



Pliego de Prescripciones Técnicas

Procedimiento: Abierto, con varios criterios de adjudicación

Servicio de evolución tecnológica de la plataforma de Administración Electrónica de la CARM e inclusión de nuevos servicios en la misma

Referencia: PAECARM-plies-170208-Migración Plataforma eA (1.1).docx
Creación: 11/12/2017
Consejería: Hacienda
CRI: Centro Regional de Informática
Servicio: Integración de Aplicaciones Corporativas



Índice de contenido

1. Objeto y precio 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 Constitución inicial del equipo de trabajo.....	4
2.3 Otras condiciones.....	4
3. Descripción técnica del servicio	6
3.1 Entorno funcional. Especificación de requisitos.....	6
3.2 Entorno tecnológico	11
3.3 Cronograma e hitos del contrato	13
4. Metodología a utilizar en la ejecución.....	13
5. Transferencia tecnológica	13
6. Documentación de los trabajos.....	14
7. Seguridad y confidencialidad de la información.....	14
7.1 Tratamientos por cuenta de terceros.....	14
7.2 Cumplimiento de los Esquemas Nacionales de Seguridad e Interoperabilidad.....	15
Anexo I. Descripción de la Plataforma eA actual.....	17
Anexo II. Plan Estratégico de Administración Electrónica de la CARM	21
Anexo III. Certificaciones a migrar	22
Anexo IV. eSatélites a migrar.....	24
Anexo V. Descripción del framework JAVATO	25
Anexo VI. Descripción del procedimiento de Integración Continua	30

Firmante: OLIVARES SANCHEZ, PEDRO 02/05/2018 20:52:47 Firmante: RODES BELMONTÉ, VICENTE 03/05/2018 08:55:52

Esta 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 introduciendo el código seguro de verificación (CSV) 24c9094d-aa03-0158-26825449468





1. Objeto y precio estimado

El objeto del contrato consiste en:

- La migración de la actual Plataforma eA que integra los servicios corporativos de administración electrónica de la Comunidad Autónoma de la Región de Murcia.
- La implantación de nuevos servicios contemplados en el PAECARM.
- La migración de los servicios finales implantados sobre la plataforma eA (formularios y certificaciones).
- La migración de los servidores eSatélites (intermediarios entre la Plataforma eA y las aplicaciones de negocio).
- La implantación de un Bus de Servicio Empresarial (ESB-Enterprise Service Bus).
- La implantación de un Cuadro de mando.

El precio estimado del contrato asciende a la cantidad de 362.100 euros, IVA excluido, no siendo el contrato susceptible de prórroga ni siendo el precio del contrato susceptible de modificación al alza.

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, por su naturaleza, el responsable del contrato considere imprescindible realizar en las dependencias de la Administración (reuniones y sesiones de formación y entrega del trabajo realizado), corriendo el coste de conexión con los entornos que proporcione la Dirección General de Informática, Patrimonio y Telecomunicaciones (DGIPT) a cuenta del adjudicatario. Dicha conexión remota deberá tener en cuenta, los criterios de diseño, seguridad y mantenimiento que el director del contrato dictamine durante la vigencia del mismo, que deberán ser asumidos por el adjudicatario y sus empresas contratadas. La DGIPT 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 Constitución inicial del equipo de trabajo

Como complemento a la solvencia los licitadores deberán adquirir el compromiso de adscribir a la ejecución del contrato el número de personas que considere apropiado/necesario para poder cumplir los hitos en el plazo exigido.

Se indican los requisitos que debe cumplir el personal que la empresa adjudicataria destine a la ejecución del contrato:

- Titulación: Ingeniero en Informática, ingeniero técnico en informática (de gestión o de sistemas), diplomado en informática, grado en informática o titulaciones equivalentes.
- Perfil profesional: Jefes de proyectos, consultores y analistas.
- Conocimientos específicos requeridos: Conocimiento del entorno tecnológico especificado en el pliego de prescripciones técnicas.
- Otras características: Conocimientos básicos del procedimiento administrativo común, según se define en la ley 39/2015.

2.3 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 salvo aquellas tareas que, por su naturaleza, el responsable del contrato





considere imprescindible realizar en las dependencias de la Administración (reuniones y sesiones de formación y entrega del trabajo realizado).

- 2.1. La Administración Regional no proporcionará certificado digital reconocido ni tarjeta de empleado 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 personal 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 servicio objeto de este contrato afecta a un servicio concreto con autonomía y sustantividad propia, sin que pueda ser considerado como tarea permanente o habitual.





8. 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.
9. 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.
 - 9.1. 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.
10. A los efectos del Apartado g) de la Instrucción SEGUNDA de dicho Acuerdo, el responsable a nivel administrativo de la contratación es José Antonio Navarro López, Técnico Responsable, 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

Descripción de la situación actual:

- Ver Anexo I.

Las actividades necesarias para cumplir el objeto de este contrato se pueden agrupar en los siguientes hitos:

- H1. Migración de la actual Plataforma eA, que integra los servicios corporativos de administración electrónica de la CARM, manteniendo el interfaz de servicios web (WSDL) así como el modelo de datos. Esto incluye migrar las integraciones actuales con servicios externos corporativos y/o estatales.
- H2. Implantación de nuevos servicios básicos contemplados en el PAECARM, y la integración con nuevos servicios corporativos y/o estatales.
- H3. Migración de los servicios finales implantados actualmente sobre la plataforma eA (formularios y certificaciones).





- H4. Migración de los servidores eSatélites (intermediarios entre la Plataforma eA y las aplicaciones de negocio).
- H5. Implantación de un Bus de Servicio Empresarial (ESB-Enterprise Service Bus).
- H6. Implantación de un Cuadro de mando.

La planificación estimada es la siguiente:

Hito	Año	Inicio estimado	Fin estimado
H0. Plan de ejecución detallada del contrato	2018	1/10/2018	30/11/2018
H1. Migración de la actual Plataforma eA que integra los servicios corporativos de administración electrónica de la CARM	2019	1/12/2018	30/4/2019
H2. Implantación de nuevos servicios contemplados en el PAECARM	2019	1/2/2019	30/4/2019
H3. Migración de los servicios finales implantados sobre la plataforma eA (formularios y certificaciones)	2019	1/3/2019	31/5/2019
H4. Migración de los servidores eSatélites (intermediarios entre la Plataforma eA y las aplicaciones de negocio)	2019	1/3/2019	31/5/2019
H5. Implantación de un Bus de Servicio Empresarial (ESB-Enterprise Service Bus)	2019	1/5/2019	30/9/2019
H6. Implantación de un Cuadro de mando	2019	1/5/2019	30/9/2019

Sin embargo, los licitadores podrán proponer otra planificación, respetando la división en hitos y el reparto de anualidades.

Detalle de los servicios básicos a migrar (H1):

- Autenticación con certificado digital.
- Firma electrónica de ciudadanos.
- Verificación de Certificados digitales.
- Presentación de solicitudes (Tramitador). Presentación de otros documentos electrónicos. Consulta de presentaciones realizadas. El adjudicatario puede proponer el framework de desarrollo de formularios o bien utilizar el framework de la CARM JAVATO – jAD.
- Notificaciones y comunicaciones electrónicas. Incluye la conexión con la plataforma estatal Notific@.
- Plataforma de Interoperabilidad, emisión y consulta de certificados. Incluye la conexión con la plataforma estatal de Intermediación.
- Generación y verificación de CSV (Código Seguro de Verificación).





- Consulta de documentos personales.
- Recepción de facturas. Incluye la conexión con la plataforma estatal FACE.
- Administración: Codificaciones, Autorizaciones y Utilidades

Detalle de las integraciones a migrar con otros servicios corporativos y/o estatales (H1):

- Servicios intermediarios entre la Plataforma eA y las aplicaciones de negocio (eSatélites).
- LDAP Corporativo (IDECRI).
- Autoridades de certificación (validación vía OCSP y CRL).
- Sistema Único de registro (AL-SIGM).
- Plataforma de Intermediación estatal (SVD).
- Plataforma de Validación y Firma Electrónica estatal (@firma).
- Plataforma de gestión de notificaciones estatal (Notific@).
- Gestión de Tasas corporativa (QUESTOR).
- Pasarela de Pagos corporativa.
- Punto general de entrada de facturas electrónicas (FACE).
- Plataforma de firma de empleados públicos (PORTAFIRMAS).

Detalle de los servicios básicos a desarrollar (H2):

- Consulta de Expedientes. Desarrollará una interfaz de aplicación web para consulta de expedientes por parte de los titulares o interesados. Conectará con los servicios web del gestor documental corporativo SANDRA. Incluirá la conexión con el servicio estatal de Carpeta Ciudadana.
- Gestión de ficheros de gran tamaño. Desarrollará una interfaz de aplicación web y una interfaz de servicios web para alta y consulta de ficheros superiores a 5 MBytes. Conectará con los servicios web del gestor documental corporativo SANDRA. Además, integrará la interfaz de aplicación web con los módulos de presentación de solicitudes, notificaciones, consulta de expedientes, CSV, DUMAS y PORTAFIRMAS.
- Validación de firma en sede. Desarrollará una interfaz de aplicación web para verificar firmas en los formatos amparados en el Reglamento eIDAS. Además, permitirá la verificación de los documentos firmados mediante herramientas de la CARM. En particular, permitirá comprobar la validez de las solicitudes presentadas, así como de los anexos incorporados a las mismas.
- Verificación en sede de los certificados digitales. Desarrollará una interfaz de aplicación web para verificar certificados digitales. Incluirá la conexión con la plataforma estatal @firma.





Detalle de las nuevas integraciones con otros servicios corporativos y/o estatales (H2):

- Gestor documental corporativo (SANDRA y DEXEL).
- Servicio de Firma y Verificación de Firma corporativo (DUMAS).
- Centro de Autorizaciones de JAVATO (jCentroAutorizacion).
- Servicio de Autenticación corporativo (PASE).
- Punto de Acceso General (PAG).
- Plataforma estatal de representación, habilitación y apoderamiento (Represent@).

Detalle de la migración de los formularios implantados actualmente en la plataforma eA (H3). Incluye la migración de hasta 10 formularios, entre los cuales estarán los siguientes:

- 0000-11 Solicitud genérica.
- 0000-21 Tramitación en un expediente ya iniciado.
- 0000-31 Desistimiento o renuncia.
- 0000-41 Carta de pago.
- TEST-31 Formulario de test de la aplicación.

Detalle de la migración de las certificaciones implantadas actualmente en la plataforma eA, tanto de las consumidas a partir de la Plataforma de Intermediación estatal o externas, como de las generadas a partir de los sistemas de información de la CARM o internas (H3):

- Incluye la migración de los procesos de consulta de cada certificación externa.
- Incluye el proceso de generación de cada certificación interna.
- Incluye los formularios de consulta para los funcionarios de todas las certificaciones, internas y externas.
- Incluye los formularios de consulta para los ciudadanos de las certificaciones internas.
- Ver Anexo III para una relación completa de las certificaciones actuales.

Detalle de la migración de los servidores eSatélites (H4):

- Ver Anexo IV para una relación de los mismos, y de las funcionalidades que incluye cada uno.

Detalle de las funcionalidades requeridas en la implantación de un ESB / Gestión de API (H5):





- Seguridad y autorizaciones. En concreto, se incorporará la gestión de autorización a todos los servicios de la plataforma, además de los servicios corporativos de firma y validación de firma (DUMAS), Portafirmas y Registro de Entrada y Salida.
- Activación/desactivación de servicios. En concreto, se incorporará la gestión de activación/desactivación a todos los servicios de la plataforma, además de los servicios corporativos de firma y validación de firma (DUMAS), Portafirmas y Registro de Entrada y Salida.
- Transformación de mensajes. En concreto, se implementarán dos casos de transformación de mensajes, a elegir conjuntamente entre la CARM y el adjudicatario.
- Gestión de Alertas. En concreto, se implementarán dos casos de gestión de alertas, a elegir conjuntamente entre la CARM y el adjudicatario.
- Gestión de Transacciones. En concreto, se implementarán dos casos de gestión de transacciones, a elegir conjuntamente entre la CARM y el adjudicatario.
- Gestión de Sincronización. En concreto, se implementarán dos casos de gestión de sincronización, a elegir conjuntamente entre la CARM y el adjudicatario.
- Gestión de Mensajería. En concreto, se implementarán dos casos de gestión de mensajería, a elegir conjuntamente entre la CARM y el adjudicatario.
- Orquestación (servicios complejos). En concreto, se implementarán dos casos de orquestación de servicios, a elegir conjuntamente entre la CARM y el adjudicatario.
- Auditoría e información de uso de los servicios y los datos. En concreto, se incorporará la auditoría de uso a todos los servicios de la plataforma, además de los servicios corporativos de firma y validación de firma (DUMAS), Portafirmas y Registro de Entrada y Salida.
- Monitorización (tests de alto nivel). En concreto, se incorporará la monitorización de uso a todos los servicios de la plataforma, además de los servicios corporativos de firma y validación de firma (DUMAS), Portafirmas y Registro de Entrada y Salida.

Detalle de las funcionalidades requeridas en la implantación de un Cuadro de mando (H6):

- El cuadro de mando tendrá una doble perspectiva:
 - Información de uso de los servicios.
 - Información del estado de los servicios (monitorización).
- La información sobre uso de los servicios tendrá las siguientes características:
 - Se basará en los servicios descritos en PAECARM.
 - Cada servicio se podrá subdividir por atributos como el procedimiento, canal, tipo de destinatario y otros.
 - Incluirá la perspectiva temporal.





- La información sobre el estado de los servicios tendrá las siguientes características:
 - Las aplicaciones a monitorizar serán las objeto de este contrato, y además los servicios corporativos de firma y validación de firma (DUMAS), Portafirmas, Registro de Entrada y Salida y Gestor Documental (SANDRA) y el Servicio de Autenticación corporativo (PASE).
 - Se monitorizará a tres niveles: aplicaciones, servicios de dichas aplicaciones y atributos de dichos servicios.
 - Para cada uno de los anteriores se comprobará si está funcionando o no, y el tiempo de respuesta (integrando la solución con el sistema de monitorización de la CARM, basado en Icinga). Se podrán indicar umbrales mínimos o máximos que ayuden a la toma de decisiones.
 - Para las llamadas a servicios externos se comprobará si está funcionando o no, y el tiempo de respuesta (integrando la solución con el sistema de monitorización de la CARM, basado en Icinga). Se podrán indicar umbrales mínimos o máximos que ayuden a la toma de decisiones.
 - También se monitorizará la demanda (dimensiones: tiempo, demandante, procedimiento).
 - Asimismo, se establecerán relaciones de dependencia entre aplicaciones, servicios y elementos.
- Las tecnologías a utilizar serán las siguientes:
 - Extracción: a partir de Base de Datos y de logs de aplicación. Se utilizarán herramientas de código abierto como Logstash y desarrollos a medida.
 - Almacenamiento. Se utilizará Elasticsearch.
 - Visualización. Se utilizarán herramientas de código abierto como Kibana y desarrollos a medida.

Como resumen de los anexos mencionados, para obtener información más detallada de alguno de los apartados anteriores, se pueden consultar los siguientes:

- La descripción de la Plataforma eA actual se encuentra en el Anexo I.
- La relación de servicios electrónicos que se incluyen en el marco del PAECARM se encuentra en el Anexo II.
- La relación completa de certificaciones a migrar se encuentra en el Anexo III.
- La relación completa de eSatélites a migrar se encuentra en el Anexo IV.

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.

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

El framework utilizado en la CARM para el desarrollo de aplicaciones web en Java siguiendo el patrón MVC se denomina JAVATO, y su descripción puede consultarse en el anexo V. El adjudicatario puede proponer el framework de desarrollo de aplicaciones web o bien utilizar JAVATO.

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

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 un Look&Feel común, y deberán ajustarse a las normas de estilo que estén vigentes.

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 Cronograma e hitos del contrato

Para cada hito del contrato, el licitador deberá establecer una planificación siguiendo la metodología Métrica V3, contemplando las siguientes fases:

1. Análisis y diseño
2. Desarrollo
3. Documentación
4. Formación
5. Implantación

Si la empresa licitadora propone otra metodología, que considere más adecuada o que complemente a Métrica V3, definirá la planificación según lo establecido en dicha metodología.

4. Metodología a utilizar en la ejecución

El proyecto se ejecutará utilizando la metodología Métrica v3, estándar en las Administraciones Públicas.

La empresa licitadora podrá proponer otra metodología que considere más adecuada o que complemente a Métrica, estando el uso de esta alternativa supeditado a la decisión del responsable del contrato.

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 de 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 Tratamientos por cuenta de terceros

El adjudicatario queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre cualquier dato que pudiera conocer con ocasión del cumplimiento del contrato.

En caso de tratamiento de datos de carácter personal, incluidos en ficheros declarados ante la Agencia de Protección de Datos y dados de alta en el correspondiente Registro General de Protección de Datos, no los podrá copiar o utilizar con fin distinto al previsto en el contrato, ni tampoco ceder a otros ni siquiera a efectos de conservación.

De conformidad con la Disposición Adicional vigésimo quinta de la ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, el adjudicatario quedará obligado al cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal y su normativa de desarrollo, contenida en el Real Decreto 1720/2007, de 21 de diciembre, y especialmente a lo establecido en el artículo 12, apartados 2, 3 y 4 de la citada Ley Orgánica, y artículos 20, 21, 22 y 82 del citado Real Decreto.





En cualquier caso la Administración podrá auditar en cualquier momento el nivel de cumplimiento por parte del contratista de las medidas de seguridad que éste tiene obligación de implementar.

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 adjudicatario deberá, previo al inicio de la ejecución del contrato, designar y comunicar al responsable del contrato la persona o personas que, sin perjuicio de la responsabilidad propia de la empresa, estarán autorizadas para las relaciones con el centro directivo a efectos del uso correcto del material y de la información a manejar. Se adjuntará una descripción de su perfil profesional, y sólo podrán ser sustituidas con la conformidad del responsable del contrato.

El adjudicatario se compromete a comunicar al responsable del contrato, de forma inmediata, la detección de cualquier error que se produzca en el sistema de seguridad de la información.

7.2 Cumplimiento de los Esquemas Nacionales de Seguridad e Interoperabilidad

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) y en el Real Decreto 4/2010, de 8 de enero, sobre el Esquema Nacional de Interoperabilidad (ENI), en lo referido a la adopción de medidas de seguridad e interoperabilidad de los servicios de administración electrónica afectados por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, incluidos en el objeto del pliego.

El adjudicatario garantizará los principios básicos y requisitos mínimos de protección requeridos en el Esquema Nacional de Seguridad, para una protección adecuada de la información. Es de aplicación que el adjudicatario garantice el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en aquellos medios electrónicos de los que sean responsables o sobre los que realizan la prestación de servicios.

El nivel de implantación de las medidas vendrá determinado por la categorización del sistema de información, determinado conforme a lo establecido en el Anexo I del Esquema Nacional de Seguridad por el órgano competente sobre la valoración e importancia de la información que se maneja y los servicios prestados por el adjudicatario en la ejecución del pliego.

La Administración se reserva el derecho de auditar en cualquier momento el nivel de cumplimiento de las medidas de seguridad, así como de las exigidas en los Reales Decretos 3/2010 y 4/2010 antes mencionados.

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





Región de Murcia
Consejería de Hacienda

Dirección General de Informática,
Patrimonio y Telecomunicaciones

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.

Murcia, (fecha y firma en el margen izquierdo)

EL JEFE DE 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.: Vicente Rodes Belmonte

03/05/2018 08:55:52
Firmante: PEDRO OLIVARES SANCHEZ, PEDRO
Firmante: VICENTE RODES BELMONTE, VICENTE

Esta 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 introduciendo el código seguro de verificación (CSV) 24-0904d-aa03-0158-26825449468





Anexo I. Descripción de la Plataforma eA actual

La plataforma eA está basada en el patrón SOA (Service Oriented Architecture). Los servicios proporcionados a través de la plataforma "eA" se pueden clasificar en Servicios de Infraestructura y Servicios Finales.

SERVICIOS DE INFRAESTRUCTURA

Son aquellos que ofrecen funcionalidades 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 de infraestructura es:

- Autenticación
- Registro telemático
- Firma electrónica / Verificación de firma
- Cifrado
- Pasarela de pagos
- Gestor de Formularios
- eSatélites (Interfaz con Back-Office)
- Gestor documental/Custodia documental

También se incluyen aquí aquellas aplicaciones genéricas donde se implementan, parametrizan y sobre las que se ejecutan los servicios finales:

- Tramitador de solicitudes
- Gestor de Notificaciones telemáticas
- Plataforma de Interoperabilidad (Certificaciones electrónicas)
- Consultador de Expedientes
- Consultador de Documentos

SERVICIOS FINALES

Dichos servicios tienen un propósito específico, para diferenciarlos de los Servicios de Infraestructura que les dan soporte. Son los servicios que están disponibles para ciudadanos, empresas, funcionarios,...

Se consideran Servicios Finales:

- Trámites electrónicos de presentación
- Notificaciones telemáticas
- Certificaciones electrónicas
- Consulta de Expedientes

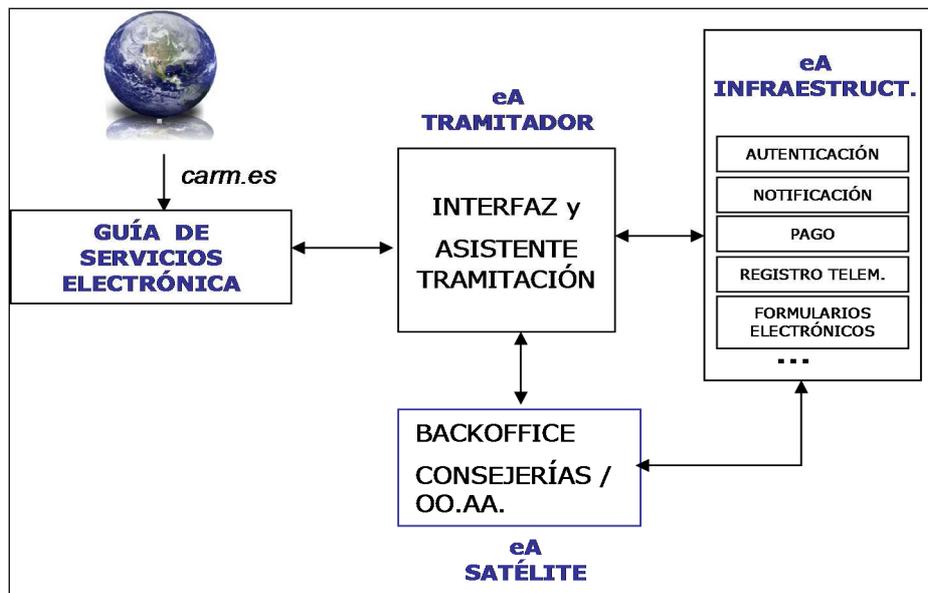


- Consulta de Documentos

A continuación se detallan los Servicios Finales más relevantes.

TRÁMITES ELECTRÓNICOS DE PRESENTACIÓN

El modelo de prestación de servicios de Tramitación de solicitudes a través del portal administrativo *carm.es* presenta el siguiente esquema funcional:



Los distintos elementos del esquema anterior presentan las siguientes funciones:

- **Guía de Servicios Electrónica:** catálogo de procedimientos publicado en el portal administrativo *carm.es*, que pretende dar una visión completa y unificada de los servicios que proporciona la CARM a los ciudadanos y empresas, a la vez que constituye un punto de entrada para la tramitación telemática de los mismos a través del mencionado portal.
- **Plataforma eA–Infraestructura:** proporciona los servicios básicos y funcionales necesarios para los procesos de tramitación telemática (autenticación, firma, registro telemático, pago, notificación telemática, consulta de expedientes,...).
- **Plataforma eA–Tramitador:** constituye el frontal de servicios de eAdministración y tiene como objetivo normalizar la capa de presentación proporcionando un asistente en la tramitación de los servicios, guiando y haciendo visibles todas las fases del trámite al ciudadano. Además integra los servicios proporcionados por la plataforma eA y gestiona las relaciones con los diferentes Back-Office.
- **Plataforma eA–Satélites:** son los clientes de los servicios de eAdministración ubicados en las Consejerías y Organismos Autónomos de la CARM. Se relacionan con la plataforma eA a través del Tramitador mediante Servicios Web para la



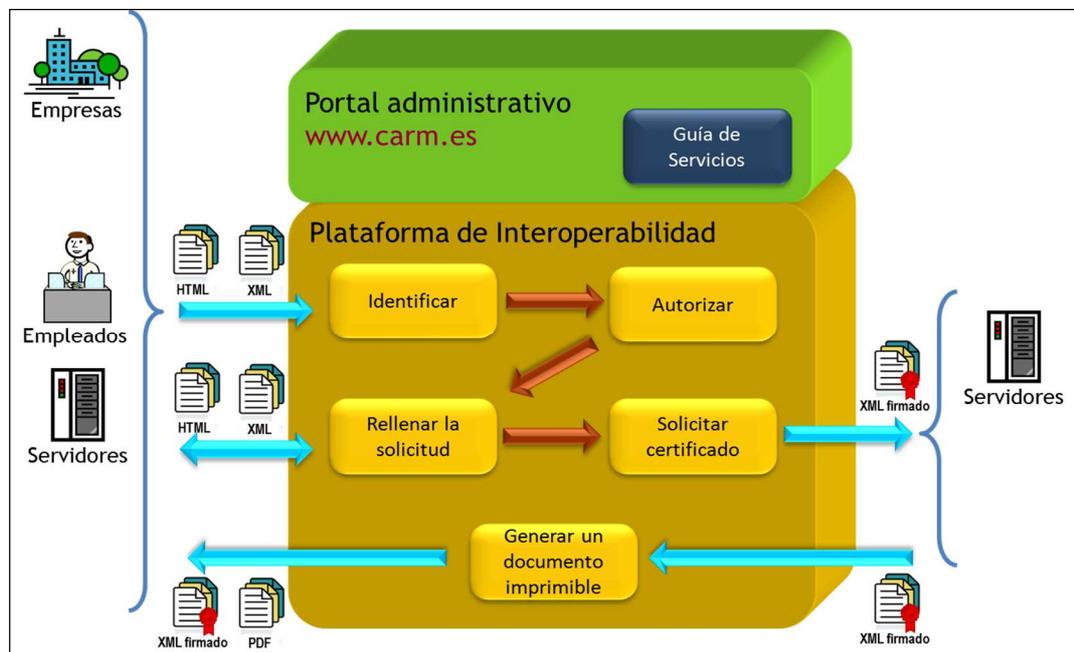
entrega de datos, gestión de listas de valores, validaciones complejas de campos de formularios, etc. Además pueden usar directamente, también a través de Servicios Web, los servicios de la plataforma eA (notificación telemática, consulta de expedientes,...) para completar los servicios de tramitación a ciudadanos, empresa, funcionarios,...

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:



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:

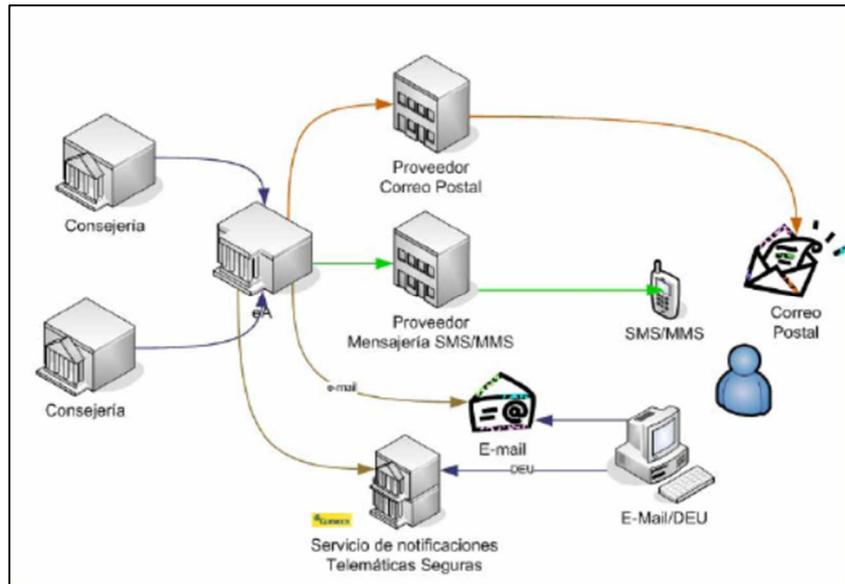
- SMS.
- Correo electrónico.
- Push (aplicaciones móviles).
- Notificaciones telemáticas legales (de acuerdo al art. 43 de la Ley 39/2015).

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:





Región de Murcia
Consejería de Hacienda

Dirección General de Informática,
Patrimonio y Telecomunicaciones

Anexo II. Plan Estratégico de Administración Electrónica de la CARM

La información sobre el Plan Estratégico de Administración Electrónica de la CARM se puede consultar en <http://transparencia.carm.es/web/transparencia/-/plan-estrategico-de-administracion-electronica-de-la-carm>

En concreto, los servicios de la nueva plataforma están descritos en el Documento de Proyecto y en el Plan Operativo.

02/05/2018 20:52:47 Firmante: RODES BELMONTE, VICENTE

Esta 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 introduciendo el código seguro de verificación (CSV) 24-0994d-aa03-0158-26825449468





Anexo III. Certificaciones a migrar

La relación de las certificaciones actuales en la Plataforma de Interoperabilidad emitidas por organismos externos es la siguiente:

Certificación	Formulario Funcionario	Organismo emisor	Descripción
AEATIR01	I018-20	AEAT	Certificado del I.R.P.F.
DOMFISC	I095-20	AEAT	Obtención del domicilio fiscal
ECOT101I	I012-20	AEAT	Corriente de pago de las obligaciones tributarias para Contratos con las Administraciones Públicas
ECOT102I	I013-20	AEAT	Certificado de Obligaciones tributarias para obtención de licencias de transporte.
ECOT103I	I014-20	AEAT	Certificado de Obligaciones tributarias para solicitud de ayudas y subvenciones
ECOT104I	I015-20	AEAT	Certificado de Obligaciones tributarias para tramitación de permisos de residencia y trabajo para extranjeros
IAE10	I093-20	AEAT	Certificado de Impuesto de Actividades Económicas 10 epígrafes
NIVRENTI	I031-20	AEAT	Certificado de Nivel de Renta Intermediado
SVDCDYGWS02	I011-30	Catastro	Descriptiva y Grafica del catastro
SVDCTITWS02	I009-30	Catastro	Consulta de Certificación de Titularidad del Catastro
SVDCCAACPASWS01	I037-20	CC. AA.	Certificado de estar al corriente de pago de obligaciones tributarias para ayudas y subvenciones. Comunidades Autónomas
SVDCCAACPCWS01	I039-20	CC. AA.	Certificado de estar al corriente de pago de obligaciones tributarias para la contratación. Comunidades Autónomas
SVDSCDDWS01	I035-20	CC. AA.	Consulta de datos de Discapacidad. Comunidades Autónomas
SVDSCTFNWS01	I036-20	CC. AA.	Consulta del título de familia numerosa. Comunidades Autónomas
SVDDGPCIWS02	I001-30	D. G. Policía	Consulta de Datos de Identidad
SVDTNUWS03	I004-30	Educación	Certificados de Títulos No Universitarios
SVDTUWS03	I003-30	Educación	Certificados de Títulos Universitarios
SVDREXTFECHAWS01	I029-20	INE	Consulta de datos de residencia con fecha de la última variación
Q2827002CINSS001	I025-20	INSS	Consulta de las prestaciones del Registro de Prestaciones Sociales Públicas, Incapacidad Temporal y Maternidad
SVDCDEPENWS01	I024-20	INSS	Consulta del Nivel y Grado de Dependencia
SVDELSEXWS01	I032-20	Justicia	Consulta de Inexistencia de Antecedentes Penales por Delitos Sexuales
SVDNOTCOPSIMWS01	I038-20	Notarios	Poderes notariales. Copia simple
SVDNOTSUBWS01	I040-20	Notarios	Poderes notariales. Subsistencia de Poderes Notariales
SVDSCCDWS01	I028-20	Registro Civil	Consulta de defunción





SVDSCCMWS01	I027-20	Registro Civil	Consulta de matrimonio
SVDSCCNWS01	I026-20	Registro Civil	Consulta de nacimiento
SVDSEPEDEMFECHAWS01	I030-20	SEPE	Consulta de Inscripción como demandante de empleo a Fecha concreta
SVDSEPEIACTWS02	I006-30	SEPE	Consulta de importes actuales de desempleo
SVDSEPEIPERWS02	I007-30	SEPE	Consulta de importes percibidos por periodos de desempleo
SVDSEPEISITWS02	I005-30	SEPE	Consulta de datos de desempleo
Q2827003ATGSS001	I016-20	TGSS	Certificado de corriente de pago con la seguridad social

Y la relación de las certificaciones generadas por la administración regional:

Certificación	Formulario Funcionario	Formulario Ciudadano	Organismo emisor	Descripción
1635-C1	1635-20	1635-10	ATRM	Estar al corriente de las obligaciones fiscales con la CARM
SVDCCAACPASW S01-INTERNO			ATRM	Certificado de estar al corriente de pago de obligaciones tributarias para ayudas y subvenciones, en Intermediación
SVDCCAACPCWS 01-INTERNO			ATRM	Certificado de estar al corriente de pago de obligaciones tributarias para la contratación, en Intermediación
2041-C1	2041-20	2041-10	Función Pública	Consulta de ejercicios aprobados en pruebas selectivas
2100-C1		2100-40	Función Pública	Pre-certificado de méritos para concurso
2460-C1	2460-20	2460-10	Función Pública	Consulta de Servicios Previos - Anexo I
NCP-C1		NCP-10	Función Pública	Nómina de empleado público
0019-C1	0019-20	0019-30	Industria	Inscripción de instalación eléctrica de baja tensión
0027-C1	0027-20	0027-10	Industria	Inscripción de instalación de distribución y utilización de combustibles gaseosos
0061-C1	0061-20	0061-10	Industria	Inscripción de instalación térmica en edificio
0987-C1	0987-20	0987-10	Industria	Inscripción de instalación radiactiva
1100-C2	1100-20	1100-10	IMAS	Discapacidad
1755-C1	1755-20	1755-50	IMAS	Pensiones no contributivas
SVDSCDDWS01-INTERNO			IMAS	Consulta de datos de Discapacidad en Intermediación
1785-C1	1785-20		Presidencia	Registro de asociaciones
0668-C1	0668-20	0668-10	Sanidad	Familia Numerosa
SVDSCTFNWS01-INTERNO			Sanidad	Consulta del título de familia numerosa en Intermediación





Anexo IV. eSatélites a migrar

La relación de los satélites actuales, junto con los servicios en uso en cada uno de ellos es la siguiente:

Satélite	Servicio				
	NOTI	CCER	ECER	RSMS	CEXP
Agricultura – eSatIo	X	X			
ATRM – eSatFobos	X	X	X		
Educación – eSatTitan	X	X		X	
Fomento – eSatTetis	X	X			
Hacienda – eSatLuna	X	X	X	X	X
IMAS – eSatEncelado	X	X	X		X
Industria – eSatMimas	X	X	X		X
Presidencia – eSatEuropa	X	X	X		
Sanidad – eSatCalisto	X	X	X		
SEF – eSatDeimos	X	X			
SMS – eSatRea	X	X			
Trabajo - eSatTrabajo	X	X			
Turismo – eSatGanímedes	X	X			

Donde los servicios son los siguientes:

- NOTI - Notificaciones: Envío de notificaciones legales (para comparecencia en sede o Dirección Electrónica Habilitada), así como comunicaciones SMS, eMail y Push.
- CCER - Consulta de Certificado: Consultas automatizadas a la Plataforma de Interoperabilidad.
- ECER - Emisión de Certificado: Consultas de datos al Back-Office para emitir un certificado de la Plataforma de Interoperabilidad.
- RSMS - Recepción de SMS: Recepción de un SMS y envío al Back-Office.
- CEXP - Consulta de Expedientes: Publicación de los datos de un expediente en 'Como va lo mío'.





Anexo V. Descripción del framework JAVATO

ENTORNO FUNCIONAL. ESPECIFICACIÓN DE REQUISITOS

JAVATO es un framework para desarrollo de aplicaciones web en Java siguiendo el patrón MVC:

- Modelo: Hibernate, JPA
- Vista: JSF
- Controlador: Spring

En el momento de redacción de este documento, las versiones disponibles son:

- Java 8
- Hibernate 5
- JPA 2.1
- JSF 2
- Spring 4

Los principales componentes horizontales del framework JAVATO en su versión actual (Javato 3) y los requisitos que cubren son:

- Gestión de seguridad (jCentroAutorizacion)
- Generador de aplicaciones dinámicas (jAD)
- Generador de informes (jInformes)
- Gestor de tareas (jTareas)
- Lanzamiento auditado de scripts contra base de datos (jTraspaso)
- Editor CRUD de tablas (jEditor)

En JAVATO se puede desarrollar de 3 formas diferentes:

- A partir de la semilla (jSemilla), desarrollo en JEE "tradicional"
- Usando el componente jAD
- Usando otra tecnología y utilizando los componentes de JAVATO mediante servicios web

A continuación se detallan los módulos más relevantes.

GESTIÓN DE SEGURIDAD (jCentroAutorizacion)

- Autenticación





- Todas las aplicaciones se autentican de la misma manera.
- Es posible usar login/password y/o cualquier certificado digital reconocido por la plataforma de Administración Electrónica de la CARM.
- Usa Single Sign-On (CAS) para que los usuarios solo se tengan que identificar una vez.
- Autorización
 - Se tiende a usar una misma administración de permisos para todas las aplicaciones, de manera que en un mismo sitio se pueda controlar todos los permisos de una persona, esto es independiente de cómo estén físicamente distribuidos los datos.
 - Se define una estructura genérica de permisos a la que se puedan incorporar el máximo número de aplicaciones.
 - La seguridad se puede gestionar desde JAVATO o aprovisionarse desde las aplicaciones.
 - Se contemplan estructuras organizativas genéricas (con posibilidad de que provengan de fuentes de información externa), que se pueden compartir, estructuras organizativas propias de aplicaciones, así como la asociación de personas a éstas.
 - Se permiten estructuras organizativas en forma de árbol y gestionar la herencia propia de ellas.
 - Se gestionan permisos y sus agrupaciones (para asignarlos más fácilmente a las personas), bien directamente, bien a través de las estructuras organizativas a las que pertenecen.
 - Se puede distinguir entre a quién se le da un permiso y sobre quién se va a poder usar, y ofrecerlo a las aplicaciones.
 - Se puede dar permisos a vínculos o características concretas asociadas a las estructuras organizativas (determinados tipos de puestos, responsables,...).
 - Se ofrece un mecanismo (selectores) para que las aplicaciones puedan gestionar distintos roles de conexión de una misma persona a determinada aplicación.
 - Se permite tener administradores parciales para una aplicación para que gestionen únicamente determinadas personas, perfiles o estructuras organizativas.
 - Es posible exportar las estructuras, permisos y relaciones entre ellas a contenedores externos, como por ejemplo un LDAP.
 - Se incluye una gestión de elementos comunes usados por las aplicaciones, como por ejemplo las cadenas de conexión a bases de datos (denominadas "entornos").





GENERADOR DE APLICACIONES DINÁMICAS (JAD)

Es una herramienta de desarrollo rápido de aplicaciones (MDD, Model-Driven Development), con la que la vista de las aplicaciones se desarrolla y mantiene mediante parametrización y se programa el Controlador y el Modelo de las aplicaciones (reglas de negocio):

- En la parametrización se tienen pantallas, zonas de operación y menús.
- Dentro de las zonas de operación se disponen los elementos: Distintos tipos de entrada/salida (cajas de texto, desplegados, ficheros,...) y botones genéricos o personalizados.
- Cada zona de operación se basa en una entidad (tabla) y sus relacionadas a cualquier nivel.
- Cada elemento de la zona tiene una serie de propiedades a completar.
- Se ofrece continuamente imagen del resultado final según se diseña (WYSIWYG).
- Las zonas de operación se pueden relacionar entre sí, por ejemplo para un maestro-detalle o filtro-resultado.
- Los procedimientos de las reglas de negocio pueden usar como parámetros de entrada / salida los elementos de la zona de operación o variables de entorno.
- Está integrada con el componente "Generador de informes"

GENERADOR DE INFORMES (jInformes)

- Dispone de interfaz de aplicación y de servicios web, de forma que las aplicaciones que lo invocan, de cara al usuario pueden usar su propia interfaz.
- La interfaz de aplicación puede usarse directamente o llamado por una aplicación, bien llamando a un informe concreto, bien a la lista de informes disponibles para que se seleccione uno.
- Posibilidad de elegir lanzar el informe on-line o en batch.
- Cuando vaya en batch, puede tener distintas colas con políticas de hora y amplitud parametrizables.
- Uso de gestión de autorizaciones corporativa con posibilidad de elegir, al conectarse, entre uno de los distintos roles asignados para ver los informes que tiene permiso.
- Los permisos se dan por aplicación cliente, no sobre la aplicación de informes propiamente.
- El esquema de base de datos al que se conecta cada informe es parametrizable.
- Se dispone de una pantalla de petición de parámetros y lanzamiento genérica o personalizada por aplicación/informe.
- Los parámetros pueden llevar listas de valores obtenidas de consultas a bases de datos así como enlazar distintos parámetros dependientes (por ejemplo, provincia-municipio).





- Parámetros de sistemas (persona conectada, rol con el que está conectado,...). Por ejemplo, para que el informe saque los datos de "Presidencia" sin que el usuario pueda cambiar este filtro.
- Se permite enviar al Portafirmas corporativo de la CARM los informes, con envío de correo al que hizo la petición (distinta del que firma) cuando está firmado y un sitio donde recogerlo firmado.
- Existen distintos tipos de orígenes de datos (procedimientos de bases de datos, consulta SQL) y son ampliables.
- Existen distintos tipos de formatos de salida (PDF, Excel, ODT) y son ampliables.
- Existen distintos tipos de generadores de formatos de salida y ampliables. Dos tipos básicos:
 - Informes rápidos tabulares, indicando declarativamente estructura de salida con posibilidad de marcar campos como cabecera, con acumulados, sumas, parciales y con logotipo/escudo parametrizable.
 - Informes hechos con alguna herramienta de tipo gráfico con plantillas, como Libre Office con algún lenguaje de marcas para iteración o condicionamiento según los datos (if) (como Free marker), o como la herramienta BIRT
- Se usa siempre la misma estructura intermedia de datos (XML) para que se pueda hacer cualquier mezcla de origen de datos con tipo de salida.
- Es posible incorporar generadores de datos ya hechos, mediante conversores a la estructura intermedia, lo que permite partir de generadores CSV o similares de los que ya se dispusiera.
- Se pueden asociar palabras clave a los informes y realizar búsqueda por ellas.

GESTOR DE TAREAS (jTareas)

- Dispone de interfaz de aplicación o de servicio web. Las aplicaciones, de cara al usuario, podrán usar su propia interfaz.
- Es posible definir las colas por aplicación así como las políticas de número de trabajos paralelos y tiempo de ejecución.
- Se dispone de distintos tipos de tareas:
 - Procedimientos de base de datos
 - Shell script
 - Informes
- Se usa la gestión de autorizaciones corporativa con posibilidad de elegir, al conectarse, entre uno de los distintos roles asignados para ver las tareas que tiene permiso.
- Los permisos sobre las tareas deben estar basadas en los selectores definidos para el componente "Gestión de seguridad".
- El esquema de base de datos al que se conecta cada tarea es parametrizable.
- Pueden definirse tareas periódicas.





Región de Murcia
Consejería de Hacienda

Dirección General de Informática,
Patrimonio y Telecomunicaciones

- Se integración con el Portafirmas corporativo de la CARM para enviar documentos a firmar y recogerlos firmados.



Anexo VI. 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
    <configuration>
        <property name="desarrollo" value="/desarrollo">>
            <property name="concatenar.properties" value="ficheros de configuración">>
        </property>
    </configuration>
    <configuration>
        <property name="pruebas" value="/pruebas">>
            <property name="ficheros de configuración" value="ficheros de configuración">>
        </property>
    </configuration>
    <configuration>
        <property name="produccion" value="/produccion">>
            <property name="ficheros de configuración" value="ficheros de configuración">>
        </property>
    </configuration>
```

- 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.





REPOSITORIOS 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

