alta aplicaciones, etc., o se trata de una solicitud que le afecta particularmente a su implementación (mensajes de ws, excepciones en certificados...) dentro del funcionamiento establecido. Los tipos de peticiones contemplados inicialmente serán:

cve: BOE-A-2010-17147

Tipología de peticiones de servicio		
Tipología Nivel 1	Tipología Nivel 2	Tipología Nivel 3
Petición de servicio	Alta/Baja/Modif.	Dirección IP. Aplicación. IP y Aplicación. organismo. Contactos. Lista de distribución @firma. Otros.
	Consultas	Documentación. Protocolos. Herramientas desarrollo. Certificados. Prestadores. Plataforma @firma. eDNI. Smartcard y lectores. Otros.
	Solicitudes	Documentación. Packs Certificados. Aplicaciones Cliente Ejemplo. Pruebas URLs. Pruebas eDNI. Envío de información masiva a toda la lista de contactos. Información integración de nuevos organismos. Informes (estadísticas/incidencias). Otros.
	Reclamaciones	Incidencias. Peticiones. Acceso Plataforma. Acceso Servicios Plataforma. Soporte @firma. Otros.

Ampliaciones o modificaciones del servicio. Se habilitará un procedimiento de gestión del cambio específico para tratar estas solicitudes, no sujeto a este acuerdo de nivel de servicio.

Los parámetros de calidad se establecen midiendo el tiempo medio de resolución de cada tipo de peticiones, esto es, desde que se registra en el centro de soporte y atención a usuarios (si no había sido identificada con anterioridad) hasta que se resuelve.

Los objetivos de calidad son:

Incidencias. Según su clasificación anterior. Ver punto 4.1

Peticiones de Servicio. Tiempo medio de resolución de todas las consultas no será superior a 24 horas. Si llegaran a 48 horas por retrasos de terceros (eje: habilitar acceso por ip a aplicaciones), se llevaría a cabo un mecanismo de emergencia.

cve: BOE-A-2010-17147

Parámetros Generales del ANS Canales	Niveles de servicio
Disponibilidad:	
Por e-mail	98 %
Por teléfono	95 % del total 90 % en menos de 30 seg. 98 % en menos de 60 seg.
Consultas:	
Por e-mail	Menor a 24 horas.
Por teléfono	80 % del total en menos de 1 hora. 95 % del total en menos de 2 horas. 98 % del total en menos de 4 horas.

ANEXO IV

Servicio ofrecido por el MPR de dirección electrónica única y catálogo de procedimientos del servicio de notificaciones telemáticas seguras.

I. *Condiciones generales*

1. Objeto.–El artículo 12 del Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado establece que «todo interesado que manifieste su voluntad de ser notificado por medios telemáticos en cualesquiera procedimientos deberá disponer, con las condiciones que se establezcan, de una dirección electrónica habilitada para ello, que será única para todas las posibles notificaciones a practicar por la Administración General del Estado y sus Organismos Autónomos».

La Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre, establece en su artículo segundo que «La titularidad de la dirección electrónica a partir de la cual se construyan las direcciones electrónicas habilitadas de los interesados, corresponde al Ministerio de la Presidencia.».

En aplicación de lo dispuesto en la normativa anteriormente citada, el Ministerio de la Presidencia (MPR) ha desarrollado un servicio de notificaciones telemáticas seguras y de dirección electrónica única para la Administración General del Estado, que es prestado en colaboración con la Sociedad Estatal Correos y Telégrafos, S.A. (CORREOS), gracias al Convenio de colaboración que ambas partes tienen suscrito con esta finalidad.

El MPR, con el objetivo de impulsar la implantación de la administración electrónica, quiere facilitar al Tribunal Constitucional la utilización del sistema de notificaciones telemáticas seguras y la Dirección electrónica habilitada para lo cual firma este anexo, sin menoscabo de que el Tribunal Constitucional pueda firmar convenio especifico con Correos.

El objeto del presente anexo es la regulación de los derechos y obligaciones que se establecen para la prestación, por parte del MPR, del Servicio de Dirección Electrónica Habilitada y Catálogo de procedimientos del Servicio de Notificaciones Telemáticas Seguras.

2. Alcance.

a) Los servicios ofrecidos por el Sistema de dirección electrónica única (DEH) y Catálogo de procedimientos, que garantizan el envío de notificaciones telemáticas de forma segura, son los siguientes:

Gestión de la DEH.
Gestión del catálogo de procedimientos. Publicación de procedimientos.
Gestión de la suscripción a procedimientos.

cve: BOE-A-2010-17147

b) Se habilita a cualquier aplicación informática de Tribunal Constitucional a utilizar los servicios citados en el punto anterior.

c) El Tribunal Constitucional podrá publicar los procedimientos a disposición del ciudadano en el catálogo de procedimientos y será su responsabilidad la actualización y descripción de los mismos.

d) Ambas partes se comprometen a comunicarse mutuamente cualquier medida de informatización que pueda afectar a la compatibilidad de la Dirección Electrónica Habilitada y a la publicación de los procedimientos a los que el ciudadano puede suscribirse.

3. Obligaciones del prestador del Servicio.–El MPR, como prestador del Servicio de Dirección Electrónica Habilitada y Catálogo de procedimientos, asume las siguientes obligaciones:

a) Velar por el buen funcionamiento del Servicio.

b) Disponer de un entorno de prueba para facilitar la integración al servicio.

c) Habilitar los mecanismos necesarios para que el usuario de los servicios pueda prestar asistencia de información y atención al ciudadano y el soporte necesario a los organismos.

4. Obligaciones del usuario de los Servicios.–El Tribunal Constitucional, como usuario del Servicio de Dirección Electrónica Habilitada y Catálogo de procedimientos, asume las siguientes obligaciones:

a) Facilitar a los ciudadanos los medios necesarios para obtener la dirección electrónica única.

b) Mantener el catálogo de sus procedimientos actualizados y facilitar a los ciudadanos información sobre los procedimientos a los que pueden suscribirse para ser notificados de manera telemática.

c) Prestar asistencia de información y atención al ciudadano y colaboración en la organización del Servicio de Notificaciones Telemáticas Seguras.

5. Acuerdo de calidad de los servicios.–Los servicios objeto del presente anexo estarán sujetos al Acuerdo de Nivel de Servicios que se adjunta en el apartado II de este anexo.

6. Coste asociado a la gestión de entrega de la notificación.–Los servicios prestados por el Servicio de Dirección Electrónica Habilitada y Catálogo de procedimientos del Servicio de Notificaciones Telemáticas Seguras del MPR se realizarán sin coste alguno conforme a la cláusula quinta del Acuerdo. Los costes asociados a la gestión de la entrega de la notificación (buzón, puesta a disposición, entrega, acuses de recibo, etc.), se inscribirán dentro de las relaciones entre Correos y Tribunal Constitucional.

7. Referencias.–El MPR podrá hacer públicas en cualquier lista de referencia de usuarios o en cualquier boletín de prensa publicado, y sin autorización previa, la relación de organismos usuarios de los servicios a los que hace referencia el presente anexo.

El Tribunal Constitucional podrá referenciar la utilización de dichos servicios sin autorización previa por parte del MPR.

8. Contactos de referencia.–La resolución de consultas técnicas relacionadas con la utilización de los servicios así como las de carácter administrativo relativas al alcance del presente anexo de prestación de servicios se ofrecerá a través de los siguientes contactos de referencia.

cve: BOE-A-2010-17147

Servicio	Dirección Electrónica Única y Catálogo de procedimientos
Oferente del servicio.	Ministerio de la Presidencia.
Responsable Técnico del Servicio.	Directora de la División de Proyectos de Administración Electrónica Teléfono: 91 2732461. Correo electrónico: sgprotec@map.es. Dirección postal: María de Molina, 50, 9.ª planta. 28071 – Madrid.
Responsable Administrativo del anexo.	José Luis Redondo Pérez. Vocal Asesor de la Dirección General para el Impulso de la Administración Electrónica. Teléfono: 91 2732463. Correo electrónico: joseluis.redondo@map.es. Dirección postal: María de Molina, 50, 9.ª planta. 28071 – Madrid.

II. *Acuerdo de nivel de Servicios (ANS)*

Este ANS contempla tanto parámetros propios del servicio, como los de soporte a los interesados y organismos emisores para la resolución de consultas e incidencias y los referentes a la propia gestión e información del ANS.

El ANS será el recogido en el convenio vigente entre MPR y Correos.

cve: BOE-A-2010-17147