

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.

7.3.3 Solicitudes de soporte de los organismos.-Las solicitudes de soporte se clasificarán en función de su impacto en el servicio según el apartado 7.1 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.	OCSF. XMLSOAP. Servicios Web. 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:

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 Cambio de Domicilio. Otros.
	Consultas.	Documentación. Protocolos. Herramientas desarrollo. Certificados. Versiones SCSP Soportadas. Otros.
	Solicitudes.	Documentación. Packs Certificados. Aplicaciones Cliente Ejemplo. 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. 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.

Parámetros generales del ANS. Canales	Niveles de servicio
Disponibilidad:	
Por eMail	98%
Por teléfono	95% del total. 90% en menos de 30 seg. 98% en menos de 60 seg.
Consultas:	
Por eMail	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.

9963

RESOLUCIÓN de 22 de mayo de 2008, de la Secretaría de Estado para la Administración Pública, por la que se publica el Convenio de colaboración, entre el Ministerio de Administraciones Públicas y la Comunitat Valenciana, 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.

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.

La cooperación entre el Ministerio de Administraciones Públicas y la Generalitat de la Comunidad Valenciana ha venido desarrollándose desde hace tiempo en la búsqueda de soluciones tecnológicas que faciliten la prestación de servicios a los ciudadanos por esta vía, la eficiente utilización de los recursos públicos y la simplificación en la tramitación administrativa.

Con fecha 12 de marzo de 2008 se formalizó un Convenio de colaboración entre el Ministerio de Administraciones Públicas y la Generalitat de la Comunidad Valenciana 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.

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, la Comunidad Autónoma podrá acceder a los servicios ofrecidos por el Ministerio de Administraciones Públicas 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, la Comunidad Autónoma podrá disponer del servicio prestado por el Ministerio de Administraciones Públicas 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.

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 Administración Pública dispone su publicación en el «Boletín Oficial del Estado».

Madrid, 22 de mayo de 2008.—La Secretaria de Estado para la Administración Pública, Mercedes Elvira del Palacio Tascón.

CONVENIO DE COLABORACIÓN ENTRE EL MINISTERIO DE ADMINISTRACIONES PÚBLICAS Y LA GENERALITAT DE LA COMUNITAT VALENCIANA PARA LA PRESTACIÓN MUTUA DE SERVICIOS DE ADMINISTRACIÓN ELECTRÓNICA

En Madrid a 12 de marzo de 2008.

REUNIDOS

De una parte, Doña Elena Salgado Méndez, en su calidad de Ministra de Administraciones Públicas, 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.

De otra parte, Don Francisco Camps Ortiz, President de la Generalitat, en representación la Generalitat de la Comunidad Valenciana, y en el ejercicio de las competencias atribuidas mediante el artículo 10 c) de la Ley 5/1983, de 30 de diciembre, de Gobierno Valenciano, facultado para la firma del presente convenio mediante Acuerdo del Consell de fecha 28 de septiembre de 2007, de acuerdo con lo dispuesto en el artículo 17 f) de la Ley 5/1983 del Consell y lo previsto por el artículo 2.º 2 del Decreto 20/1993, por el que se regula el Registro de Convenios y se establece el régimen jurídico-presupuestario de los convenios que suscriba la Generalitat.

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

EXPONEN

1.º Que tanto el Ministerio de Administraciones Públicas (MAP) como la Generalitat de Comunitat Valenciana 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.

2.º Que asimismo, tienen entre sus competencias 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 y las empresas.

3.º Que las partes están de acuerdo en impulsar la prestación de servicios en línea al ciudadano que permitan 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 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 las Administraciones Públicas, el presente acuerdo resulta de especial utilidad para las dos Administraciones.

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

CLÁUSULAS

Primera. *Objeto.*—El presente Convenio 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 Convenio 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 Convenio podrán acceder a las funcionalidades proporcionadas por los servicios relacionados en los anexos al presente Convenio que a continuación se especifican:

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

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

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

Tercera. *Reciprocidad.*—Los servicios sujetos al presente Convenio 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 como oferentes de servicios, como 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 Convenio 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 General para la Administración Pública del MAP y dos miembros designados por el titular de la Conselleria de Justicia y Administraciones Públicas de la Generalitat de la Comunitat Valenciana, 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 trimestre 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 Convenio.

Corresponde a la Comisión Técnica de Seguimiento resolver los problemas de interpretación y cumplimiento que se deriven del presente Convenio, 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 Convenio.

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

Sexta. *Plazo de duración del Convenio.*—El presente Convenio comenzará su vigencia a partir del día de su firma y tendrá una duración de tres años. El Convenio 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 Convenio.*—Cualquiera de las partes podrá proponer la revisión de este Convenio en cualquier momento para introducir las modificaciones que se estimen pertinentes. De producirse la revisión del clausulado del Convenio, 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 Convenio.

Octava. *Régimen Jurídico.*—El presente Convenio tiene la naturaleza de los previstos en el artículo 3.1 c) del Texto Refundido de la Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto Legislativo 2/2000, de 16 de junio. Este convenio se regirá por las disposiciones contenidas en la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en concreto por lo dispuesto en los artículos 6 y 8 de esta Ley.

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

Ambas partes podrán resolver el convenio por ineficacia sobrevenida o incumplimiento grave de sus respectivas obligaciones establecidas en las cláusulas tercera y cuarta de los anexos del presente convenio.

Las cuestiones litigiosas que surjan entre las partes durante el desarrollo y ejecución del presente Convenio 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 Convenio en dos ejemplares y a un solo efecto, en el lugar y fecha señalados en el encabezamiento.—La Ministra de Administraciones Públicas, Elena Salgado Méndez.—El President de la Generalitat, Francisco Camps Ortiz

ANEXO I

Servicio de conexión a la Red SARA

I. CONDICIONES GENERALES

1. Objeto

El Ministerio de Administraciones Públicas (MAP), en colaboración con las Comunidades Autónomas, ha desarrollado la red SARA (Sistemas, Aplicaciones y Redes para las Administraciones), 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.

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 de la Generalitat de la Comunitat Valenciana y que es instalada, administrada y mantenida por el MAP.

(iii) El AC comunica de manera segura la Red Corporativa de la Generalitat de la Comunitat Valenciana con las redes corporativas de otras Administraciones y entidades públicas conectadas a la red SARA (Extranet), con la Intranet Administrativa de la Administración General del Estado y con la Red TESTA II de la Comisión Europea.

(iv) Se habilita a cualquier aplicación informática de la Generalitat de la Comunitat Valenciana y de la Administración General del Estado, así como a sus entidades de derecho público vinculadas o dependientes, 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 MAP

El MAP, como responsable de la Red SARA asume las siguientes obligaciones:

(i) Instalar, administrar y mantener un enlace para la comunicación y el AC de la Generalitat de la Comunitat Valenciana ubicado en las dependencias que ésta determine y que mejor permitan la conexión con su correspondiente Red Corporativa.

(ii) Proporcionar la documentación técnica correspondiente a la arquitectura y configuración de los sistemas que componen el AC de la Generalitat de la Comunitat Valenciana

(iii) Mantener un servicio de soporte 24x7 para garantizar la continuidad del servicio del AC, Punto Neutro e Intranet Administrativa de la Administración General del Estado 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.

(iv) Habilitar y gestionar un Portal de Administradores que sirva como espacio para facilitar información a los responsables técnicos de la Generalitat de la Comunitat Valenciana 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 de la Generalitat

(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 SARA permitiendo al MAP el acceso de lectura y monitorización de los mismos, con independencia de que estas tareas sean realizadas por Generalitat de la Comunitat Valenciana o por su operador.

(iii) Garantizar condiciones adecuadas en la ubicación, condiciones medioambientales, suministro eléctrico, cableado, etc, del AC con el fin de asegurar la continuidad del servicio.

(iv) Mantener un servicio de soporte, a ser posible 24x7, para garantizar la continuidad del servicio en el enlace de comunicaciones y los elementos activos del mismo, así como de los elementos ajenos al MAP. Para ello se facilitarán al MAP los contactos, tanto de los responsables de la conexión a SARA en la Comunitat Valenciana, como los del Centro de Soporte, CAU o equivalente.

(v) Colaborar con el MAP 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.

(vi) Facilitar y promover el acceso a la Red SARA de las Diputaciones Provinciales y/o Ayuntamientos de su ámbito territorial, con la tecnología, mecanismos y procedimientos que estos acuerden, así como a garantizar la continuidad del servicio en la parte que le corresponda.

(vii) Colaborar con el MAP 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 contingencias. Dicho catálogo permitirá la difusión de los servicios a los usuarios de SARA, facilitará la elaboración de estadísticas, cuadros de mandos, etc, que el MAP 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 MAP 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 Administraciones Públicas 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.

La Generalitat de la Comunitat Valenciana podrá referenciar la utilización de la red SARA sin autorización previa por parte del Ministerio de Administraciones Públicas.

7. Elementos de identificación

7.1 Identificación del centro de soporte de la Red SARA

Identificación: Centro de Soporte de la red S.A.R.A.

Responsable de la Unidad: Ignacio Martínez Arrieta, Subdirector General de Proceso de Datos de la A.P.

Responsable técnico: Jorge Fabeiro Sanz, Jefe de Servicio.

Horario de servicio: 24x7.

Localización: Ministerio de Administraciones Públicas, María de Molina, 50.

Gestión de incidencias:

9h a 17h30 de lunes a jueves: 912732032.

9h a 14h30 los viernes: 912732202. incidencias.ia@map.es

Fuera del horario laboral, sábados, domingos y festivos: 902013114-618586324

Observaciones.

7.2 Identificación del centro de soporte de la red de la Generalitat de la Comunitat Valenciana.

Identificación: Centro de Soporte de la Generalitat.

Responsable de la Unidad: Marlen Ripoll Aracil, Jefe del Servicio de Telecomunicaciones Corporativas y Certificación Electrónica.

Responsable técnico: Enrique Ballester Alpuente, Guillermo Castelló García.

Horario de servicio: 24x7.

Localización: CTSI -GVA, c/ General Elio, 2 entlo. 46010 Valencia.

Gestión de incidencias: CTSI -963985300 (24x7)

Observaciones.

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.

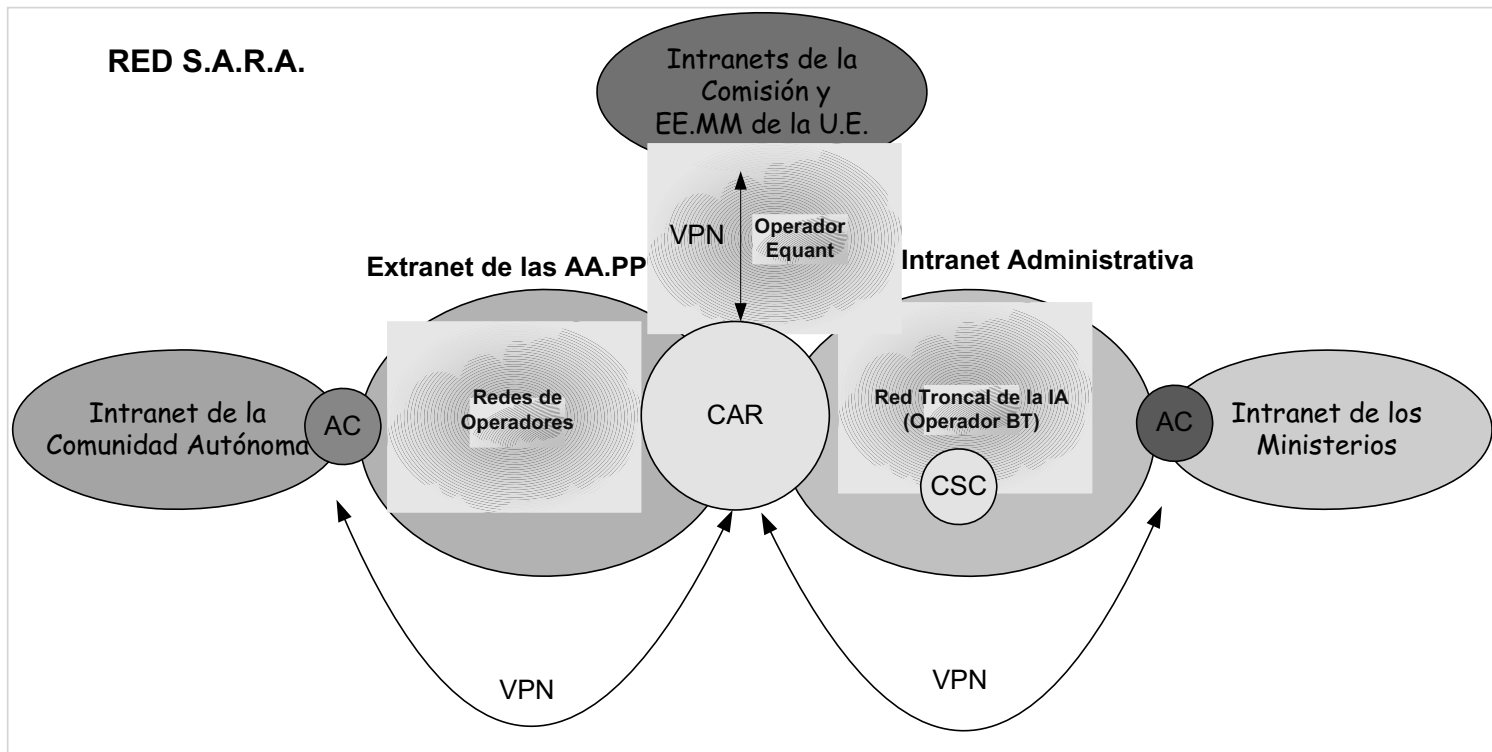
Observaciones.

II. CONDICIONES TÉCNICAS Y FUNCIONALES

1. Descripción del sistema

1.1 Descripción de la Red SARA y sus elementos de conexión.—La Red SARA está formada por la Intranet Administrativa, que hoy ofrece un amplio número de servicios que se prestan en cooperación en el ámbito de la Admi-

nistración General del Estado, sus elementos de incardinación en TESTA II, y los elementos de enlace con las Redes Corporativas de las Comunidades Autónomas conocido como Extranet de las Administraciones Públicas. TESTA II es la Red transeuropea que enlaza la Red Corporativa de la Comisión de la Unión Europea, con las de los Estados Miembros, para el soporte de intercambio de datos y cooperación en la prestación de servicios.



La interconexión a la Extranet se realiza a través de lo que se denomina Área de Conexión (AC).

Este AC responde básicamente al esquema de una zona desmilitarizada (DMZ) formada por un cortafuegos externo (que, en este caso, conecta con el resto de la red), un servidor donde residen los servicios básicos que se mencionan más adelante y un cortafuegos interno (hacia el interior de la Generalitat de la Comunitat Valenciana).

El sistema que actúa como cortafuegos externo será también el encargado, siempre que sea posible, de cerrar una VPN con el Centro de Acceso Remoto (CAR) de la Intranet Administrativa de la Administración General del Estado o con el AC de otro Organismo conectado directamente a la Red S.A.R.A. Este cortafuegos puede realizar igualmente funciones de NAT dinámico para las conexiones entrantes desde el resto de la Extranet hacia la Generalitat de la Comunitat Valenciana).

Por su parte, el sistema que actúa como cortafuegos interno puede realizar también funciones de NAT contra destinos situados en el interior de la Generalitat de la Comunitat Valenciana).

1.2 Descripción de los elementos que componen el área de conexión de la Generalitat de la Comunitat Valenciana.

Router externo: este elemento conecta con la línea que une con la Red Troncal de la Extranet de las AA.PP.

Conmutador LAN: para el conjunto de conexiones LAN de los elementos que componen la solución. Se configuran tres VLAN para separar el tráfico correspondiente a tres zonas:

Tráfico entre el router y el firewall externo (VLAN externa).

Tráfico de la propia AC (VLAN DMZ).

Tráfico hacia el interior de la Generalitat de la Comunitat Valenciana.

Cluster externo: formado por dos servidores en una configuración activo-activo. En condiciones normales los sistemas prestan las funcio-

nes que se describen a continuación; en degradado, cualquiera de ellos puede suministrar ambas funciones:

Cortafuego externo: cumple las funciones de cortafuegos y cierre de VPNs. Reside en un servidor Linux utilizándose productos de licencia GPL para cumplir estas funciones.

Servidor para los servicios de la Extranet: en él residen los servicios básicos de la Extranet de las AAPP que haya que implementar. Los servicios instalados son DNS, correo, proxy, servidor web, servidor socks y servidor NTP. También en este caso se trata de un servidor Linux con productos bajo licencia GPL.

Cluster interno: formado por dos servidores en una configuración activo-pasivo. Las funciones que cumplen son:

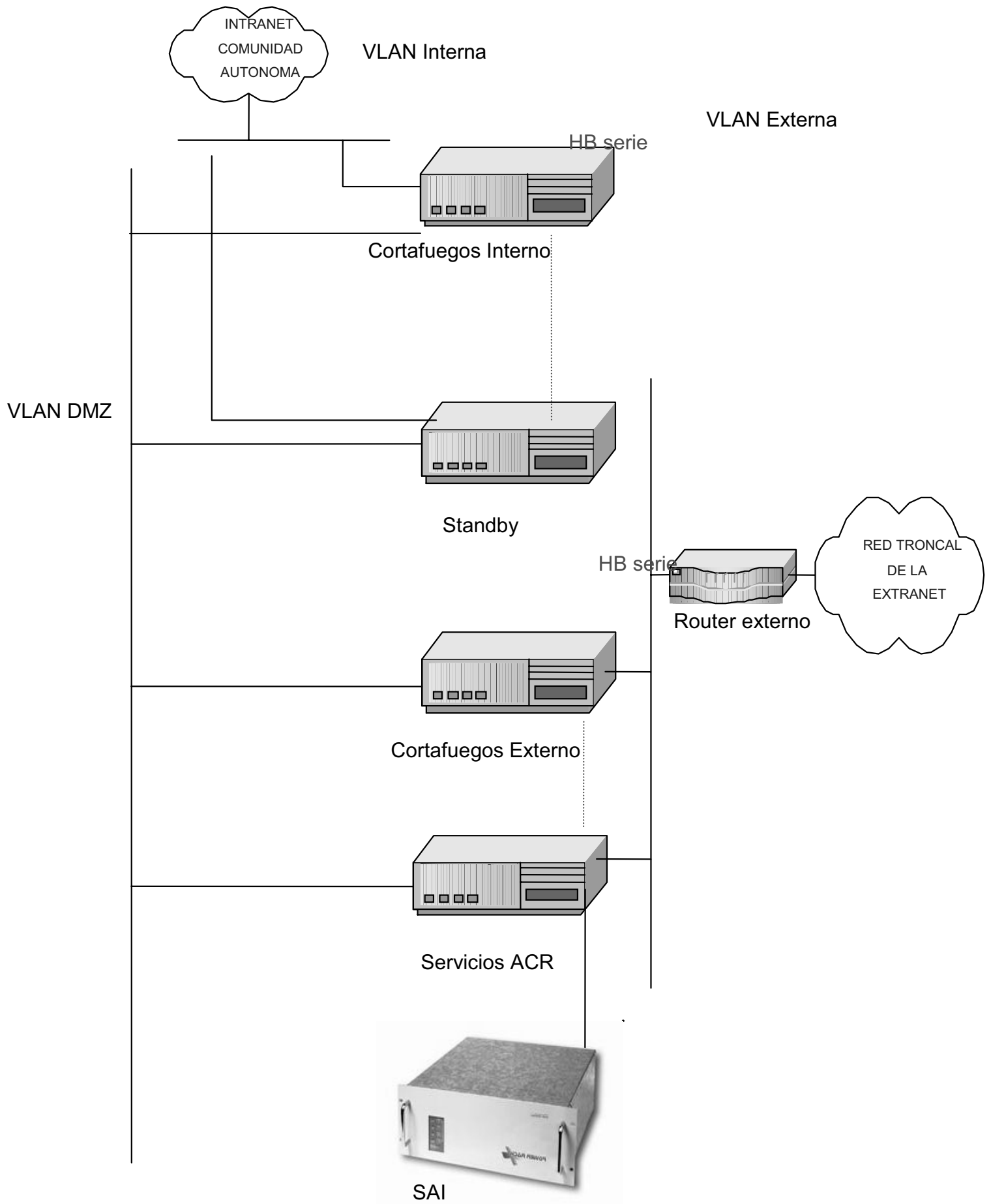
Cortafuego interno: cumple las funciones de cortafuegos y NAT hacia el interior del organismo. Reside en un servidor Linux y se utilizan productos con licencia GPL.

Servidor de backup: es el nodo pasivo del cluster. En caso de fallo del nodo activo los servicios de cortafuego interno basculan a este servidor.

Sistema de alimentación ininterrumpida (SAI): para mejorar la disponibilidad de los elementos en caso de cortes de alimentación. Este elemento estará conectado a uno de los servidores que actúa como maestro y es capaz de controlar a agentes disponibles en los otros servidores. Se instalará siempre que sea posible.

Armario de media altura (rack): todos los elementos de la solución se integran en un único armario de media altura. Se instalará siempre que sea posible.

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



1.3 Características físicas de los elementos.—Los sistemas a implantar en las dependencias que la Generalitat de la Comunitat Valenciana determine incorpora un armario básico para montaje en Rack de todos los elementos, apoyan directamente en el suelo y disponen de las siguientes dimensiones:

Ancho: 610 mm.
Alto: 1.200 mm.
Profundo: 1.000 mm.
Peso Máximo: 300 Kg.

1.4 Instalación eléctrica.—Será efectuada siempre de acuerdo con las especificaciones del Reglamento Electrotécnico para Baja Tensión e Instrucciones Complementarias (Decreto 2413/1973 de 20 de Septiembre).

Para garantizar un correcto funcionamiento del equipo, es necesario respetar las siguientes condiciones de alimentación eléctrica:

Tensión de alimentación: 220V (+6 -10 %).
Frecuencia de alimentación: 50Hz (+3 -3 %).
Distorsión armónica total: < 5%.

Tolerancia a micro-cortes sin perturbación en el funcionamiento, duración: < 20 ms.

Potencia armario AC: 3500 W.

La potencia indicada es la correspondiente a la ocupación del armario según la configuración prevista.

1.5 Condiciones de ambiente.—Los servidores actuales de gama media, no requieren una instalación específica de aire acondicionado ya que está diseñado para trabajar dentro de un ambiente de oficina, en condiciones de confort establecidas para el personal. No obstante, por las propias condiciones del recinto elegido, o bien en configuraciones grandes, puede ser necesaria la instalación de una consola de aire acondicionado.

Para asegurar la mayor fiabilidad en su funcionamiento se debe mantener el recinto dentro de los límites siguientes:

Temperatura comprendida entre 15 y 32 °C.
Temperatura óptima recomendada 22 °C.
Gradiente horario máximo T < 5 °C/h.
Humedad relativa entre 20 y 80 %.
Humedad relativa óptima recomendada 50%.
Gradiente horario máximo HR < 10% /h.

En general al elegir el local para la instalación del equipo, se tendrá en cuenta que sea lo más limpio posible, evitar la radiación directa del sol sobre los elementos, y que sea espacioso para que no se produzca una acumulación excesiva del calor disipado.

Cuando sea necesario recurrir a la instalación de aire acondicionado, se tendrá en cuenta que el desprendimiento térmico máximo del conjunto de los elementos instalados dentro del armario: Cabinet AC. 7.000 Btu/h.

1.6 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 Extranet: DNS, relay SMTP, WWW, PROXY y NTP (sincronizado con el Real Observatorio de la Armada del Ministerio de Defensa).

ANEXO II

Servicios ofrecidos por el MAP para la verificación de datos de identidad y de residencia de un ciudadano

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 MAP, de los servicios de Verificación de Datos de Identidad y Verificación de Datos de Residencia a la Comunitat Valenciana

En el ámbito de la Administración General del Estado, el pasado 28 de abril del 2006, se aprobaron dos Reales Decretos con relación a los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes:

El R.D. 522/2006, por el que se suprime la aportación de fotocopias de documentos de identidad, y

El R.D. 523/2006, por el que se suprime la exigencia de aportar el certificado de empadronamiento, como documento probatorio del domicilio y residencia.

En estos reales decretos se establece que dichos documentos podrán ser sustituidos por una consulta al Sistema de Verificación de Datos de Identidad (SVDI) y al Sistema de Verificación de Datos de Residencia (SVDR) cuya regulación se establece respectivamente en la

Orden PRE/3949/2006, de 26 de diciembre, y la Orden PRE/4008/2006, de 27 diciembre.

Dado el interés por parte del resto de Administraciones Públicas en desarrollar los elementos normativos y técnicos equivalentes para poder eliminar la obligación de aportar los citados documentos, se establece la oportunidad de utilizar los servicios desarrollados por el MAP para la Verificación de Datos de Identidad y Verificación de Datos de Residencia.

2. Alcance

La aplicación de este Anexo habilita a cualquier aplicación informática de los órganos o entidades dependientes de Generalitat de la Comunitat Valenciana a utilizar el SVDI y el SVDR para verificar los datos de identidad y de residencia de los ciudadanos en los términos que se desarrollan más adelante.

3. Obligaciones del prestador del servicio

El MAP, como prestador del SVDI y del SVDR, asume las siguientes obligaciones:

(i) Poner a disposición de la Generalitat de la Comunitat Valenciana los servicios de verificación y consulta de datos de identidad y de residencia de un ciudadano.

(ii) 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.

(iii) Habilitar los mecanismos para ofrecer el soporte necesario a los equipos de integración y desarrollo de la Comunitat Valenciana 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 auditabilidad de las operaciones realizadas que permitan certificar el no repudio de las transacciones.

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

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

4. Obligaciones del beneficiario de los servicios

La Generalitat de la Comunitat Valenciana, como beneficiaria del SVDI y del SVDR, se compromete a:

(i) Realizar las labores de conectividad y despliegue pertinentes para poder acceder desde sus propias dependencias o instalaciones a los SVDI y a los SVDR a través del Sistema de Aplicaciones y Redes para las Administraciones (S.A.R.A) desarrollado por el MAP.

(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 MAP 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) Designar a un responsable, que será el encargado de autorizar los accesos en el ámbito de la Generalitat de la Comunitat Valenciana, y comunicar su nombramiento y cese al Ministerio de Administraciones Públicas.

(v) Coordinar con el MAP los procesos de administración de aplicaciones y sistemas usuarios de los SVDI y SVDR, suministrando al MAP la información requerida para dar de alta tanto a empleados públicos como aplicaciones informáticas usuarias de los servicios.

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. Referencias

El MAP podrá hacer públicas en cualquier lista de referencia de beneficiarios o en cualquier boletín de prensa publicado, y sin autorización previa, la relación de organismos usuarios de los servicios.

La Generalitat de la Comunitat Valenciana podrá referenciar la utilización de dichos servicios sin autorización previa por parte del MAP.

7. 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 Administraciones Públicas.

Responsable Técnico del Servicio: Director de la División de Proyectos Tecnológicos para la AGE.

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 de Modernización Administrativa.

Teléfono: 91 2732463. Correo electrónico: joseluis.redondo@map.es

Dirección postal: María de Molina, 50, 9.ª planta

II. CONDICIONES TÉCNICAS Y FUNCIONALES DEL SISTEMA DE VERIFICACIÓN DE DATOS DE IDENTIDAD Y RESIDENCIA

1. Descripción de los sistemas de verificación de datos de identidad y de residencia

El Sistema de Verificación de Datos de Identidad puesto a disposición de las Administraciones Públicas por parte del Ministerio de Administraciones Públicas se establece como servicio horizontal para la consulta y comprobación de los datos del Documento de Identificación del Ciudadano custodiados por la Dirección General de la Policía y de la Guardia Civil en base a lo dispuesto en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, que atribuye al Cuerpo Nacional de Policía, la función de expedición del Documento Nacional de Identidad y el control de entrada y salida del territorio nacional de españoles y extranjeros. Esta información se encuentra registrada y custodiada en los ficheros de la Dirección General de la Policía y de la Guardia Civil, quienes soportan la gestión del Documento Nacional de Identidad y de la Tarjeta de Identificación de Extranjeros (sus denominaciones, conforme a las Órdenes INT/1751/2002, de 20 de junio e INT/2190/2006, de 19 de junio, son ADDNIFIL y ADEXITTRA, respectivamente).

El Sistema de Verificación de Datos de Residencia puesto a disposición de las Administraciones Públicas por parte del Ministerio de Administraciones Públicas se establece como servicio horizontal para la consulta y comprobación de los datos sobre residencia de los ciudadanos mediante el acceso a los padrones municipales coordinados por el Instituto Nacional de Estadística, en base a lo dispuesto en la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, en relación con el Padrón Municipal, en la que se atribuye al Instituto Nacional de Estadística, entre otras, la función de coordinación de los distintos padrones municipales. Esta información se encuentra registrada y custodiada en los ficheros del Instituto Nacional de Estadística registrados en la Agencia de Protección de Datos con la denominación «PADRONES MUNICIPALES», conforme a la Orden ECO/143/2002, de 10 de enero, publicada en el BOE 26, de 30 de enero de 2002.

2. Adopción de medidas de seguridad, organizativas o técnicas del acceso a los sistemas de verificación de datos de identidad y residencia

2.1 Con carácter general los organismos que accedan a los Sistema de Verificación de Datos de Identidad y Residencia 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 994/1999, de 11 de junio.

3. Acceso a los sistemas de verificación de datos de identidad y residencia

3.1 El acceso a los Sistemas de Verificación de Datos de Identidad y Residencia 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.

3.2 Los Sistemas de Verificación de Datos de Identidad y Residencia presentarán dos formas de acceso para realizar las correspondientes consultas sobre la identidad y el lugar de domicilio y residencia de un ciudadano:

Un interfaz accesible a través de un navegador de Internet, conforme al RFC 2616: Protocolo de Transferencia de Hipertexto-HTTP/1.1 o superior, del IETF, donde un empleado público, debidamente acreditado e identifi-

cado, podrá realizar consultas con sólo disponer de un navegador con acceso a SARA y firma electrónica.

Un interfaz automatizado de servicio web, conforme al estándar WSDL 1.1 o superior del W3C cuya definición inicial, y sucesivas actualizaciones, serán puestas a disposición de los departamentos y organismos a través del Consejo Superior de Administración Electrónica y su Comisión Permanente.

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

4.1 Los accesos a los Sistemas de Verificación de Datos de Identidad y Residencia se efectuarán utilizando certificados electrónicos reconocidos que cumplan la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 95948 de 1997).

4.2 No podrán utilizarse certificados electrónicos caducados o revocados para acceder a los Sistemas de Verificación de Datos de Identidad y Residencia.

5. Requisitos de confidencialidad de los sistemas de verificación de datos de identidad y residencia

5.1 El Sistema de Verificación de Datos de Identidad ofrecerá consultas en las que, a partir del Número del Documento de Identificación del Ciudadano o Extranjero, se devolverá el total, o un subconjunto, de los datos incorporados en dicho documento:

Nombre y apellidos del titular del documento.
Lugar y fecha de nacimiento.
Nombre de los padres.
Sexo.
Estado de vigencia del Documento.

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

5.2 El Sistema de Verificación de Datos de Residencia, a partir del Número del Documento de Identificación del Ciudadano y/o de un conjunto de datos personales suficientes para identificar unívocamente al mismo, devolverá el total, o un subconjunto de los datos referentes al domicilio y residencia asociados a un ciudadano:

Provincia.
Municipio.
Entidad Colectiva.
Entidad Singular.
Núcleo.
Dirección (Vía, Kmt, Número, Número Superior, Bloque, Portal, Escalera, Planta, Puerta).

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 ningún ciudadano.

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

5.3 En la Generalitat de la Comunitat Valenciana existirá un responsable o administrador delegado de los Sistemas que determinará los usuarios de su administración que tienen acceso a los mismos y los datos que pueden obtener.

5.4 Para realizar la consulta a los Sistemas de Verificación de Datos de Identidad y Residencia, será preciso el consentimiento del interesado 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.

5.5 La consulta y el acceso a la información proporcionada por los Sistemas de Verificación de Datos de Identidad y Residencia 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 los sistemas de verificación de datos de identidad y residencia

Todas las consultas que se realicen a los Sistemas de Verificación de Datos de Identidad y Residencia, 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 los Sistemas de Verificación de Datos de Identidad y Residencia deban realizar a la Dirección General de la Policía, al Instituto Nacional de Estadística o a otros organismos con capacidad de informar sobre la identidad o la residencia de los ciudadanos, 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 de ambos organismos.

7. *Requisitos de disponibilidad de la información proporcionada por los sistemas de verificación de datos de identidad y residencia*

Los Sistemas de Verificación de Datos de Identidad y Residencia estarán disponibles los 7 días de la semana las 24 horas del día.

8. *Garantías jurídicas de los sistemas de verificación de datos de identidad y residencia ante posibles recursos*

8.1 Los servicios web proporcionados por estos sistemas siguen 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 Los Sistemas de Verificación de Datos de Identidad y Residencia dispondrán de un módulo de auditoría, en el que quedarán registradas todas las consultas de datos de residencia 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 los Sistemas de Verificación de Datos de Identidad y Residencia se hará uso del Servicio de Sellado de Tiempo de la Plataforma de Firma Electrónica del Ministerio de Administraciones Públicas, sincronizada con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio de la Armada como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

8.4 Sólo personal de la Administración Pública debidamente autorizado y acreditado podrá acceder a las funcionalidades de auditoría de los Sistemas de Verificación de Datos de Identidad y Residencia.

9. *Condiciones de la prestación del servicio*

9.1 La gestión de los Sistemas de Verificación de Datos de Identidad y Residencia corresponde al Ministerio de Administraciones Públicas.

9.2 Los órganos y organismos públicos de la Comunitat Valenciana 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 MAP a través de plataforma de validación y firma electrónica @firma

I. CONDICIONES GENERALES

1. *Objeto*

En el ejercicio de sus competencias el Ministerio de Administraciones Públicas (MAP) impulsa el uso de los servicios de certificación y firma electrónicos por ciudadanos y Administraciones Públicas. Para ello el MAP 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 MAP, de los servicios ofrecidos por su Plataforma de validación y firma electrónica.

2. *Alcance*

(i) El presente Anexo abarca un conjunto de servicios electrónicos que el MAP pone a disposición de la Generalitat de la Comunitat Valenciana con fines de identificación, validación o generación de firma electrónica.

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

- Validación de firmas y certificados electrónicos.
- 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 de los órganos o entidades dependientes de la Generalitat de la Comunitat Valenciana 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 de la Generalitat de la Comunitat Valenciana a suscribir un acuerdo particular de colaboración con los Prestadores de Servicio de Certificación emisores de los correspondientes certificados digitales con los que el MAP tenga firmado un Convenio de colaboración que recoja estas circunstancias. A estos efectos, el MAP facilitará la lista de Prestadores que incorporen esta facilidad.

En el caso de aquellos Prestadores de Servicios de Certificación con los que el MAP no tenga firmado un Convenio al respecto, y mientras no concurre esta circunstancia, la Generalitat de la Comunitat Valenciana deberá disponer de los preceptivos Acuerdos vigentes con cada Prestador.

3. *Obligaciones del prestador del servicio*

El MAP, como prestador de los servicios ofrecidos por la Plataforma de validación y firma electrónica, asume las siguientes obligaciones:

(i) Poner a disposición de La Generalitat de la Comunitat Valenciana, a través de la Autoritat de Certificació de la Comunitat Valenciana (ACCV) los servicios de validación y firma electrónica ofrecidos por la Plataforma de servicios basada en @firma versión 5.0 ó posteriores.

(ii) 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.

(iii) Habilitar los mecanismos para ofrecer el soporte necesario a los equipos de integración y desarrollo de la ACCV de la Generalitat Valenciana para la integración de sus aplicaciones con el servicio.

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

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

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

(vii) 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.

(viii) 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 beneficiario de los servicios*

La ACCV de la Generalitat Valenciana, como beneficiario de los servicios ofrecidos por la Plataforma de validación y firma electrónica, asume las siguientes obligaciones:

(i) 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 (S.A.R.A) desarrollado por el MAP.

(ii) Cooperar con el MAP 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)

(iii) Respetar la caracterización tecnológica definida por el MAP 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.

(iv) Concertar con el MAP 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.

(v) Seguir los procedimientos establecidos por el MAP 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 MAP 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 MAP que se adjunta en el apartado II de este Anexo.

6. Modificaciones y evolución de @firma

La Generalitat de la Comunitat Valenciana se convierte en miembro del Programa de Evolución Continua (PEC) de @firma, que se registrará 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 Convenio y a sus posteriores prórrogas.

La Generalitat de la Comunitat Valenciana 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.

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

7. Referencias

El MAP podrá incluir a la Generalitat de la Comunitat Valenciana, sin autorización previa, en cualquier boletín de prensa o lista de beneficiarios que haga referencia a los organismos usuarios de los servicios a los que hace referencia el presente Anexo.

La Generalitat de la Comunitat Valenciana podrá referenciar la utilización de dichos servicios sin autorización previa por parte del MAP.

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 Administraciones Públicas.

Responsable Técnico del Servicio: Ricardo Delgado Casanova, Subdirector General de Recursos Tecnológicos de la Administración General del Estado.

Teléfono: 91 27324 73. Correo electrónico: ricardo.delgado@map.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 de Modernización Administrativa.

Teléfono: 91 2732463. Correo electrónico: joseluis.redondo@map.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 MAP 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 MAP 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.

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 MAP.

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 MAP (modelo ASP o Application 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 MAP 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 MAP 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 MAP 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,

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.

4. Participantes

Los participantes acuerdan actuar de buena fe y cooperar en el seno del 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 MAP, 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 MAP y dos representantes de la Junta de Andalucía, que serán designados respectivamente por el Director General de Modernización Administrativa del MAP y por el Director General de Administración Electrónica y Calidad de los Servicios de la Junta de Andalucía.

Los representantes del MAP 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 MAP, 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 MAP.

Tanto la Junta de Andalucía como el Ministerio de Administraciones Públicas han sustentado los costes e inversiones necesarios para ofrecer los servicios de firma-e desde el MAP y culminar el desarrollo de la versión 5.0 del producto @firma y la prestación del servicio que en el se basa.

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.

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 MAP

1. *Objeto*

Según la ley 59/2003 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 Administraciones Públicas (MAP), 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 MAP 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.

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 MAP, como prestador de los servicios de validación y firma electrónica a través de su plataforma de servicios basada en @firma, se registrará 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 MAP.

El MAP 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 MAP, servicios de sistemas y comunicaciones, servicio de atención a usuarios, monitorización de sistemas, etc.

2. Calendario para la implantación del ANS

El MAP 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.

Periodo 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/m², 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 600x600 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 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.°C +/-5.°C 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 4x18 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 24x7 (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 que tienen programados los caminos de acceso permitidos al cliente. La entrada/salida es controlada por los vigilantes jurados del servicio de seguridad del edificio en 24x7 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 24x7 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 ruta

Parámetros generales del ANS		Niveles de servicio
Suministro de energía eléctrica segura		99,999%
Condiciones ambientales:		
Temperatura	22.°C +/-5.°C	99,90%
Temperatura	22.°C +/-8.°C	99,99%
Humedad	20% a 70%	99,90%

3.2 Comunicaciones.

3.2.1 Punto neutro de interconexión a S.A.R.A.—El acceso a los servicios de la Plataforma se realiza a través de S.A.R.A., 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 S.A.R.A., 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 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 x 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.

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 Back-ups.
- Inspección visual e identificación de alarmas.
- 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 24x7x365.

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 24x7 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 24x7 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: 24x7. Avisos <= 15 minutos.
Monitorización Preventiva.	Período: 24x7. Avisos <= 15 minutos.
Monitorización Avanzada.	Período: 24x7. Actuación procedimentada tras aviso <= 15 minutos.
Monitorización Internet. De dominios, portales y aplicaciones en Internet desde varias redes.	Período: 24x7. Avisos <= 15 minutos.

3.5 Copias de seguridad.-Se realiza un backup a dos niveles:

Backup Centralizado, consistente en la integración de los sistemas de la Plataforma en una red y plataforma de Backup basada en HP Data Protector.

Backup Remoto, consistente en la gestión de la plataforma de backup particular de los sistemas de la Plataforma.

La política aplicada es la siguiente:

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

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

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

Parámetros Generales del ANS	Niveles de servicio
Disponibilidad de servicios de backup y 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 interrumpen 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

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

Prioridad	Descripción	Tiempo máximo resolución
P1	Crítica	1 hora.
P2	Importante	8 horas.

Prioridad	Descripción	Tiempo máximo resolución
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:

Incidencias graves y leves: Horas laborables de lunes a domingo de 9,00 a 19:00 h.

Incidencias críticas: servicio 24 x 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 límites 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	100
		1	100
Arquitectura y configuración	5	3	92
		4	95
Plataforma Base	31	29	94
		28	92
Conectividad	21	21	100
		21	100
Servicios externos.	3		
		3	100
Conexión PSCs		3	100
TSA		3	100
Integración	4	4	100
		4	100
Total	292	287 284	98 97

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,

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 MAP.

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@map.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, 24x7. 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 electrónicos y telefónico será la del sistema, 24x7, 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 eMail personalizada. Se incluyen festivos no nacionales con este horario.

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. Validar Certificado. Obtener InfoCertificado. 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:

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.

Parámetros generales del ANS. Canales	Niveles de servicio
Disponibilidad:	
Por eMail	98%
Por teléfono	95% del total. 90% en menos de 30 seg. 98% en menos de 60 seg.
Consultas:	
Por eMail	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.

MINISTERIO DE CULTURA

9964

RESOLUCIÓN de 16 de mayo de 2008, del Instituto de la Cinematografía y de las Artes Audiovisuales, por la que se publica la concesión de ayudas para la organización y desarrollo en España de festivales y certámenes de cinematografía y artes audiovisuales durante el año 2008, correspondiente a la primera fase de la convocatoria.

En cumplimiento de lo dispuesto en el artículo 18 de la Ley 38/2003, de 17 de noviembre, General de Subvenciones, y en el apartado duodécimo, punto 4, de la Resolución de 20 de noviembre de 2007, de este Instituto, por la que se convoca la concesión de ayudas para la organización y desarrollo en España de festivales y certámenes de cinematografía y artes audiovisuales durante el año 2008 (Boletín Oficial del Estado de 8 de diciembre de 2007),

Esta Dirección General ha resuelto hacer pública la relación de beneficiarios de las ayudas concedidas, cuyo detalle se especifica en el anexo adjunto, correspondiente a la primera fase de la referida convocatoria.

Madrid, 16 de mayo de 2008.-El Director General del Instituto de la Cinematografía y de las Artes Audiovisuales, Fernando Lara Pérez.

ANEXO

Relación de beneficiarios y ayudas concedidas

Beneficiario	N.I.F.	Finalidad	Ayuda	Aplicación presupuestaria
Ayuntamiento de Lorca.	P-3002400-D	XII Festival «Primavera cinematográfica» de Lorca.	6.000,00	24.101.335C.460
Ayuntamiento de Medina del Campo.	P-4708600-D	XXI Semana de Cine de Medina del Campo.	21.000,00	24.101.335C.460
Ayuntamiento de Madrid.	P-2807900-B	V Festival Internacional de Documentales de Madrid.	15.000,00	24.101.335C.460
Total			42.000,00	24.101.335C.460
Promoción de la Ciudad de Las Palmas de Gran Canaria, S. A.	A-35250737	9.º Festival Internacional de Cine de Las Palmas de Gran Canaria.	18.000,00	24.101.335C.472
Great Ways Advertising, S. L.	B-82065590	9.ª Temporada de estrenos de cortometrajes «CORTOGENIA».	10.000,00	24.101.335C.472
Cooperativa Promotora de Medios Audiovisuales SCCL.	F-08310013	XVI Muestra Internacional de Films de Mujeres.	8.000,00	24.101.335C.472
Festival de Málaga e Iniciativas Audiovisuales, S. A.	A-92666049	XI Festival de Málaga-Cine Español.	50.000,00	24.101.335C.472
Total			86.000,00	24.101.335C.472