



Pliego de Prescripciones Técnicas

Procedimiento: Abierto, con varios criterios de adjudicación

Servicio de soporte de la nueva plataforma de Administración Electrónica de la CARM

Referencia: PAECARM-plies-180131-Soporte (1.1).doc

Creación: 12/04/2018

Consejería: Hacienda

CRI: Centro Regional de Informática

Servicio: Integración de Aplicaciones Corporativas





Índice de contenido

1	Objeto y valor estimado	3
2	Condiciones del equipo de trabajo	3
2.1	Lugar de realización de los trabajos y recursos vinculados al proyecto	3
2.2	Horario	4
2.3	Constitución inicial del equipo de trabajo	4
2.4	Modificaciones en la composición del equipo de trabajo	4
2.5	Formación del equipo de trabajo.....	5
2.6	Otras condiciones.....	5
3	Descripción técnica del servicio	6
3.1	Entorno funcional. Especificación de requisitos	6
3.2	Entorno tecnológico	15
3.3	Fases del contrato	17
3.4	Indicadores	18
4	Metodología a utilizar en la ejecución.....	19
5	Transferencia tecnológica	20
6	Documentación de los trabajos.....	20
7	Seguridad y confidencialidad de la información	20
7.1	Sistemas de información y tratamiento	20
7.2	Reglamento General de Protección de Datos	21
7.3	Esquema Nacional de Seguridad	24
7.4	Política de Seguridad	24
	Anexo I. Descripción de perfiles profesionales.....	26
-	Jefe de proyecto.....	26
-	Consultor.....	26
-	Analista	27
-	Analista-programador	27
	Anexo II. Cuestionario de personal	29
	Anexo III. Descripción del procedimiento de Integración Continua	31





1 Objeto y valor estimado

El objeto del contrato consiste en el soporte evolutivo, adaptativo, correctivo y perfectivo de la plataforma de Administración Electrónica implantada en la CARM debido a la ejecución del Plan Estratégico de Administración Electrónica de la CARM.

El valor estimado del contrato es de 4.675.968 euros IVA excluido, con el siguiente desglose:

- Contrato original: 1.520.640 euros IVA excluido
- Posible prórroga del contrato (hasta 3 años): 2.280.960 euros IVA excluido
- Posibles modificaciones al alza del precio del contrato: 304.128 euros IVA excluido
- Posible prórroga por un periodo máximo de nueve meses contemplada en el último párrafo del artículo 29.4 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (“...cuando al vencimiento de un contrato no se hubiera formalizado el nuevo contrato que garantice la continuidad de la prestación...”): 570.240 euros IVA excluido

2 Condiciones del equipo de trabajo

2.1 Lugar de realización de los trabajos y recursos vinculados al proyecto

Los trabajos serán realizados por el equipo de trabajo del adjudicatario en sus propias dependencias, salvo aquellas tareas que el responsable del contrato considere necesario que se realicen en dependencias de la Administración (como reuniones de seguimiento, puesta en marcha de servicios, periodos con previsión de gran número de incidencias,...), corriendo el coste de conexión con los entornos que proporcione la Dirección General de Informática, Patrimonio y Telecomunicaciones (en adelante, DGIPyT) a cuenta del adjudicatario. Dicha conexión remota deberá tener en cuenta, los criterios de diseño, seguridad y mantenimiento que el responsable del contrato dictamine durante la vigencia del mismo, que deberán ser asumidos por el adjudicatario y sus empresas contratadas. La DGIPyT tiene, dentro de su catálogo de accesos remotos para personal externo, los siguientes 3 modelos:

- Acceso VPN-SSL individual para técnicos externos, a través de plataforma Juniper SA600 propiedad de la CARM, con acceso a través de navegador, software Juniper Network Connect con uso de tarjeta criptográfica de usuario de la FNMT o DNI electrónico.
- VPN LAN2LAN, Túnel a través de Internet, con terminador de túneles CISCO ASA-5550.
- LAN2LAN a través de línea de datos dedicada, instalada y mantenida por el licitador. Esquema similar al anterior con una línea de datos entre la sede del licitador y el CPD corporativo de la CARM.





Cada trabajador del adjudicatario que vaya a acceder mediante conexión segura a la red de la Comunidad Autónoma de la Región de Murcia deberá firmar un documento de compromiso de confidencialidad y privacidad que le será facilitado por el responsable del contrato. Es condición necesaria para autorizar el acceso la firma de dicho documento.

2.2 Horario

Los trabajos se realizarán de lunes a viernes, de acuerdo con el horario que se establezca con el responsable del contrato dentro del rango comprendido entre las 7:30h y las 20:30h, cubriendo un máximo de 40 horas semanales.

Se deberá garantizar una atención mínima en la siguiente franja horaria:

Día	Ventana de servicio normal
Lunes	8:00 – 15:00, 16:00 – 20:00
Martes	8:00 – 15:00, 16:00 – 20:00
Miércoles	8:00 – 15:00, 16:00 – 20:00
Jueves	8:00 – 15:00, 16:00 – 20:00
Viernes	8:00 – 15:00, 16:00 – 20:00

El nivel de atención debe adaptarse a los periodos de menor y mayor carga del servicio (periodos vacacionales y periodos críticos como la apertura y cierre del ejercicio presupuestario, respectivamente).

2.3 Constitución inicial del equipo de trabajo

Se estima que, para la realización de los trabajos objeto de este pliego, se requiere la siguiente dedicación mínima:

Perfil	Jornadas (8 horas)
Jefe de proyecto	440
Consultor	1.320
Analista	2.200
Analista-programador	2.640

2.4 Modificaciones en la composición del equipo de trabajo

La valoración final de la productividad y calidad de los trabajos de las personas que realizan el servicio corresponde al responsable del contrato, siendo potestad suya solicitar el cambio de cualquiera de los componentes del equipo de trabajo, con un preaviso de quince





días, por otro de igual categoría, si existen razones justificadas que lo aconsejen. La persona sustituta ha de tener una cualificación igual o superior a la de la persona sustituida.

Los posibles inconvenientes de adaptación al entorno de trabajo y al proyecto debidos a las sustituciones de personal, deberán subsanarse mediante periodos de solapamiento sin coste adicional durante el tiempo necesario. Si a criterio del responsable del contrato esto no fuera posible, las 10 primeras jornadas de trabajo de la persona sustituta no serán facturables.

2.5 Formación del equipo de trabajo

La empresa será responsable de la formación necesaria para que sus técnicos puedan desarrollar las tareas encomendadas englobadas en el objeto de este contrato.

2.6 Otras condiciones

En cumplimiento del Acuerdo de Consejo de Gobierno de 5 de abril de 2013, por el que se aprueban las instrucciones para la gestión de los contratos de servicios y encomiendas de gestión, y por lo que respecta al personal que ha de realizar los trabajos objeto de este contrato, se hace constar en el pliego de prescripciones técnicas lo siguiente:

1. La empresa adjudicataria deberá ejercer de modo real, efectivo y periódico, el poder de dirección inherente a todo empresario con relación a sus trabajadores, asumiendo absolutamente todas sus obligaciones (negociación y pago de salarios, concesión de permisos, vacaciones, etc.). En ningún caso se identificará, en el contrato de servicios, el nombre de los trabajadores que la empresa designe para cumplir el contrato.
2. La Dirección General de Informática, Patrimonio y Telecomunicaciones no cederá equipos ni material para la realización del servicio contratado, debiendo llevarse a cabo el mismo en las dependencias del empresario adjudicatario.
 - 2.1. La Administración Regional no proporcionará certificado digital reconocido ni tarjeta de empleo de la Administración Regional al personal del equipo de trabajo que desarrolle las tareas objeto de este contrato, siendo obligación del adjudicatario el proporcionar a dicho personal un certificado digital de persona física admitido por la plataforma de Administración Electrónica de la Comunidad Autónoma de la Región de Murcia.
 - 2.2. La Administración Regional no proporcionará cuenta de correo al personal del equipo de trabajo que desarrolle las tareas objeto de este contrato, siendo obligación del adjudicatario el proporcionar a dicho personal una cuenta de correo.
 - 2.3. La Administración Regional no proporcionará ordenadores personales al personal del equipo de trabajo que desarrolle las tareas objeto de este contrato, siendo obligación del adjudicatario el proporcionar a dicho personal equipos de trabajo con, al menos, sistema operativo, suite ofimática y antivirus actualizados.
3. Por parte de la empresa adjudicataria se habrá de designar, al menos, un coordinador técnico o responsable, perteneciente a su plantilla, que será el interlocutor con quien se relacionará únicamente el responsable del contrato, funcionario de la Dirección General de Informática, Patrimonio y Telecomunicaciones.





- 3.1. La CARM podrá establecer la forma de comunicación con el equipo de trabajo de la empresa adjudicataria que considere necesaria para agilizar la comunicación con éstos (teléfono, videoconferencia, mensajería instantánea, etc.).
- 3.2. El adjudicatario deberá utilizar el sistema de gestión de incidencias corporativo de la CARM. No obstante, si así lo acuerdan las partes, se podrá utilizar un sistema de gestión de incidencias alternativo.
4. En el contrato que se formalice con la empresa adjudicataria no podrán figurar cláusulas de subrogación empresarial en las que la Consejería de Hacienda asuma compromisos sobre los empleados del adjudicatario o de la empresa instrumental encomendada.
5. Al equipo de trabajo de la empresa adjudicataria de la contratación no es aplicable el régimen jurídico de los empleados públicos, en especial los aspectos relativos al cumplimiento y control de horario, vacaciones, permisos y licencias y otros de análoga naturaleza.
6. El equipo de trabajo que desarrolle las tareas objeto de este contrato no formará parte de los organigramas y directorios de la Administración Regional, ni dispondrá de claves de acceso a recursos propios de los funcionarios, en particular al sistema de control horario.
7. El adjudicatario deberá organizar y dirigir al equipo de trabajo que designe para la realización de las tareas objeto de este contrato, no dependiendo este equipo, en ningún caso, de ninguna unidad administrativa de la Administración Regional.
8. Para la realización de este trabajo únicamente se proporcionarán a dicho personal accesos temporales a los sistemas y servidores implicados o relacionados directamente con el objeto de este contrato.
 - 8.1. La Administración Regional no proporcionará claves de acceso (login y contraseña) a la intranet de la Administración Regional al personal del equipo de trabajo que desarrolle las tareas objeto de este contrato, salvo que resulte necesario para la ejecución del contrato, en cuyo caso se dispondrá de las mismas con carácter temporal, debiendo quedar reflejado de manera inequívoca que el usuario autorizado es o forma parte de la empresa contratista y que dicha excepción lo es en virtud de las específicas funciones a desarrollar.
9. A los efectos del Apartado g) de la Instrucción SEGUNDA de dicho Acuerdo, el responsable a nivel administrativo de la contratación será Pedro Olivares Sánchez, Jefe del Servicio de Integración de Aplicaciones Corporativas, así como el Director General de Informática, Patrimonio y Telecomunicaciones, los cuales serán los encargados de velar porque la ejecución del mismo se ajuste estrictamente a lo contratado, asumiendo las responsabilidades a que se refiere la instrucción quinta de este Acuerdo.

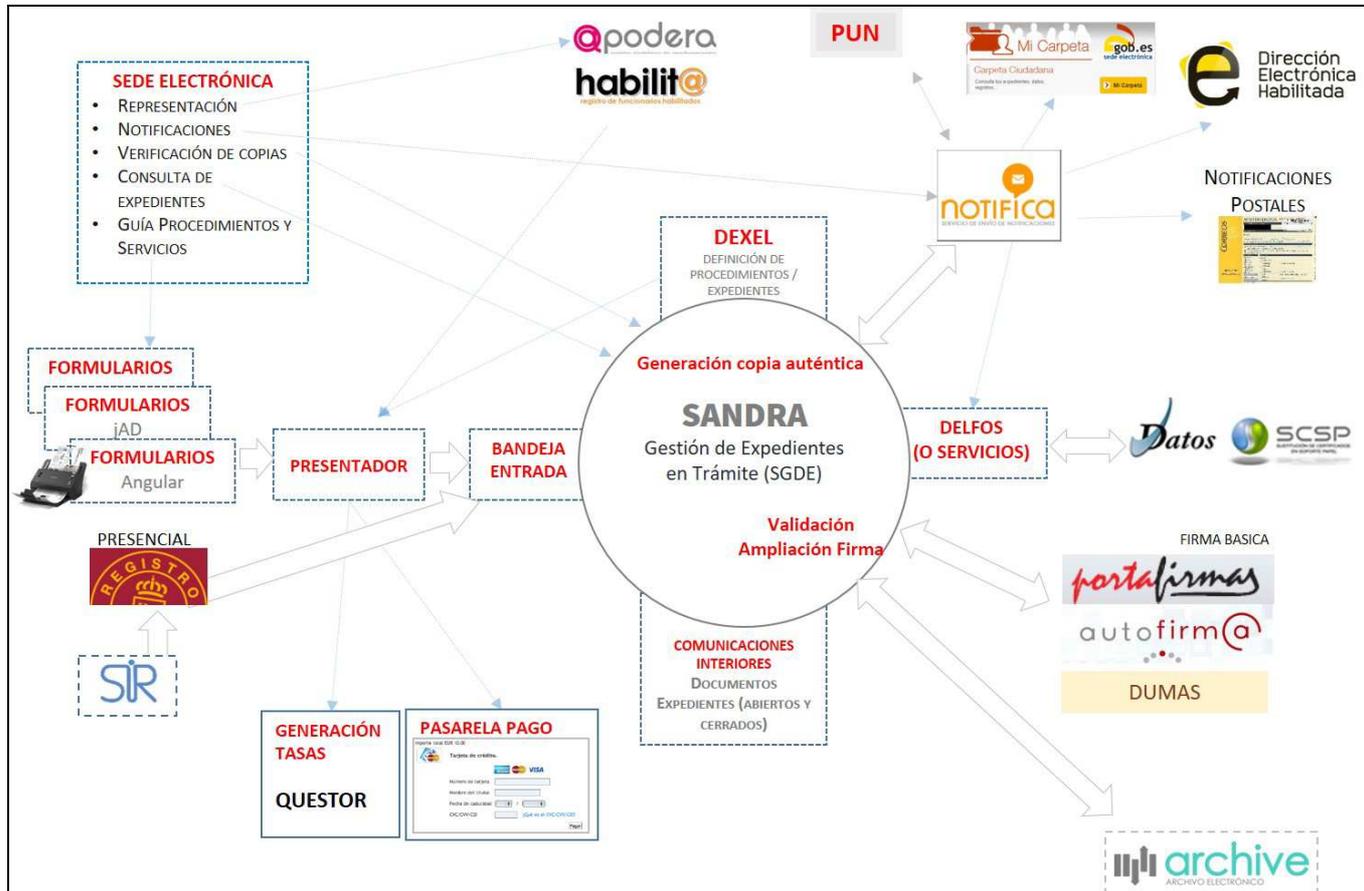
3 Descripción técnica del servicio

3.1 Entorno funcional. Especificación de requisitos



La plataforma de Administración Electrónica (en adelante, eA) está basada en el patrón SOA (Service Oriented Architecture).

El esquema general de componentes de eA es:



Los servicios proporcionados a través de la plataforma eA se pueden clasificar en Servicios Comunes y Aplicaciones.

SERVICIOS COMUNES

Son aquellos servicios que ofrecen funcionalidad de valor añadido, pudiendo ser utilizados directamente por las distintas aplicaciones/sistemas clientes de la plataforma, o para la composición de nuevos servicios. Una relación de dichos servicios es:

- Autenticación (PASE, interfaz con Cl@ve)
- Validación de certificados digitales
- Firma electrónica / Verificación de firma (DUMAS)
- Interfaz con Pasarelas de pagos (UMBELA) y de tasas (QUESTOR)
- Gestor de Formularios
- Interfaz con Registro de E/S





- eSatelites (Interfaz con Back-Office)
- Parametrización de procedimientos administrativos (DEXEL)
- Gestor documental/Gestor de Expedientes/Custodia documental (SANDRA)
- Generación de CSV y copias auténticas
- Interfaz con FACe, el punto general de entrada de facturas electrónicas
- BI – Inteligencia de negocio
- ESB – Bus de Integración de Servicios

APLICACIONES

Son servicios y aplicaciones que tienen un propósito específico, y hacen uso de los Servicios Comunes anteriores. Incluyen tanto los destinados a ciudadanos y empresas como los destinados a funcionarios.

Para ciudadanos/empresas:

- Presentación de Solicitudes (PRESENTADOR)
- Presentación de Solicitudes genéricas de inicio y de trámite
- Gestor de Notificaciones telemáticas
- Plataforma de Interoperabilidad (Certificaciones electrónicas)
- Consulta de Expedientes
- Consulta de Documentos
- Validación de documentos CSV y copias auténticas

Para empleados:

- Tramitación de Expedientes (DELFO)
- Registro de Entrada/Salida (Registr@-RM)
- Firma de empleado (PORTAFIRMAS)
- Gestión de la Inspección General de Servicios (MADRE)
- Comunicaciones Interiores (COMINTER)

A continuación se detallan los servicios y aplicaciones más relevantes:

3.1.1 DUMAS

Se trata del servicio de firma en servidor, utilizado para la firma con sello de órgano o entidad (actuaciones administrativas automatizadas) así como para completar y extender firmas.

A grandes rasgos, el servicio de firma realiza dos funciones diferenciadas pero estrechamente relacionadas:





1. Por un lado, el servicio recibe solicitudes de generación de firma. Estas solicitudes indican al servicio que genere firmas con unas características determinadas sobre ciertos documentos.

2. Por otro lado, el servicio atiende solicitudes de verificación de firma. Además de establecer si una determinada firma es válida o no, el servicio de firma es capaz de ofrecer información relativa al firmante y a la fecha de la firma.

Adicionalmente, el servicio puede modificar una firma recibida a petición del cliente, devolviendo una firma equivalente pero con otro formato distinto o ampliar la firma recibida con información adicional (por ejemplo, propiedades no firmadas de la firma).

3.1.2 DEXEL

DEXEL es la aplicación de definición de expedientes electrónicos, permite a los gestores definir el funcionamiento de cada procedimiento administrativo.

Centraliza gran parte de la información relacionada con los procedimientos que será utilizada por todas las aplicaciones, a nivel:

- Informativo (Guía de Servicios, SIA, DIR3, etcétera)
- Tramitación (SANDRA, DELFOS, aplicaciones SECTORIALES, etcétera)

La definición de cada procedimiento permite:

- Clasificar el procedimiento (áreas temáticas, colectivos destinatarios, familias, etcétera)
- Parametrizar las formas de inicio, plazos, efectos del silencio, etcétera
- Establecer qué formularios y documentación se requieren para su tramitación
- Identificar las tasas asociadas al tipo de trámite
- Relacionar la regulación legal
- Establecer qué documentos forman parte del expediente, su nivel de confidencialidad y su estado, tanto los que aporta el interesado (DI) como los que se generan internamente por la propia administración (DA)
- Definir las condiciones de acceso a los expedientes, por el personal y por las aplicaciones

3.1.3 SANDRA

El gestor documental corporativo SANDRA (Sistema de Almacenamiento Normalizado Documental de la Región de Murcia) se basa en una plataforma de gestión documental única y con un modelo de uso uniforme.

Es el sistema electrónico de administración de expedientes electrónicos donde residen los expedientes electrónicos en trámite, proporcionando soporte a la normalización





necesaria y descargando a los responsables de los procedimientos de la tarea de interpretación de la información.

Se compone de:

- **Repositorio documental**, que incluye todos los documentos electrónicos y una caracterización con un sistema común de clasificación (series documentales). Es un sistema capaz de custodiar los documentos durante todo su ciclo de vida, asegurando su custodia longeva.
- **Servicios de gestión documental comunes** para toda la organización, que implantan la lógica de negocio de la gestión documental mediante un conjunto de acciones comunes. El uso de estos servicios garantiza un uso homogéneo del gestor de acuerdo a las políticas de gestión documental. Los servicios disponibles son:
 - ExpedienteService: Operaciones para la gestión de expedientes electrónicos (alta, modificación, recuperación, cierre y eliminación)
 - DocumentoService: Operaciones para la gestión de documentos electrónicos (alta, modificación, recuperación, mover y eliminación)
 - EniService: Operaciones de interoperabilidad según los esquemas definidos por el Esquema Nacional de Interoperabilidad (recuperar expediente electrónico y documento electrónico)
 - BusquedaService: Operaciones de búsqueda sobre expedientes y documentos (buscar expedientes y documentos)
 - MaestrosService: Operaciones para la obtención de los posibles valores de atributos (obtener valores maestros)

3.1.4 Presentador

Se trata de un servicio que permite la presentación en sede electrónica con todas las garantías jurídicas de formularios web generados en cualquier tecnología. Se configura desde DEXEL y permite a los formularios web centrarse en su negocio, delegando en Presentador:

- La autenticación (para formularios simples)
- La información para la Notificación
- La inclusión de los certificados de interoperabilidad a aportar y cláusulas de consentimiento
- La inclusión de los anexos a aportar obligatorios y opcionales
- La generación de las tasas
- El pago electrónico
- La firma de la solicitud, generación del recibo de presentación y entrega en la Bandeja de entrada del procedimiento / departamento tramitador



3.1.5 Gestor de notificaciones telemáticas

Es un servicio que permite a aplicaciones y funcionarios realizar notificaciones de forma centralizada usando un conjunto diverso de canales de notificación.

El envío de notificación desde las aplicaciones es un proceso asíncrono: se realiza la solicitud y se consulta a posteriori el estado.

Los canales disponibles son:

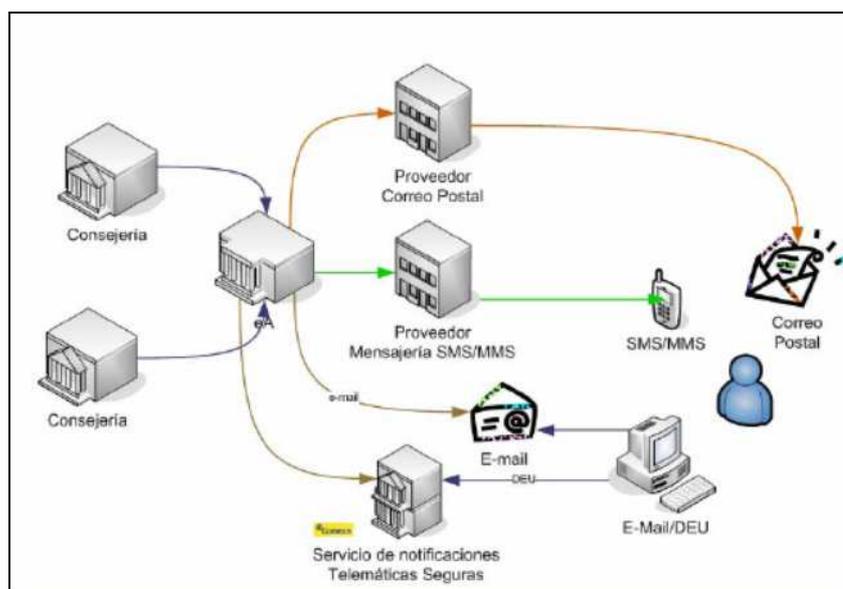
- SMS.
- Correo electrónico.
- Push (aplicaciones móviles).
- Notificaciones telemáticas legales (de acuerdo al art. 43 de la Ley 39/2015).

Las notificaciones legales se practican, dependiendo de la condición del receptor:

- Mediante comparecencia en sede electrónica de la CARM.
- A través de la dirección electrónica habilitada única. Para ello se utiliza la plataforma estatal Notific@.
- Mediante notificación postal.

Las notificaciones telemáticas legales pueden ir además acompañadas de aviso mediante SMS y/o correo electrónico.

El esquema funcional del servicio de Notificaciones se puede describir mediante el siguiente diagrama:



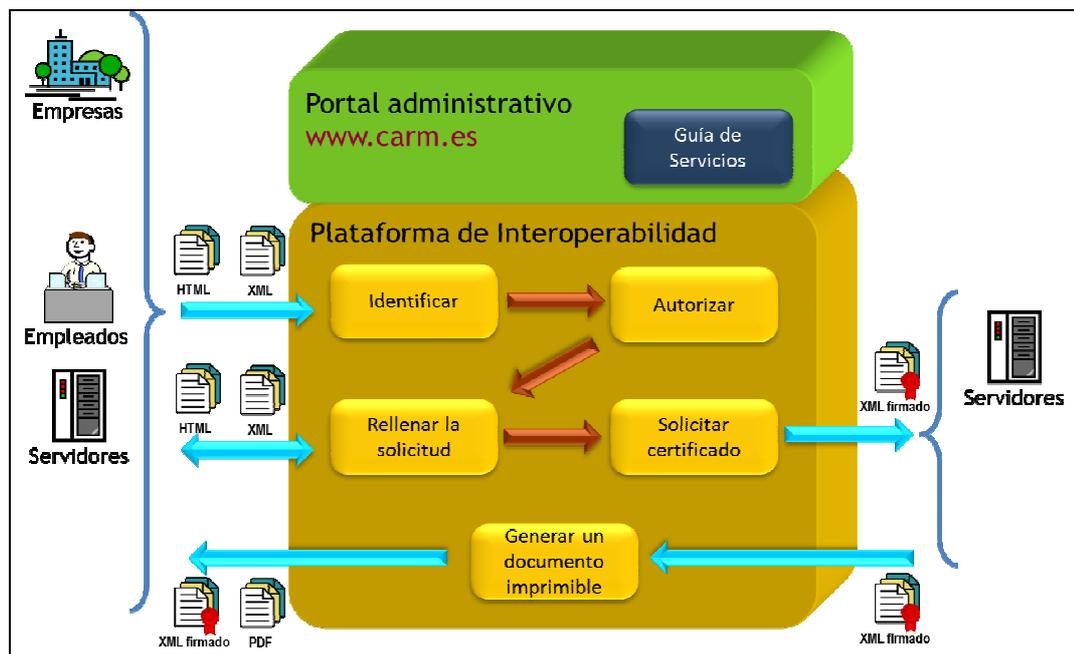
3.1.6 Plataforma de Interoperabilidad (Certificaciones electrónicas)

La generación de Certificaciones electrónicas está centralizada en la Plataforma de Interoperabilidad, que tiene las siguientes características:



- Centraliza los intercambios, no importa el proveedor ni el destinatario.
- Utiliza una interfaz común y un formato estándar para el intercambio de certificados telemáticos entre Administraciones Públicas.
- Los proveedores pueden ser tanto los distintos órganos de la CARM como otras administraciones (a través de la red SARA).

El esquema funcional de la Plataforma de Interoperabilidad se puede describir mediante el siguiente diagrama:



3.1.7 DELFOS

Aplicación que permite realizar operaciones directamente sobre el expediente electrónico, está pensada para uso de los gestores que no disponen de aplicación sectorial, o cuando, teniendo aplicación, haya documentos no integrados.

El acceso a los expedientes es por procedimiento y departamento y las autorizaciones de esta aplicación se establecen en DEXEL.

3.1.8 Registr@-RM

El Sistema de Registro de la Administración Pública de la Región de Murcia Registr@-RM es un desarrollo basado en AL SIGM que gestiona:

1. Los asientos de registro de Entrada y Salida (incluyendo la digitalización certificada de la documentación presentada en Registro).





2. El control y seguimiento electrónico del flujo de las solicitudes presentadas por los interesados en cualquier Oficina Corporativa de Atención al Ciudadano de la CARM, mediante la validación de la entrada en el Órgano Administrativo competente para su resolución y su despacho al servicio que le corresponda.

Este sistema consta de Oficinas de la CARM y Unidades Administrativas de todas las Administraciones Públicas, con un código unívoco DIR3.

3.1.9 Portafirmas

Aplicación corporativa de firma electrónica de la Administración Regional que debe ser utilizada en aquellos actos y trámites que sean objeto de firma electrónica conforme a la Ley 59/2003, de 19 de diciembre, la Ley 5/2012, de 29 de junio y el Decreto 302/2011, de 25 de noviembre.

Para los usuarios es una plataforma centralizada donde, independientemente de donde se generen los documentos a firmar, pueden acumular peticiones de firma y proceder a la firma de éstas. Es, por tanto, una herramienta corporativa destinada a facilitar el uso de la firma electrónica de documentos procedentes de diferentes sistemas de información y/o usuarios, cuyo uso conlleva agilizar los procedimientos de la actividad administrativa.

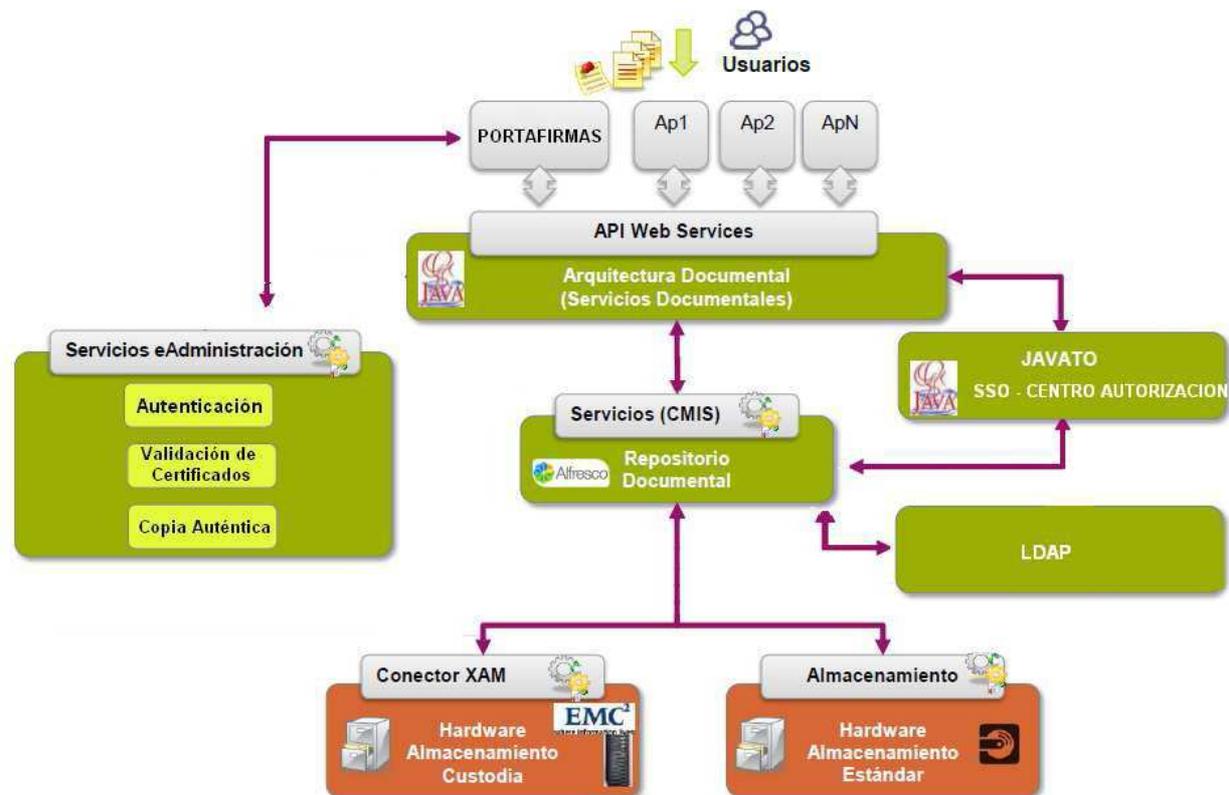
La aplicación admite la firma electrónica de archivos en formato PDF, ODT y JPG mediante el empleo de firma electrónica reconocida y firma electrónica avanzada (artículos 3.2. y 3.3 de la Ley de Firma Electrónica), y genera los siguientes documentos:

- Un **documento firmado** en XAdES, en la extensión XML que tiene la condición jurídica de documento electrónico de naturaleza administrativa, conforme a lo establecido en los artículos 3.5 y 6 de la Ley de Firma Electrónica, y que constituye el documento electrónico original y hace prueba plena del documento electrónico
- Una **copia auténtica** del documento firmado en formato PDF. Se trata de un documento que cumple con los requisitos legales, al incluir un código seguro de verificación (CSV), que permite a cualquier poseedor comprobar su autenticidad a través de la Sede Electrónica de la CARM. Este documento permite al gestor realizar copias auténticas en papel del documento firmado electrónico, con plena validez, facilitando así su archivo en el expediente físico y su envío o notificación por medios convencionales.

Esta funcionalidad de copia auténtica es esencial, pues ha permitido extender el uso de la aplicación Portafirmas a todos los gestores administrativos y no únicamente a los que disponen de aplicación informática para la gestión de sus procedimientos.

La integración entre los servicios SANDRA, Portafirmas y CSV queda reflejada en el siguiente esquema:





3.1.10 MADRE

Madre es la aplicación de seguimiento y control de la Inspección General de Servicios para el seguimiento de los planes de mejora de la Simplificación Administrativa y Normativa así como para gestionar la Plataforma de Interoperabilidad.

Las actividades de simplificación administrativa y normativa deben desarrollarse por todas las Direcciones Generales y Organismos Autónomos, a través de esta aplicación se lleva el seguimiento de dichas actividades, que se agrupan en 3 tipos de medidas:

1. Medidas de simplificación para las que no son necesarias modificaciones normativas.
2. Medidas de simplificación para las que son necesarias modificaciones normativas.
3. Modificaciones normativas que tienen por objetivo puramente la simplificación normativa (refundición de textos legales por ejemplo).

Se definen 11 tipos de medidas, cada una de las cuales define unos datos a completar, existiendo datos comunes a todas ellas como la fecha de entrada en vigor prevista, la fecha de entrada en vigor efectiva, el responsable de su ejecución, etcétera.

Un Plan de Mejora se define como el conjunto de todas las actividades de simplificación que realiza un servicio, centro directivo o Consejería/Organismo Autónomo sobre sus procedimientos administrativos. Estas actividades implantan los posibles tipos





de medidas de simplificación existentes y pueden incluir una relación de ítems a los que se podrán asociarse fechas de inicio y fin.

Para cada fecha a punto de vencer o vencida el sistema envía avisos tanto al responsable de la ejecución de la actividad/ítem como al responsable del procedimiento administrativo y a los responsables del Plan de Inspección de la CARM.

En cuanto a la gestión de la Plataforma de Interoperabilidad, incluye:

- Tramitación de las solicitudes de autorización de alta en la Plataforma de Interoperabilidad.
- Registro de las solicitudes tramitadas, así como de toda la documentación asociada a las solicitudes.

3.2 Entorno tecnológico

Todos los trabajos técnicos, diseños y desarrollos se realizarán de acuerdo a los estándares de trabajo definidos por la Dirección General de Informática, Patrimonio y Telecomunicaciones.

Cualquier desarrollo a realizar en el marco de esta contratación se realizará en lenguaje Java (JEE, arquitectura de 3 capas). Se implantará sobre la siguiente plataforma tecnológica (o la evolución de la misma que en cada momento esté disponible):

- Base de datos: Oracle.
- Servidor de aplicaciones: Tomcat (para algunos servicios, JBoss o WebLogic Server).

Como herramientas de trabajo estarán disponibles, entre otras, Eclipse y JDK.

En particular, las aplicaciones DEXEL, Presentador, Madre y Delfos están desarrolladas en la siguiente tecnología:

- Capa de presentación
 - Spring MVC
 - JSP
 - Apache Tiles
 - Bootstrap + jQuery + DataTables + Highcharts
- Capa lógica de negocio
 - Spring
- Capa de persistencia
 - Spring JDBC





- Driver JDBC Oracle Database 11g Release 2 (11.2.0.4)
- Servicios core
 - Web services: Apache CXF
 - Seguridad: Spring Security
 - Log: SLF4J y Log4j 2

La descripción del procedimiento de Integración Continua utilizado en la CARM puede consultarse en el anexo III.

El diseño e implantación de las aplicaciones garantizará la alta disponibilidad y escalabilidad de la plataforma. Los desarrollos deberán ser serializables y/o clusterizables. Los entregables de los desarrollos incluirán:

- Pruebas de disponibilidad y escalabilidad.
- Pruebas de rendimiento y de carga.
- Test de alto nivel de las aplicaciones (a realizar, por ejemplo, con Selenium).

Las aplicaciones se desarrollarán atendiendo a principios de accesibilidad, usabilidad y neutralidad tecnológica.

Además, las interfaces de usuario deberán tener mantener un Look&Feel común, y deberán ajustarse a las normas de estilo definidas para el Plan Estratégico de Administración Electrónica de la CARM (PAECARM).

La arquitectura de seguridad existente en la CARM para las aplicaciones orientadas a Internet es la siguiente:

- Se dividen las aplicaciones en tres partes diferentes y relacionadas entre sí por políticas estrictas de seguridad. Estas políticas permiten supervisar la interconexión entre las tres partes.
- Estas partes son:
 - Sistema servidor frontal hacia el usuario (frontal).
 - Sistema servidor de aplicaciones (aplicaciones).
 - Sistema servidor de bases de datos (BD).
- Las conexiones entre los usuarios (Internet e intranet) y el sistema frontal (web, portal, https,...) están supervisadas por un cortafuegos.
- Las conexiones entre el sistema frontal y las aplicaciones (Tomcat,...) están supervisadas por otro cortafuegos.
- Las conexiones entre las aplicaciones y las bases de datos están supervisadas por cortafuegos.





3.3 Fases del contrato

Se establecen tres fases en este contrato: inicio, ejecución y devolución del servicio.

3.3.1 Fase de inicio

La fase de inicio del contrato tiene por objetivo que el adjudicatario se familiarice con la plataforma de Administración Electrónica de la CARM y adquiera el conocimiento necesario para prestar dicho servicio.

En ella, el adjudicatario analizará la documentación disponible (modelo de datos, procedimientos definidos, etcétera), así como el código fuente de la aplicación y preparará sus entornos de trabajo.

El plazo de esta fase será de un mes, durante la misma el adjudicatario prestará el servicio pero no se aplicarán penalizaciones.

3.3.2 Fase de ejecución

Esta fase constituye la mayor parte del contrato. Durante ella, el adjudicatario realizará la ejecución propia del servicio de acuerdo a las condiciones mínimas exigidas en el presente pliego y las aportadas en su oferta, junto con las propuestas adicionales y transformaciones que se consideren necesarias para una gestión eficiente.

Las tareas de soporte a la explotación de la plataforma de Administración Electrónica de la CARM se concretan en:

- Corrección de incidencias y errores conocidos detectados, ya sean por aspectos técnicos o funcionales, que impidan el correcto funcionamiento de la plataforma.
- Elaboración de procedimientos de detección, solución provisional y corrección de incidencias frecuentes.
- Implantación de mejoras técnicas que, sin añadir funcionalidad, aumenten la calidad, seguridad y/o el rendimiento de la plataforma.
- Implantación de cambios requeridos por modificaciones normativas o tecnológicas.
- Implantación de mejoras funcionales requeridas por los responsables funcionales (usuarios clave).
- Resolución de dudas (funcionales y técnicas) de los usuarios finales mediante el establecimiento de un soporte especializado de segundo nivel.
- Actuaciones formativas de los usuarios finales y técnicos de la CARM relativas a los trabajos realizados.
- Apoyo puntual al personal destinado a las tareas de administración de los sistemas y el mantenimiento de la CMDB, así como colaboración en la detección y eliminación de riesgos y amenazas que pudiesen afectar a la plataforma.





La fase de ejecución comprende desde el fin de la fase de inicio hasta el fin del contrato o el fin de la prórroga, de producirse.

3.3.3 Fase de devolución del servicio

Con objeto de garantizar una adecuada devolución del servicio, el adjudicatario del presente pliego se compromete a colaborar activamente con la CARM y, en su caso, con otro adjudicatario, para facilitar la transferencia de conocimiento, asegurando el mantenimiento de la calidad del servicio. Para ello se establece una fase de devolución del servicio, que convive con la fase de ejecución. A criterio del responsable del contrato (si considera que la documentación disponible es insuficiente), el adjudicatario estará obligado a transferir el conocimiento a través de sesiones de formación tanto a técnicos de la CARM como al siguiente adjudicatario del servicio.

El adjudicatario es enteramente responsable de la prestación del servicio, con la capacidad y agilidad requeridas hasta que finalicen de forma simultánea tanto la fase de ejecución como la de fase de devolución del servicio.

La duración de la fase de devolución del servicio se determinará una vez que se conozca la duración de la fase de inicio del contrato que sustituya al que es objeto del presente documento. Se estima que tendrá una duración máxima de tres meses.

3.4 Indicadores

A continuación se definen los indicadores objetivos por los que se va a evaluar la prestación del servicio, la periodicidad con la que se van a medir, el nivel de acuerdo de servicio requerido y el nivel de mejora máximo admitido:

- PIFP (Porcentaje de Interacciones Fuera de Plazo): Porcentaje de interacciones cerradas fuera de plazo en el periodo considerado (sobre el total de interacciones cerradas en el periodo considerado) más el porcentaje de interacciones abiertas que ya están fuera de plazo en el último día del periodo considerado (sobre el total de interacciones abiertas en el último día del periodo considerado).
- FRP (Factor de Rotación de Personal): Número de cambios en el equipo de trabajo del adjudicatario que no ha solicitado el responsable del contrato ni son por causa de fuerza mayor en el periodo considerado. Persigue la estabilidad del equipo de soporte para optimizar el tiempo de resolución de interacciones y minimizar el tiempo de transferencia de conocimiento a los nuevos miembros del equipo.
- IR (Índice de Reclamaciones): Porcentaje de quejas sobre el total de interacciones dadas de alta en el periodo considerado.
- CP (Calidad del Proceso): Número de no conformidades leves detectadas por el responsable del proceso durante el periodo considerado (documentación incorrecta, deuda técnica generada, etcétera). Una no conformidad grave se considera equivalente a tres leves.





Indicador	Periodicidad medida	SLA requerido	Nivel de mejora máximo admitido
PIFP	Mensual	20%	5%
FRP	Trimestral	2	0
IR	Mensual	1%	0,25%
CP	Mensual	3	0

Consideraciones en la aplicación del indicador PIFP:

- Los plazos de las interacciones a realizar serán:
 1. En el caso de incidencias, 50 horas.
 2. En el caso de solicitudes y tareas: consensados entre el responsable del contrato y el responsable del equipo de trabajo asignado por el adjudicatario en el momento de dar de alta la tarea.
- El tiempo de resolución se define como el tiempo transcurrido desde que se asigna una interacción al equipo de soporte hasta que el trabajo a realizar en dicho ticket por parte del equipo de soporte está correctamente concluido. Esto incluye la gestión del repositorio de código fuente, la elaboración de la documentación asociada, las pruebas y las posibles iteraciones en el desarrollo por defectos en la solución entregada. Se excluye el tiempo imputable a otros equipos de trabajo (remisión de información por parte de los usuarios, despliegues en los servidores por parte del personal informático de la CARM, etcétera).
- El cómputo del tiempo de resolución descontará el horario no laboral así como los festivos y fines de semana.
- En situaciones excepcionales, para interacciones debidamente justificadas, el adjudicatario podrá solicitar al responsable del contrato una modificación del Acuerdo de Nivel de Servicio, siendo potestad del responsable del contrato admitir esta modificación.

Consideraciones en la aplicación del indicador CP:

- Se considera que una no conformidad es grave cuando se trate de un error relevante que pueda causar fallos en la prestación del servicio o en el trabajo de los usuarios, que afecte a la imagen del servicio o tenga una repercusión importante.

4 Metodología a utilizar en la ejecución

Durante la prestación del servicio, la empresa seguirá la guía de buenas prácticas ITIL/ ISO 20.000. En particular, se aplicará la gestión de problemas para resolver las causas raíz de las incidencias.





5 Transferencia tecnológica

Durante la ejecución de los trabajos objeto del contrato el adjudicatario se compromete, en su caso, a facilitar a las personas designadas por la Dirección General de Informática, Patrimonio y Telecomunicaciones a tales efectos, la información, manuales empleados en la formación y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

La titularidad plena de todos los trabajos realizados (documentación, código fuente desarrollado, etc.) pasará a la Comunidad Autónoma de la Región de Murcia.

6 Documentación de los trabajos

Como parte de los trabajos objeto del contrato, el adjudicatario se compromete a generar toda la documentación requerida por la Dirección General de Informática, Patrimonio y Telecomunicaciones. En particular, se generarán como mínimo los siguientes documentos:

- Manual de usuario.
- Manual de instalación/implantación.
- Documento de Análisis/Diseño.
- Documento de Desarrollo.
- Documento de Pruebas.
- Documento de Soporte y Mantenimiento (en particular, los protocolos de resolución de incidencias y cambios reglados).

La documentación quedará en propiedad exclusiva de la Administración Regional sin que el contratista pueda conservarla ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización de la Dirección General Informática, Patrimonio y Telecomunicaciones, que la facilitará en su caso previa petición formal del contratista con expresión del fin.

7 Seguridad y confidencialidad de la información

7.1 Sistemas de información y tratamiento

Los sistemas de información objeto del contrato se categorizan de nivel MEDIO (en el caso de GLPI) y de nivel ALTO (en el caso de la plataforma de Administración Electrónica de la CARM). La categoría de las distintas dimensiones es la siguiente:

Sistema de Información	Dimensión Disponibilidad	Dimensión Integridad	Dimensión Confidencialidad	Dimensión Autenticidad	Dimensión Trazabilidad
GLPI	B	B	M	B	B
Plataforma eA	B	A	A	M	B





7.1.1 Objeto del encargo del tratamiento

El adjudicatario del contrato ejercerá como encargado del tratamiento de datos (en adelante, ETD) de carácter personal referidos a los tratamientos de los sistemas de información anteriormente mencionados.

7.1.2 Identificación de la información afectada

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este pliego, la DGIPyT pondrá a disposición de licitador que lo solicite y del adjudicatario la lista de tipos de información de datos de carácter personal afectados por el contrato.

7.1.3 Duración

El encargo del tratamiento tiene la duración definida para el contrato en el Pliego de Condiciones Administrativas Particulares y el inicio y fin establecido durante el proceso de contratación.

7.1.4 Subcontratación

No se permite subcontratar ninguna de las prestaciones que formen parte del objeto de este encargo que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito a la DGIPyT, con una antelación de 30 días, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse a cabo si la DGIPyT no manifiesta su oposición en el plazo establecido.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el subencargado del tratamiento y las instrucciones que dicte la DGIPyT. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante la DGIPyT en lo referente al cumplimiento de las obligaciones.

7.2 Reglamento General de Protección de Datos

El encargado del tratamiento y todo su personal se obliga a:





a) Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, solo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.

b) Tratar los datos de acuerdo con las instrucciones de la DGIPyT.

Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al DPD.

c) Llevar, por escrito, un registro¹ de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.

2. Las categorías de tratamientos efectuados por cuenta de cada responsable.

Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:

a) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

d) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa de la DGIPyT, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros subencargados del tratamiento del mismo responsable, de acuerdo con las instrucciones de la DGIPyT. En este caso la DGIPyT identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

e) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

f) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

g) Mantener a disposición de la DGIPyT la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

h) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

i) Notificación de violaciones de la seguridad de los datos

¹ Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa que emplee a menos de 250 personas, salvo que el tratamiento que realice pueda suponer un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1 del RGPD, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 de dicho Reglamento. (Art. 30.5 RGPD).





El encargado del tratamiento notificará al RT, DPD y la DGIPyT, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, y comunicar las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

b. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.

c. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

j) Colaborar con la DGIPyT en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.

k) Colaborar con la DGIPyT en la realización de las consultas previas a la autoridad de control, cuando proceda.

l) Poner disposición de la DGIPyT toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por aquella.

m) Medidas de Seguridad:

a. Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

b. Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.

c. Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.

n) Designar un Delegado de Protección de Datos y comunicar su identidad y datos de contacto a la DGIPyT.

ñ) Destino de los datos: Destruir los datos², una vez cumplida la prestación. Una vez destruidos, el encargado debe certificar su destrucción por escrito y debe entregar el certificado a la DGIPyT.



² Se entiende que se refiere a los datos que puedan haberse extraído y/o almacenado en dispositivos bajo la administración del ETD, no a los existentes en el SI GLPI.



7.3 Esquema Nacional de Seguridad

El adjudicatario asumirá el cumplimiento de lo establecido en el Real Decreto 3/2010, de 8 de enero, modificado por Real Decreto 951/2015, de 23 de octubre, sobre el Esquema Nacional de Seguridad (ENS), en este sentido, y para los servicios objeto del contrato, dispondrá de la Certificación de Conformidad con el ENS o se comprometerá a disponer de la Certificación de Conformidad con el ENS en el plazo de 12 meses a partir del inicio del contrato.

El nivel exigible por la Dirección Técnica en la implantación de las medidas de seguridad en los entregables correspondientes a los servicios contratados para cada uno de los sistemas de información vendrá determinado por la categorización del sistema de información objeto de este contrato y son los siguientes:

Sistema de Información	Dimensión Disponibilidad	Dimensión Integridad	Dimensión Confidencialidad	Dimensión Autenticidad	Dimensión Trazabilidad
GLPI	B	B	M	B	B
Plataforma eA	B	A	A	M	B

7.4 Política de Seguridad

El adjudicatario, al inicio del contrato y siempre que varíe el personal relacionado con el servicio contratado, recabará y entregará al Director Técnico una declaración responsable individual del personal a su servicio en relación con el objeto del contrato en la que:

- El firmante asume que, salvo que la información tenga carácter público, toda la información que conozca en relación con el contrato será considerada confidencial a los efectos contemplados en la Política de Seguridad de la CARM, cuerpo documental que se desarrolle en aplicación de su Artículo 20 y Manual de Uso de los Medios Electrónicos.

- Bajo la premisa anterior se obliga como persona usuaria a las condiciones fijadas por dicha normativa.

Mantener a disposición de la DGIPyT la documentación acreditativa del cumplimiento de las obligaciones establecidas para el cumplimiento normativo en materia de seguridad.

La Administración se reserva el derecho de auditar en cualquier momento el nivel de cumplimiento de las medidas de seguridad.

El adjudicatario deberá facilitar el acceso a los recursos que solicite la Administración para la correcta realización de la auditoría.

El adjudicatario deberá, en un plazo no superior a 3 meses, solventar sin coste para la Administración, aquellas deficiencias detectadas en dicha auditoría cuando los recursos o servicios afectados sean de su competencia o estén incluidos en la prestación de los servicios que realiza.

El incumplimiento de condiciones y compromisos puede conllevar, además de la responsabilidad civil y judicial, las correspondientes penalizaciones.





Murcia, fecha y firma en el margen izquierdo

EL JEFE DEL SERVICIO DE
INTEGRACIÓN DE APLICACIONES
CORPORATIVAS

EL SECRETARIO DE LA COMISIÓN TÉCNICA DE
COORDINACIÓN INFORMÁTICA Certifica que el presente
documento ha sido informado favorablemente por la
Comisión celebrada el 12/04/2018

Fdo.: Pedro Olivares Sánchez

Fdo.: José Arturo Botí Espinosa





Anexo I. Descripción de perfiles profesionales

En este anexo se describen los perfiles profesionales normalizados dentro de las que se debe encuadrar el personal adscrito a la oferta. Se muestran ordenados de mayor a menor nivel profesional.

- Jefe de proyecto

o Titulación

- Ingeniero informático, ingeniero de telecomunicación, licenciado en matemáticas, ingeniero técnico en informática (de gestión o de sistemas), diplomado en informática, o grado en informática. En caso de no poseer éstas, también será válida la posesión de cualquier titulación universitaria combinada con 6 años de experiencia laboral en el entorno tecnológico requerido.

o Tareas/responsabilidades

- Coordinación y dirección del equipo de trabajo.
- Distribución de tareas.
- Garantizar la calidad del trabajo realizado y de la documentación generada.
- Interlocutor con la Administración.
- Participación en la resolución de incidencias que le sean asignadas.

o Experiencia previa para la capacitación del puesto

- 2 años de experiencia como jefe de proyecto o consultor en proyectos dentro del entorno tecnológico propuesto en este pliego y en el ámbito funcional de la administración electrónica o 3 años de experiencia como analista en proyectos dentro del entorno tecnológico propuesto en este pliego y en el ámbito funcional de la administración electrónica.

- Consultor

o Titulación

- Ingeniero informático, ingeniero de telecomunicación, licenciado en matemáticas, ingeniero técnico en informática (de gestión o de sistemas), diplomado en informática, o grado en informática. En caso de no poseer éstas, también será válida la posesión de cualquier titulación universitaria combinada con 6 años de experiencia laboral en el entorno tecnológico requerido

o Tareas/responsabilidades

- Asesoramiento tecnológico en las tareas que así lo requieran
- Garantiza la calidad del trabajo realizado y de la documentación generada
- Participación en la resolución de incidencias que le sean asignadas





- **Experiencia previa para la capacitación del puesto**

- 2 años de experiencia como consultor o jefe de proyecto en proyectos dentro del entorno tecnológico propuesto en este pliego y en el ámbito funcional de la administración electrónica o 3 años de experiencia como analista en proyectos dentro del entorno tecnológico propuesto en este pliego y en el ámbito funcional de la administración electrónica.

- **Analista**

- **Titulación**

- Ingeniero informático, ingeniero de telecomunicación, licenciado en matemáticas, ingeniero técnico en informática (de gestión o de sistemas), diplomado en informática, o grado en informática. En caso de no poseer éstas, también será válida la posesión de cualquier titulación universitaria combinada con 5 años de experiencia laboral en el entorno tecnológico requerido.

- **Tareas/responsabilidades**

- Apoyo al jefe de proyecto en la distribución de tareas.
- Participa en la relación con el área usuaria y obtiene información para la realización de módulos del sistema.
- Análisis y diseño de la solución técnica de los desarrollos establecidos.
- Coordinación del equipo técnico de analistas-programadores.
- Participación en la resolución de incidencias que le sean asignadas.

- **Experiencia previa para la capacitación del puesto**

- 2 años de experiencia como analista en proyectos dentro del entorno tecnológico propuesto en este pliego y en el ámbito funcional de la administración electrónica o 3 años de experiencia como analista-programador en proyectos dentro del entorno tecnológico propuesto en este pliego y en el ámbito funcional de la administración electrónica.

- **Analista-programador**

- **Titulación**

- Ingeniero informático, ingeniero de telecomunicación, licenciado en matemáticas, ingeniero técnico en informática (de gestión o de sistemas), diplomado en informática, o grado en informática. En caso de no poseer éstas, también será válida la posesión de cualquier titulación universitaria o de una formación profesional de nivel 2 (FP II) de informática, en ambos casos combinada con 5 años de experiencia laboral en el entorno tecnológico requerido.

- **Tareas/responsabilidades**

- Apoyo a los analistas en el análisis y diseño de la solución técnica de los desarrollos establecidos.
- Programación y documentación del código generado.
- Pruebas del software, en colaboración con los usuarios.





- Participación en la resolución de incidencias que le sean asignadas.
- **Experiencia previa para la capacitación del puesto**
 - Al menos 2 años de experiencia como analista-programador en proyectos dentro del entorno tecnológico propuesto en este pliego o 3 años de experiencia como programador en proyectos dentro del entorno tecnológico propuesto en este pliego.





Anexo II. Cuestionario de personal

Datos comunes

Empresa licitante:

Perfil ofertado:

Apellidos y nombre:

Titulación académica

Título académico	Centro	Años	Fecha expedición

Años: Duración oficial

Certificaciones

Certificado	Organismo certificador	Periodo de validez





Firmante: OLVARES,SANCHEZ, PEDRO 05/10/2018 16:12:23 Firmante: BOTI,ESPINOSA, JOSE ARTURO 11/10/2018 09:22:31

Este es una copia auténtica imprimible de un documento electrónico administrativo archivado por la Comunidad Autónoma de Murcia, según artículo 27.3.c) de la Ley 39/2015. Su autenticidad puede ser contrastada accediendo a la siguiente dirección: https://sede.carm.es/verificardocumentos e imprimiendo por código seguro de verificación (CSV) 62018097-nd04-d47c-832697374723

Datos relativos a los proyectos (para experiencia en entornos tecnológico y funcional)

Clave	Nombre Proyecto	Fecha Inicio	Fecha Final	Meses	% dedicación	Entidad usuaria	Perfil	Funcionalidad del proyecto	Descripción entorno tecnológico proyecto	C1	C2	C3	C4	C5
P1														
P2														
..														
..														
Pn														

Deben rellenarse todos los campos de este formulario a excepción de los Cx que no sean procedentes.

A continuación se detallan algunos campos de este formulario.

Meses: Meses reales trabajados en ese periodo

% dedicación: Porcentaje de dedicación al proyecto

Perfil: Perfil que ha desempeñado en el proyecto. Ver cuadro de valores.

Funcionalidad del proyecto: breve descripción de la/s funcionalidad/des del proyecto

Descripción entorno tecnológico proyecto: Relación detallada de la configuración informática del proyecto que justifique la información reflejada en el cuadro de experiencia en el entorno tecnológico. Por ejemplo, indicar el sistema operativo utilizado, la base de datos, los lenguajes de programación, herramientas de programación, de documentación, de análisis, etc.

Los Ci corresponden con los siguientes elementos tecnológicos:

- C1: Base de datos Oracle (SQL, PL/SQL)
- C2: Java EE
- C3: Web Services (SOAP, REST) y XML
- C4: HTML, CSS y JavaScript
- C5: Tomcat y JBoss

Los perfiles serán los descritos en el anexo "Descripción de perfiles profesionales", por ejemplo:

- JP: Jefe Proyecto
- CO: Consultor
- AN: Analista
- AP: Analista Programador

En caso de requerir otras deben describirse detalladamente.

Un proyecto se considera dentro del entorno tecnológico requerido si incluye al menos 3 de los 5 elementos tecnológicos indicados.





Anexo III. Descripción del procedimiento de Integración Continua

El presente anexo marca unas directrices mínimas para incluir aplicaciones Java en el sistema de integración continua de la CARM.

REQUISITOS DE LAS APLICACIONES

Las aplicaciones desarrolladas para la CARM en Java deberán cumplir los siguientes requisitos:

1. Deberá indicarse la URL del repositorio de código fuente donde se almacena la aplicación.
2. Los ejecutables (artefactos: jar, war, ear) de la aplicación deberán construirse desde el código fuente con Maven.
3. La configuración de la aplicación estará externalizada en ficheros independientes (.properties, .xml, etcétera). Cada fichero y parámetro de configuración deberá estar documentado en el propio repositorio junto al código fuente. Los ejecutables de la aplicación no contendrán ninguna dependencia del entorno (Linux, Windows, desarrollo, producción) en el que se ejecuten.
4. La configuración de los logs de la aplicación deberá estar externalizada en ficheros y no en el propio código. Se identificarán para que el Servicio de Sistemas pueda configurarlos hacia un servidor central de log.

FICHEROS DE PROPIEDADES Y CONFIGURACIÓN

Como ya se ha indicado, la configuración de la aplicación estará externalizada en ficheros independientes que se encontrarán junto al código fuente en el repositorio. Para facilitar la actualización de estos ficheros desde las tareas Jenkins será necesario respetar la siguiente estructura:

- Al nivel donde se encuentre el fichero pom.xml raíz o padre se creará la carpeta/directorio "configuracion" que contendrá una carpeta/directorio por entorno, "desarrollo/pruebas/produccion".
- Dentro de cada carpeta de entorno se situarán los ficheros de propiedades y configuración correspondientes.
- Para facilitar la configuración de propiedades "sensibles" (que no deben quedar almacenadas en el repositorio por ser contraseñas o cuyo valor debe asignarlo el Servicio de Sistemas, por ejemplo rutas de recursos NFS o ficheros de almacén de certificados), se creará el fichero "concatenar.properties" en la carpeta de Desarrollo, que contendrá las propiedades que hay que concatenar al fichero de propiedades correspondiente. El fichero "concatenar.properties" en la carpeta de desarrollo deberá existir siempre, si no hay propiedades "sensibles" no contendrá ninguna propiedad, documentando de este modo que el Servicio de Sistemas





no tiene que gestionarlo para los entornos de pruebas y producción, conteniendo las propiedades correspondientes en caso contrario.

EJEMPLO DE FICHERO "CONCATENAR.PROPERTIES"

```
root@servidor-pro-cri1:/opt/configuracion/desarrollo# cat
concatenar.properties
##### PROPIEDADES AÑADIDAS DESDE JENKINS
#####
usuario_alfresco=tramitador
clave_usuario_alfresco=laquesea
recurso_NFS=/opt/aplicacion/data
fichero_certificado=certificado.pfx
clave_certificado=123456
```

EJEMPLO DE FICHERO "CONCATENAR.PROPERTIES" VACÍO

```
root@servidor-pro-cri1:/opt/configuracion/desarrollo# cat
concatenar.properties
##### PROPIEDADES AÑADIDAS DESDE JENKINS
#####
##### NO HAY PROPIEDADES QUE CONCATENAR
```

- Para el resto de entornos (es decir, Pruebas y Producción), el fichero "concatenar.properties" será provisto por el Servicio de Sistemas de forma conveniente y por tanto no debe estar alojado en sus correspondientes carpetas del repositorio.

pom.xml

```
                                /desarrollo
                                concatenar.properties
                                ficheros de configuración
/configuracion /pruebas
                                ficheros de configuración
                                /produccion
                                ficheros de configuración
```

- Los ficheros de propiedades se copiarán finalmente en su destino correspondiente (servidor de desarrollo, pruebas o producción), en la ruta "\$CATALINA_HOME/conf/<nombre_app>".
- El Servicio de Sistemas no manipulará ni gestionará el contenido de los ficheros context.xml de las aplicaciones, aplicará el context.xml contenido en el WAR de la aplicación.





REPOSITARIOS DE CÓDIGO FUENTE

Los repositorios de código fuente aceptados serán:

- Repositorio Subversion.
- Repositorio Git.

La organización del código fuente responderá al siguiente esquema:

- Directorio /trunk/ (o branch:master en GIT) para la versión estable de la aplicación, que siempre será candidata a desplegar en los servidores de aplicaciones.
- Directorio /branches/ (o branches de GIT) para versiones en las que se trabaje en el desarrollo de nuevas funcionalidades: Una vez que estén validadas y sean estables se llevarán con merge al trunk/master.
- Directorio /tags/ (o tags de GIT), lo usará Maven para etiquetar las distintas versiones estables de la aplicación y servirán de referencia para la instalación en los servidores de aplicaciones.

TRABAJO CON MAVEN

La construcción de la aplicación partirá de un fichero pom.xml compatible con Maven 3 desde el directorio /trunk, que deberá cumplir los siguientes requisitos:

1. El groupId deberá hacer mención explícita al nombre de la aplicación o del proyecto.
2. El version deberá incluir siempre -SNAPSHOT.
3. Incluirá el tag scm con la configuración del repositorio de código fuente.
4. No incluirá configuración para el tag distributionManagement.

Deberá funcionar correctamente la ejecución de los comandos:

```
mvn deploy
```

... que construirá todos los artefactos de la aplicación y los instalará en el directorio .m2 del usuario, con la versión X.Y.Z-SNAPSHOT configurada en el pom.xml

```
mvn release:prepare release:perform -Darguments="-  
Dmaven.javadoc.skip=true"
```

... que actualizará la versión de los ficheros pom.xml, creará una nueva etiqueta/tag en el repositorio y construirá todos los artefactos e instalará en .m2 para la versión X.Y.Z.





Para las dependencias que no se resuelvan, se podrá solicitar la subida de artefactos a <https://nexus.carm.es/>

JENKINS

La construcción y despliegue de las aplicaciones en los servidores de aplicaciones se automatizará en <https://jenkins.carm.es>, previa petición al Servicio de Sistemas.

Una vez procesada la petición, se dispondrá de dos tareas Jenkins para su aplicación:

- Una tarea de compilación, que le ofrecerá dos posibilidades:
 - Construcción de un SNAPSHOT (invocación de mvn deploy)
 - Construcción de una RELEASE (invocación de mvn release:prepare release:perform -Darguments="-Dmaven.javadoc.skip=true")

Con la diferencia que, en vez de instalar en el directorio .m2 local de Maven, lo hará sobre el servidor Nexus:

- <https://nexus.carm.es/nexus/content/repositories/snapshots/> y
- <https://nexus.carm.es/nexus/content/repositories/releases/>
- Una segunda tarea de despliegue, que le ofrecerá la posibilidad de instalar los artefactos generados para su aplicación y disponibles en Nexus en los servidores de aplicaciones, con los condicionantes:
 - En los servidores del entorno de desarrollo sólo podrá instalar SNAPSHOTs
 - En los servidores del entorno de producción sólo podrá instalar RELEASEs
 - En los servidores del entorno de pruebas podrá elegir si instalar SNAPSHOT/RELEASE

