Pliego de prescripciones técnicas para la contratación de los servicios que proporcionen la puesta en marcha y funcionamiento del nuevo Sistema de Información de Gestión y Recaudación de Tributos de la Diputación de Valencia

26 de Septiembre de 2013

SUMARIO

1 Introducción

1.1 Objeto y codificación

El objeto de la licitación es la contratación de los servicios que proporcionen un nuevo **Sistema de Información de Gestión y Recaudación de Tributos (SIGTR en adelante**) de la Diputación de Valencia para las entidades locales, consorcios y demás instituciones (EELL en adelante) que delegan los servicios tributarios, siguiendo un modelo de prestación de servicio de Software como un Servicio (SaaS[1] siglas en inglés) y un modelo de despliegue de nube privada (Private cloud [1] en inglés), que incluyen los servicios de infraestructura, plataforma tecnológica y soporte de operación necesarios.

El objeto del contrato se identifica con el código **CPV 72510000-3 –** "Servicios de gestión relacionados con la informática" a que se refiere el artículo 10 en relación con el anexo II del TRLCSP.

El adjudicatario que preste los servicios deberá desplegar, configurar, migrar los datos actuales, mantener y actualizar el funcionamiento adecuado del SIGTR mediante la infraestructura necesaria de la nube para que los servicios se suministren según los niveles de servicio esperados por la Diputación de Valencia.

El adjudicatario asume las responsabilidades, extremo a extremo, en la gestión y el control del SIGTR, así como de los componentes en todas las capas de las tecnologías de entrega de la nube (red, hardware y software).

Por lo tanto, la Diputación de Valencia e IMELSA, no gestionarán ni serán responsables de los sistemas tecnológicos, comunicaciones ni de las aplicaciones necesarias, más allá de las capacidades de gestión de usuarios, configuración y personalización del SIGTR que ofrece el adjudicatario.

El licitador proporcionará una solución que deba incluir, al menos:

- El software necesario que cubra los requerimientos funcionales y técnicos descritos en el apartado 2.1 y el proyecto de implantación del SIGTR y establecimiento del servicio necesario.
- El hardware y las comunicaciones que requiere el software propuesto.
- El servicio de soporte operativo necesario.
- El compromiso y garantía del nivel de servicio.

[1] SP800-145 NIST Definition of Cloud Computing

1.2 Contexto

La Diputación de Valencia está emprendiendo un proyecto de evolución tecnológica de su sistema de información de Gestión Tributaria que cubra las necesidades actuales y futuras de las EELL y del contribuyente, alineado con las principales tendencias del mercado de las tecnologías de la información actuales.

Por ello, la Diputación de Valencia está interesada en trasladar a un entorno de computación en la nube, un nuevo SIGTR y sus servicios relacionados, como parte de una provisión más amplia de Servicios Tributarios a las EELL y a los ciudadanos, racionalizando las Tecnologías de la Información de la administración local, reduciendo duplicidades en esfuerzos y costes, y resolviendo los problemas que generan los sistemas actuales.

La solución a proporcionar será compartida con los usuarios de la Diputación de Valencia, EELL de Valencia y el ciudadano, utilizando el mismo sistema de información. El objetivo de esta puesta en común de los recursos tecnológicos, permitirá un uso más eficiente de hardware, software y servicios, generando economías de escala.

Todo ello redundará en una mejora, tanto de tareas internas (peticiones de usuarios, soporte técnico de sistemas,.. etc.), como el servicio ofrecido a los ciudadanos (gestión, recaudación, etc.).

Los objetivos generales que persigue con ello el Servicio de Gestión Tributaria de la Diputación de Valencia (SGT en adelante) de la Diputación de Valencia para mejorar el área de la Gestión Tributaria actual son:

- Mejorar la orientación al contribuyente y al servicio.
- Mejorar la disponibilidad de los servicios tributarios.
- Mejorar la funcionalidad de los procesos de Gestión Tributaria.
- Facilitar el trabajo colaborativo entre la EELL y el Servicio de Gestión Tributaria.
- Cumplir con las leyes y regulaciones externas.
- Innovar
- Mejorar la integración (interoperabilidad) entre el sistema de información de Gestión Tributaria y los sistemas de gestión contables municipales y de la propia Diputación de Valencia.

Por su parte, el Servicio de Informática y Organización (SIO en adelante) de la Diputación de Valencia, es actualmente responsable de asegurar los recursos de la

Tecnología de la Información para el Servicio de Gestión Tributaria, dispone de los siguientes objetivos alineados con los anteriores:

- Asegurar la satisfacción de los usuarios de SGT con niveles de servicio prestados.
- Asegurar que la información de Gestión Tributaria crítica y confidencial está a salvo de los accesos no autorizados, es integra y está disponible cuando se requiere
- Asegurar que las transacciones automáticas y los intercambios de información son seguros.
- Asegurar un impacto mínimo sobre el negocio cuando se produzca un cambio o indisponibilidad en el servicio directa o indirectamente.
- Asegurar que los servicios proporcionados están disponibles cuando se requieren.
- Mejorar la gestión de cambios y peticiones de nuevos requerimientos de los usuarios.
- Optimizar el modelo operativo al Servicio de Gestión Tributaria a través de la definición de un nuevo modelo de servicios, medible y que aporten credibilidad.

El mapa de procesos de negocio actual del Servicio de Gestión Tributaria es el siguiente:

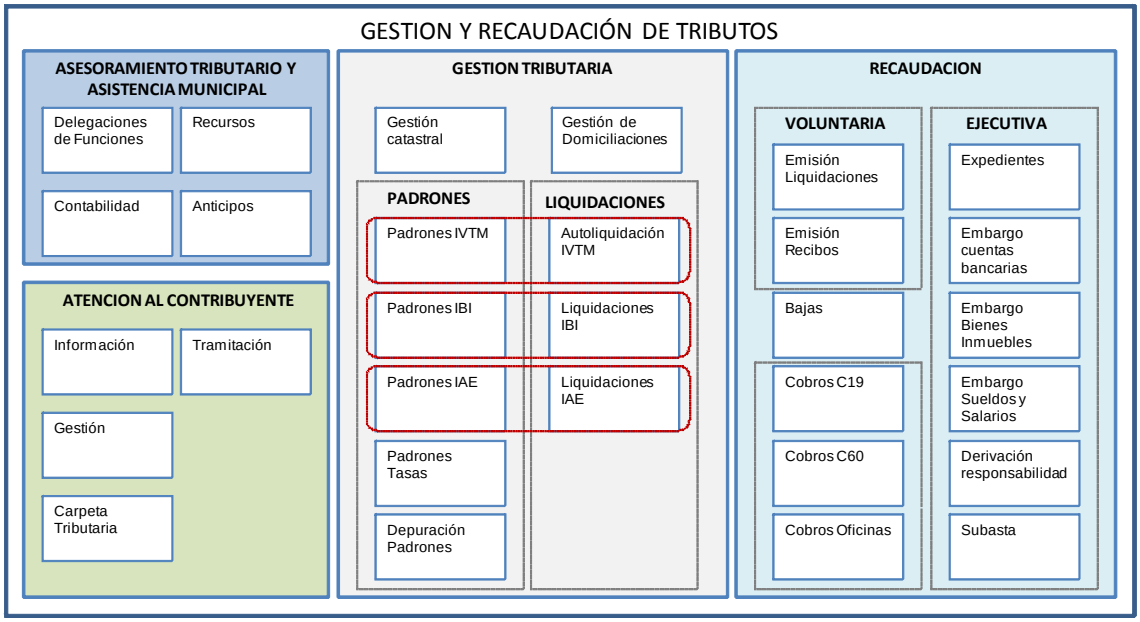


Tabla 1: Procesos actuales de Gestión y Recaudación Tributaria

El Sistema de Información de Gestión Tributaria actual se encuentra en la Diputación de Valencia, instalado en modo cliente/servidor en 8 servidores de *Citrix* dedicados,

repartidos en la granja "*Presentation Server 4.0*". El punto de acceso consiste en una interfaz web específica de *Citrix Secure Gateway*, que habilita el acceso a los aplicativos desde redes externas no gestionadas por la Diputación de Valencia.

Los datos residen en base de datos Oracle bajo sistema operativo AIX. Se dispone de un sistema de *reporting* con más de 500 informes que son usados por los distintos usuarios, bajo plataforma *Access* con *OLDB* contra Oracle, en un servidor con acceso Citrix.

Los servicios que proporciona a las EELL el SGT incluyen los siguientes impuestos que generan recibos o valores:

- IBI urbana y rústica.
- IVTM Impuesto sobre vehículos de tracción mecánica.
- Tasa de transferencia y valorización de residuos urbanos.
- Otras tasas (cementerios, mercados, vados, contribuciones especiales, cuotas de urbanización, etc.)
- IAE Impuesto de actividades económicas.
- Multas de tráfico (sólo recaudación ejecutiva).

Para que los licitadores puedan dimensionar adecuadamente las necesidades actuales como punto de partida, se facilita la siguiente información de volumetría:

- Volumen anual de recibos :
  - Ejercicio 2009: 1.436.518 recibos
  - Ejercicio 2010: 1.610.430 recibos
  - Ejercicio 2011: 1.766.888 recibos
  - Ejercicio 2012: 2.932.964 recibos

- Se dispone de 283 EELL que tienen delegado algún servicio de Gestión y Recaudación Tributaria en la Diputación de Valencia. Están trabajando con la gestión y recaudación de tributos actual unos 250 usuarios y unos 1.000 usuarios a nivel de consulta mediante la actual carpeta tributaria.

1.3 Necesidades administrativas a satisfacer con el objeto del contrato.

La Diputación Provincial de Valencia (Diputación de Valencia en adelante), en sesión de Pleno de 24 de abril de 2012, acordó ampliar la actual encomienda en materia catastral realizada a la empresa pública IMPULSO ECONÓMICO LOCAL, S.A. (IMELSA en adelante), al desarrollo de actividades complementarias inherentes a la gestión tributaria y recaudatoria que no impliquen ejercicio de autoridad. Una de las líneas de actuación es proporcionar la disponibilidad de un sistema de información y

cualquier otra actividad complementaria técnica o de servicio que permita ofrecer cobertura para prestar los servicios de administración electrónica en estas materias, y que asegure el funcionamiento continuado de los servicios en las distintas oficinas y centros de trabajo.

El Servicio de Gestión Tributaria (SGT) de la Diputación de Valencia tiene como misión principal la asistencia técnica y la cooperación en materia tributaria local con los municipios de la provincia que así lo soliciten, sobre todo con aquellos de menores recursos y capacidad económica, y más en estos momentos en que la coyuntura económica obliga a un ajuste de los medios municipales.

Para cumplir esa misión, el SGT, a través de IMELSA, pretende proporcionar un servicio eficiente que atienda a los contribuyentes en todas las materias del ciclo tributario desde cualquiera de sus oficinas y/o centros de atención.

Dado el volumen de trabajo, el incremento de los municipios solicitantes y la inclusión de nuevas delegaciones, IMELSA, de acuerdo a lo previsto en la ampliación de encomienda de la gestión en materia catastral, aprobada en el Pleno de la Corporación de la Diputación de Valencia de fecha 24 de abril de 2012, necesita la colaboración de empresas especializadas en la materia.

Con este contrato, la Diputación de Valencia e IMELSA posibilitan el objetivo del SGT de forma eficiente, garantizando el correcto funcionamiento y continuidad del servicio del SIGTR como herramienta fundamental para el desempeño de sus funciones.

La planificación conjunta y la coordinación efectiva entre IMELSA y el SGT, en el desempeño de las actividades de colaboración, será una garantía de integridad de los procesos de trabajo y de eficacia de los resultados a conseguir para los ayuntamientos y para la propia Diputación de Valencia. Asimismo el SIO, en coordinación con IMELSA, garantizará la compatibilidad de las soluciones desarrolladas con las líneas informáticas estratégicas de la Diputación de Valencia.

IMELSA, como responsable administrativo y garante técnico del contrato a licitar, dispone de los siguientes objetivos para desarrollar de forma eficaz y eficiente la encomienda:

- Garantizar que se entregan los proyectos y servicios siguiendo los plazos y los estándares de calidad.
- Asegurar el cumplimiento de las leyes y regulaciones que apliquen a la Diputación de Valencia, por parte de los prestadores de los servicios a licitar.
- Asegurar que se presta un servicio de calidad eficiente en costes, mejora continua y facilidad de adaptación al cambio.

- Asegurar que el nuevo modelo de servicios cumple las expectativas de la Diputación de Valencia.
- Asegurar la transparencia y el entendimiento de los niveles de servicio, validando el cumplimiento y exactitud de los Acuerdos de Nivel de Servicio (ANS en adelante)
- Gestionar los riesgos del contrato.
- Validar el cumplimiento de los acuerdos contractuales.

IMELSA designará un equipo de trabajo específico para la consecución de estos objetivos.

2 Características del Servicio a contratar

2.1 Alcance

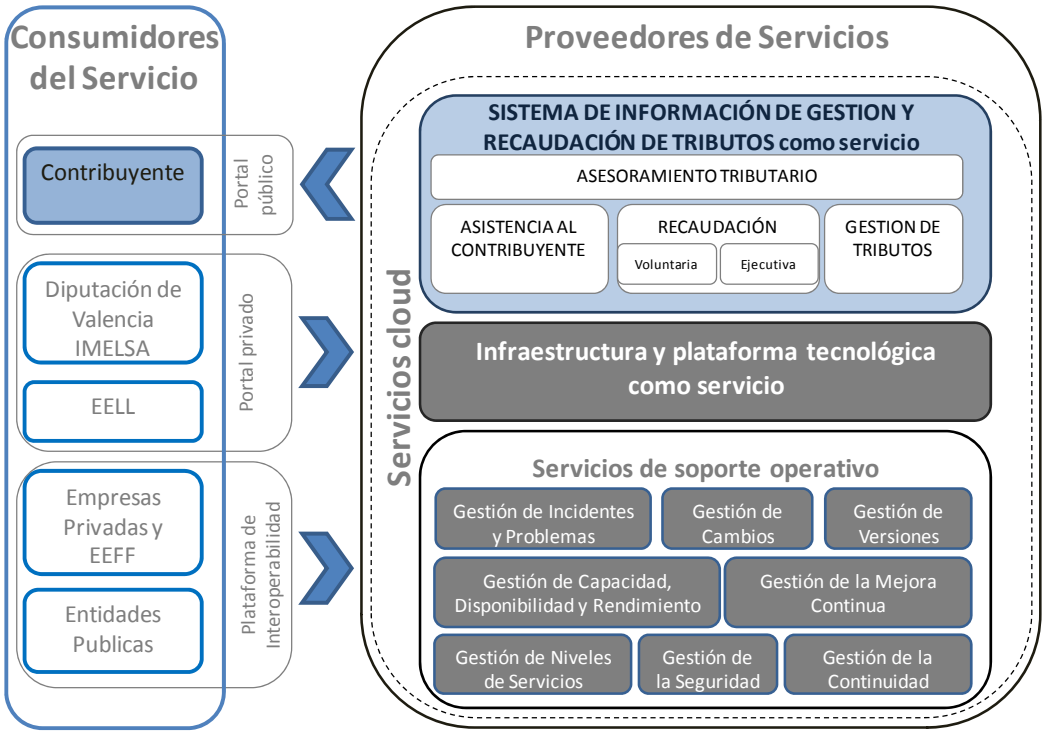
El alcance general de este pliego es disponer de un SIGRT como servicio, que incluya el software, infraestructura tecnológica, y soporte operativo necesarios para su correcto funcionamiento y evolución, para el SGT, EELL y el contribuyente. Asimismo, se considera que entra dentro del alcance, el proyecto para implementar el SIGTR migrar los datos actuales, ponerlo en producción y transformarlo en un servicio continuado.

IMELSA entiende que la prestación del servicio solicitado puede requerir dos o más proveedores de servicios que trabajen juntos de manera eficiente. También entiende que la mejor manera de gestionar los servicios proporcionados, es que IMELSA, o el equipo designado, interactúe con un único interlocutor para todos los servicios extremo-a-extremo, con independencia de las capas de proveedores que sean subcontratadas. Por tanto, los servicios deben proporcionar una solución extremo-a-extremo, agregando servicios y niveles de servicios.

Las empresas licitadoras no podrán superar el 75% de los servicios subcontratando a otras empresas.

De forma gráfica el modelo conceptual al que desea acercarse la Diputación de Valencia es el siguiente:

Tabla 2: Modelo conceptual objetivo



2.1.1 Modelo de servicios del SIGTR bajo petición

La Computación en la Nube o Cloud Computing es una tecnología puntera que tiene el potencial de mejorar la colaboración, la agilidad, la escalabilidad y la disponibilidad. IMELSA requiere un Servicio en la nube, que permita el uso del SIGTR, siguiendo un modelo de despliegue privado, que puede evolucionar funcionalmente y en recursos requeridos bajo petición y siguiendo un modelo de facturación de pago por uso, liberando por completo a la Diputación de Valencia y a las EELL de la gestión y mantenimiento del software, infraestructura y la plataforma tecnológica.

2.1.2 Requerimientos funcionales del SIGTR

El nuevo SIGTR deberá cubrir los siguientes requerimientos funcionales que tienen los procesos actuales del SGT y otros procesos nuevos que no están cubiertos actualmente. A continuación se indican los requerimientos funcionales mínimos que deben ser cubiertos.

2.1.2.1 Características Generales, Organización y Seguridad

2.1.2.1.1 Gestión de la organización y seguridad

El sistema deberá disponer de una gestión de roles y autorizaciones de usuarios del SIGTR. Se podrá autorizar acceso a objetos por el valor que tenga el campo (para el caso de limitar accesos a expedientes por municipio).

Asegurará las salvaguardas necesarias para hacer seguras la autenticación, la autorización y las funciones de control de acceso.

Se deberá poder asignar los usuarios a roles o perfiles y sobre éstos se concederán permisos de acceso a funciones, ejecución de tareas y datos.

El sistema permitirá la definición de unidades organizativas de los usuarios. Se deberá permitir una clara definición de la agrupación de usuarios por ayuntamientos y cualquier tipo de entidad que delegue en la Diputación de Valencia la gestión tributaria o la recaudación, de tal forma que los usuarios externos a la Diputación de Valencia sólo tengan acceso a los datos tributarios de su ámbito territorial y tributos delegados.

Cualquier módulo funcional del sistema deberá estar completamente integrado con la definición de seguridad y organización definida.

2.1.2.1.2 Gestión de Personas y Territorio

La gestión de personas y terceros integrará toda la información, que disponga la Diputación respecto de un contribuyente, ya sea persona física o jurídica, relativa a datos identificativos, direcciones de notificación, y datos de contacto, entre otros, así como, la correspondiente a otros contribuyentes con alguna relación de interés en el ámbito tributario.

El sistema permitirá guardar información de representantes de las personas físicas y jurídicas, así como otras relaciones, y el idioma preferente de comunicación.

La aplicación proporcionará una ficha completa de los contribuyentes y acceso a toda la información tributaria relacionada con él.

El sistema proporcionará interfaces para la carga de información de personas y terceros desde fuentes externas.

El sistema permitirá representar la estructura de objetos territoriales del municipio o supra-municipales: parcelas, calles, direcciones, códigos postales, tramos de calle, etc.

2.1.2.1.3 Gestión de Expedientes

Se proporcionará un sistema para la gestión completa de los expedientes tributarios que abarque todo el ciclo de la gestión y recaudación.

Los expedientes almacenarán toda la información relacionada con su actividad tributaria, constituyéndose como instrumento organizativo y de control.

Contemplará los expedientes que la Diputación inicie de oficio y a instancia del interesado. Permitirá la creación de expedientes de forma masiva en base a diferentes criterios de gestión o recaudación.

El sistema de gestión de expedientes interoperará con los registros de entrada y salida, tanto electrónico como presencial de la Diputación. Permitirá incluir todos los documentos de entrada, tanto de forma presencial como telemática, que presenten los contribuyentes con destino al SGT así como los documentos de salida generados en la tramitación.

Facilitará el seguimiento de la situación y trámites del expediente que se hayan realizado. Asimismo, el sistema informará sobre los trámites pendientes de realizar, unidades de tramitación y plazos legales, si procede.

Se proporcionará un sistema de indicadores de gestión y una metodología de Cuadro de Mandos, basado en la tecnología "Business Intelligence" que dé apoyo a la toma de decisiones.

El sistema permitirá la integración con el sistema de gestión documental corporativo de la Diputación (Alfresco) y se ajustará a los cuadros de clasificación documental definidos.

Permitirá definir circuitos de firma electrónica y funcionalidades de porta-firma, o proporcionar mecanismos de integración con el porta-firmas corporativo de la Diputación.

En los casos de actuaciones administrativas automatizadas, se permitirá la utilización de un certificado de sello de órgano.

El sistema incluirá un mecanismo de verificación de documentos electrónicos firmados basado en un código seguro de verificación (CSV).

2.1.2.1.4 Gestión de Notificaciones

Se proporcionará un control completo de los procesos de notificación a los contribuyentes, manteniendo el conjunto de datos de domicilio necesarios.

La impresión de documentos a notificar se realizará de forma masiva o individual.

Para la impresión masiva de notificaciones en papel se podrán generar ficheros para la impresión en papel, y que serán tratados por empresas especializadas, permitiendo el seguimiento de estos procesos.

El módulo de notificaciones deberá estar adaptado al sistema de retorno de información de certificados de Correos (SICER), pero abierto al retorno de otras empresas de notificación.

El sistema permitirá la selección de notificaciones de cualquier tipo con dos intentos de notificación. Permitirá la inclusión de notificaciones fallidas en remesas para publicar al BOP.

El documento que se notifica y su acuse de recibo escaneado o electrónico, quedarán asociados para su consulta e impresión.

Cualquier documento que se genere en cualquier módulo de la aplicación, se podrá emitir de forma masiva por el módulo de gestión de notificaciones, de forma convencional o telemática.

Todos los documentos electrónicos firmados, incluirán un código seguro de verificación (CSV). El sistema permitirá el envío de notificaciones telemáticas a los contribuyentes que autoricen dicho medio de notificación. El sistema podrá integrarse con los sistemas de notificaciones telemáticas de la Diputación de Valencia como el ofrecido por la plataforma PAI-eSIRCA (http://esirca.gva.es), mediante la utilización de los servicios web que se proporcionen.

2.1.2.1.5 Oficina virtual del contribuyente

El contribuyente podrá acceder, previa identificación según se indica en el apartado 3.1.1.3, a la consulta de los datos personales, consulta de recibos pendientes de pago, simulaciones de cálculo de liquidaciones de distintos tributos, pagos telemáticos, solicitudes telemáticas, consulta del estado de los trámites iniciados, y cualquier otro trámite telemático necesario.

Del mismo modo, la información generada por los ciudadanos en la ejecución de los diversos trámites (pagos, cambios de datos, solicitudes de domiciliación, etc.) deberá quedar almacenada en el sistema.

Por otro lado, para dar validez jurídica a los trámites realizados de forma telemática a través de la oficina virtual, el sistema contemplará:

- La necesidad de registrar las solicitudes de los ciudadanos y la documentación asociada a dichas solicitudes mediante firma electrónica del ciudadano (las aceptadas por la diputación de Valencia).
- Garantizar la autenticidad y veracidad tanto de la información proporcionada por el interesado como de los empleados públicos.
- El cumplimiento de los estándares de usabilidad y accesibilidad.

La oficina virtual del contribuyente incluirá información almacenada en el propio sistema, así como información de sistemas externos con los que exista integración.

La oficina virtual del contribuyente incluirá un calendario tributario generado a partir de los tipos de delegaciones, ordenanzas y periodos de cobros de las EELL.

2.1.2.1.6 Informes

El sistema incluirá el catálogo de informes y listados que actualmente está utilizando el SGT (aproximadamente 500 informes). Además deberá proporcionar herramientas para la elaboración de consultas y listados personalizados como se detalla en el apartado 2.1.3.2.

2.1.2.2 Asesoramiento tributario y asistencia municipal

Las principales funcionalidades que debe contemplar el proceso de asesoramiento tributario son:

- Gestión del catálogo de los servicios delegados.
- Gestión de las cuentas de recaudación y entidades a liquidar.
- Recursos y revisión en vía administrativa.

2.1.2.2.1 Gestión del catálogo de los servicios delegados.

Se incluirá un módulo para gestionar las delegaciones de cada entidad indicando el tipo de delegación para cada concepto tributario. El sistema mantendrá un histórico de las delegaciones.

2.1.2.2.2 Gestión de las cuentas de recaudación.

El sistema deberá ser configurable para que permita proporcionar información suficiente para registrar los derechos reconocidos, anulaciones y cancelaciones de la deuda, cobros, compensaciones, devoluciones, la reclasificación de la deuda aplazada o fraccionada y todos aquellos movimientos contables que son reflejo de la gestión tributaria y recaudatoria realizada.

Se contemplarán las entidades a las que se les recauda conceptos, cuyo ámbito sea municipal o supra-municipal y, por tanto, los procesos de liquidación han de tener en cuenta estas particularidades (Entidades Locales, Generalitat Valenciana, Diputación, Mancomunidades, Consorcios, etc.).

El sistema permitirá el cierre anual de operaciones de cada ejercicio, y se deberá poder definir y establecer todos los cierres parciales que se considere oportunos.

Además de la cuenta de recaudación anual, el sistema proporcionará un mecanismo de rendición de cuentas para cada uno de los períodos parciales establecidos e incluso diarios. Se deberá poder obtener un pendiente nominal a una fecha (incluso pasada), y deberá cuadrar con la cuenta de recaudación a la misma fecha.

Se deberá elaborar y remitir los distintos documentos generados, fruto de la gestión recaudatoria del SGT, (Cargos, Bajas, Cobros y Cuenta anual), para la información y control contable de las entidades.

Deberá implementar la integración necesaria entre el sistema de gestión de cuentas de recaudación y los diferentes módulos contables de las entidades que tienen delegada la recaudación, así como el propio sistema de gestión contable de la

Diputación de Valencia (SICALWIN). Esta integración será asumida por el adjudicatario y deberá estar realizada antes del periodo de transición al nuevo modelo de servicio.

Se deberá poder calcular los anticipos de la recaudación voluntaria, y las tasas de gestión de acuerdo con lo establecido en la Ordenanza. Permitirá tener una cuenta financiera por Ayuntamiento, que recoja las transferencias realizadas mensualmente por anticipos de la recaudación voluntaria, a las EELL que han delegado las funciones tributarias y que así lo han solicitado, y también recoja los pagos en firme que se efectúen a las EELL, así como cualquier anticipo extraordinario que se acuerde conceder. Permitiendo conocer, en todo momento, la posición deudora o acreedora de cada ente, pudiendo incluso hacer simulaciones.

2.1.2.2.3 Recursos y Revisión en Vía Administrativa.

Gestionará los recursos de reposición, especiales de revisión y otros recursos y solicitudes en vía administrativa.

Permitirá la configuración de un catálogo de actos, tributarios o no, susceptibles de ser recurridos.

Permitirá la tramitación de la suspensión del procedimiento en el mismo expediente de recurso o como procedimiento separado y vinculado al recurso.

Registrará las garantías vinculadas a la suspensión del procedimiento.

Las propuestas de resolución determinarán las posibles consecuencias económicas o de cualquier otra índole que deberán ejecutarse en la resolución (liquidaciones, sanciones, reposición a voluntaria, devoluciones, bajas, etc.).

Gestionará las ejecuciones de las resoluciones enviadas por tribunales económicos administrativos y de lo contencioso administrativo y su posible relación con recursos de reposición.

Gestionará de forma masiva las propuestas de resolución y otros actos administrativos definidos.

Controlará los plazos en que deben ser atendidos los requerimientos de documentación. La documentación a generar se basará en plantillas predefinidas. Las notificaciones asociadas a la gestión de recursos deberán estar integradas con la gestión de notificaciones del sistema.

2.1.2.3 Gestión Tributaria

El proceso de Gestión Tributaria tendrá por objeto la gestión completa de los siguientes subprocesos:

- Gestión de domiciliaciones.
- Gestión de padrones y liquidaciones.
- Gestión del Impuesto sobre Bienes Inmuebles IBI (Urbana, Rústica y Características especiales).
- Gestión del Impuesto sobre Actividades Económicas IAE.
- Gestión del Impuesto sobre Vehículos de Tracción Mecánica IVTM.
- Gestión del Impuesto sobre el Incremento del Valor de los Terrenos de Naturaleza Urbana.
- Gestión de la Tasa por el Tratamiento y Revalorización de Residuos Urbanos TTRU.
- Gestión de otros impuestos, tasas, precios públicos, contribuciones especiales y cualquier otro ingreso de derecho público.

La gestión tributaria tendrá una integración total con la información básica del sistema (territorio, personas, organización y seguridad), y con cualquier otro módulo del sistema con el que comparta información tributaria.

El sistema contemplará que la gestión tributaria pueda ser compartida con las EELL, de forma que algunas fases de la gestión sea realizada por empleados de las EELL.

Los distintos objetos tributarios estarán unificados por contribuyente, sin perjuicio de disponer de múltiples direcciones y cuentas bancarias por contribuyente.

Existirá un historial de cambios realizados por cada objeto tributario.

El sistema permitirá el mantenimiento de las bonificaciones y exenciones que correspondan.

Se permitirá la confección a medida de listados y documentos, individuales o múltiples, referidos en objetos tributarios, así como de un diccionario de datos que permita posibles explotaciones complementarias.

2.1.2.3.1 Gestión de domiciliaciones

Incluirá el mantenimiento de las domiciliaciones bancarias para cada contribuyente, en función de los tributos. Deberá ser posible, también, mantener domiciliaciones para

aquellos recibos que se generen directamente a partir de información procedente de organismos externos en formato recibo.

Permitirá la gestión de cotitulares y su posible domiciliación.

Posibilitará realizar operaciones de domiciliación desde la gestión de personas y terceros.

Actualizará y podrá depurar cuentas a través del Cuaderno 19.

Tendrá la capacidad de domiciliar desde Cuaderno 60 con control de incidencias.

Permitirá una gestión de las domiciliaciones unificada independiente del origen de la domiciliación con las siguientes características:

- Dispondrá de una opción específica para introducir las domiciliaciones de forma interactiva y que permita la expedición de un documento de confirmación para ser firmado por el contribuyente.
- Permitirá domiciliar todos los objetos tributarios de un contribuyente a una misma cuenta o especificar una cuenta diferente para cada concepto u objeto tributario.
- Guardará un histórico de domiciliaciones donde se incluya la fecha de validez y el objeto tributario asociado, indicando si están activas o inactivas.

2.1.2.3.2 Gestión de padrones y liquidaciones

Permitirá el cálculo y emisión de padrones simulados, con distintas tarifas.

Se permitirá la gestión de los tributos por el procedimiento de autoliquidación a criterio de la Diputación.

Permitirá la gestión de todos los tributos y otros ingresos de derecho público, ya sean de carácter periódico, ingresos directos en régimen de liquidaciones o autoliquidaciones.

Permitirá la carga de soportes informáticos provenientes de otras Administraciones (DG de Catastro, Agencia tributaria, DG de Tráfico, Entidades Locales, consorcios, etc.). Se contemplarán todos los formatos de carga de entidades externas que colaboren en cualquier fase del ciclo tributario. Permitirá la planificación de cargas planificadas.

El sistema permitirá la definición de las ordenanzas fiscales de cada municipio y sus tarifas vigentes e históricas.

Gestionará los datos básicos sobre los hechos imponibles.

Gestionará las exenciones y bonificaciones correspondientes a cada figura tributaria. Se podrán definir información textual (cajetín) para su visualización en los recibos, liquidaciones, objetos tributarios y su incorporación en ficheros c19.

Permitirá la gestión de las liquidaciones tanto del ejercicio actual como de anteriores, permitiendo la emisión unificada y/o individualizada de todas las liquidaciones no prescritas desde la fecha de conocimiento del hecho imponible, y aplicando las ordenanzas correspondientes a cada ejercicio.

Permitirá las liquidaciones complementarias o sustitutorias, generación de una propuesta de devolución, etc.

El sistema contemplará de igual manera la generación de liquidaciones complementarias en una ya realizada.

Permitirá procesos de aprobación de liquidaciones, con generación de la propuesta de aprobación permitiendo la elección de aprobación individualizada o por relaciones.

Permitirá procesos de baja de liquidaciones y, como en el caso de rectificaciones de liquidaciones, con generación de la propuesta de baja automáticamente.

Permitirá anulaciones parciales de liquidaciones, en caso de que éstas recojan diversos conceptos tributarios.

Permitirá el cálculo de intereses de demora derivados de la presentación de declaraciones y autoliquidaciones fuera de plazo, así como los recargos y/o sanciones aplicables.

Deberá disponer de un sistema de generación y emisión de padrones multi-entidad, con herramientas para gestionar de manera conjunta o individual los padrones de cada municipio.

Sistema de muestreo para la comprobación de los padrones generados atendiendo a diferentes criterios que podrán ser definidos por el usuario. Permitirá la gestión de plazos en los padrones definidos según importe, porcentajes, si están o no domiciliados, etc.

2.1.2.3.3 Gestión del Impuesto sobre Bienes Inmuebles y Gestión Catastral

Gestionará los padrones del Impuesto sobre Bienes Inmuebles de naturaleza urbana, rústica y de características especiales, los cuales tendrán que estar integrados con el módulo de gestión catastral y del territorio.

Establecerá la vinculación de cambios de dominio y demás cambios de sujeto pasivo, así como las alteraciones catastrales a los objetos tributarios de IBI y las tasas relacionadas con consecuencias tributarias en los recibos / liquidaciones.

Permitirá la emisión automática de consecuencias tributarias a partir de las alteraciones remitidas por la DG de Catastro en el fichero DOC.

Incluirá herramientas y procedimientos de conciliación de los padrones de IBI con la base de datos catastral.

Permitirá las consultas externas de acuerdo al convenio FEMP – ANCERT de deudas pendientes de IBI.

Permitirá la carga de la información procedente del Colegio de Notarios (ANCERT) y cruce de la misma por diferentes criterios para la detectar las omisiones de declaraciones y generará los requerimientos a los contribuyentes.

Se integrará con los servicios ofrecidos por el convenio FEMP - ANCERT en lo referente a la simulación, liquidación y pago de deudas de plusvalías.

Permitirá la emisión de liquidaciones/recibos fraccionados según coeficientes de propiedad en todos los casos, o agrupados por titular en el caso del IBI Rústica.

Verificación por medio de la referencia catastral o del número de protocolo y notario, si hay una liquidación o autoliquidación registrada con la misma fecha de transmisión.

2.1.2.3.4 Gestión del Impuesto sobre Actividades Económicas

El sistema permitirá la gestión tributaria del IAE.

Permitirá la tramitación de declaraciones-liquidaciones de alta, baja y variación censal.

Tramitará la gestión de los soportes multi-municipio enviados por la AEAT, herramientas para la resolución de incidencias y actualización automática del censo, tratamiento de los soportes trimestral, con las altas, bajas y modificaciones realizadas. Soporte anual, con las actividades al inicio de año y cálculo de cuota tarifa y censo de no obligados.

Deberá disponer de herramientas y procedimientos de conciliación del padrón de IAE con la información recibida del AEAT.

Gestionará las bonificaciones, tanto potestativas como para cooperativas.

Dispondrá de comunicación automatizada con la AEAT sobre los fallidos en la recaudación del IAE.

2.1.2.3.5 Gestión del Impuesto sobre Vehículos de Tracción Mecánica

Incluirá una gestión completa que permita la actualización del padrón de forma automática a partir de la información enviada por la DG Tráfico y el mantenimiento del censo de IVTM, altas, bajas, modificaciones y transferencias.

Gestionará los beneficios fiscales y exenciones asociados al impuesto.

Gestionará los soportes multi-municipio enviados por la DGT, con herramientas para la resolución de incidencias y actualización automática del censo. En particular, poder secuenciar los registros con misma matrícula/fecha de trámite.

Permitirá la elaboración de autoliquidaciones previo a la matriculación, tanto a personas físicas como jurídicas y gestorías.

Realizará el cálculo de liquidaciones y devoluciones de ingresos por baja.

Podrá realizar el intercambio con la DGT para la gestión de los impagos del impuesto de tracción mecánica de vehículos (ATMV).

Permitirá la utilización de todos los mecanismos de interoperabilidad con la DGT según estén disponibles.

2.1.2.3.6 Gestión del Impuesto sobre el Incremento del Valor de los Terrenos de Naturaleza Urbana

La Gestión del Impuesto sobre Incremento de Valor de Terrenos de Naturaleza Urbana (IIVT) deberá permitir la generación de liquidaciones, permitirá calcular los retrasos en la liquidación, así como los recargos e intereses correspondientes. Asimismo, deberá permitir la generación de autoliquidaciones asistidas por la Administración.

El procedimiento del IIVT deberá estar asociado previamente a un procedimiento de registro de transmisiones.

Deberá asignar automáticamente el sujeto pasivo de la liquidación a partir de la titularidad catastral.

Permitirá efectuar una única liquidación a nombre de la totalidad de titulares del bien inmueble, o efectuar liquidaciones asociadas a cada uno.

Calculará la base imponible en función del tipo de transmisión (compra-venta, mortis causa, usufructo, etc.).

Calculará recargos e intereses por presentación extemporánea.

Podrá verificar por medio de la referencia catastral o del número de protocolo y notario, si hay una liquidación o autoliquidación registrada con la misma fecha de transmisión.

Dispondrá de información de plazos e hitos que están definidos por ley, dependiendo del tipo de transmisión (inter vivos/ mortis causa).

2.1.2.3.7 Gestión del Impuesto sobre Construcciones, Instalaciones y Obras

El sistema realizará una gestión completa del Impuesto sobre Construcciones, Instalaciones y Obras (ICIO) y permitirá:

- Efectuar liquidaciones provisionales y definitivas.
- Mantener los beneficios fiscales.
- Generación de los correspondientes documentos cobratorios de las liquidaciones.
- Generación de liquidaciones complementarias, para los casos en los que el presupuesto inicial de la obra resulte inferior al final.
- Compensación de la deuda definitiva con el importe ya cobrado en la liquidación provisional.
- Integración con los módulos de inspección y sanción.

2.1.2.3.8 Gestión de las contribuciones especiales y cuotas de urbanización.

Permitirá gestionar las contribuciones especiales y cuotas de urbanización.

Permitirá simulaciones y/o cálculo de diversos padrones con la opción de utilizar diversos parámetros (superficie, metros lineales de fachada, valor catastral, coeficiente de participación, volumen edificable, etc.).

Permitirá la incorporación de la información de las fincas que figuran en la base de datos catastral.

2.1.2.3.9 Gestión de otras Tasas y Precios Públicos

Permitirá vincular las tasas relacionadas al inmueble con el IBI y la base de datos catastral.

Permitirá generar contador automático de referencia cuando no haya referencia (Vados sin número, agua sin contador, perros).

Permitirá gestionar cualquier tasa o precio público con la opción de utilizar diversos parámetros de cálculo (superficie, metros lineales...), que a su vez permita liquidaciones de conceptos varios y padrones multi-concepto.

Tendrá la posibilidad de definir tasas genéricas mediante la utilización de una definición de parámetros y cálculos genéricos.

Realizará la emisión automática de consecuencias tributarias a partir de las alteraciones remitidas por la DGC en el fichero DOC, la gestión de beneficios fiscales, la gestión de padrones para tasas periódicas.

Gestionará la liquidación adaptada a los datos particulares de cada tasa definida y parametrizada.

Gestionará la tasa de tratamiento de residuos urbanos (TTRU).

Permitirá la creación de objetos tributarios de la tasa por tratamiento de residuos urbanos para emitir los correspondientes padrones fiscales y documentos de cobro (liquidaciones y recibos).

2.1.2.4 Recaudación voluntaria

El sistema contemplará todos los preceptos establecidos por la Ley General Tributaria y el Reglamento General de Recaudación.

Tendrá un acceso integrado desde recaudación al objeto tributario o hecho imponible asociado a la liquidación o recibo de padrón.

Permitirá la gestión recibos multi-concepto y de diferentes entidades a liquidar. Se permitirá una gestión homogénea de los recibos y liquidaciones.

Permitirá la generación de certificados de deudas y de pago, ya sea globalmente o por conceptos, por el importe de la deuda total o parcial hasta el nivel de cotitulares, de forma presencial y telemática.

La documentación generada por la aplicación o escaneada podrá asociarse al recibo y/o expediente.

Se permitirá una gestión mediante agrupación de recibos o relaciones de recibos, pudiendo aplicar operaciones de forma conjunta a toda la relación.

Permitirá la gestión de cotitulares y cuotas de participación a efectos de informar al contribuyente y también a la hora de emitir documentos separados por cotitulares, y para el procedimiento en ejecutiva.

Permitirá la representación para sujetos pasivos nacionales y extranjeros.

Gestionará fraccionamientos, entregas a cuenta y planes de pago mediante una operativa sencilla, incluida las simulaciones.

Se incluirán los procesos de interoperabilidad de datos mediante servicios web con otras administraciones y organismos, para los que exista convenio en vigencia: Agencia Tributaria, DGT, DGC, TGSS, colegios de notarios y otros.

Permitirá la gestión de forma agrupada de “Grandes Deudores” en función del importe del recibo/liquidación o por el número de objetos tributarios puestos al cobro por cada grupo de remesas.

2.1.2.4.1 Aplazamientos y fraccionamientos de pago

Cada Ayuntamiento podrá establecer unas condiciones diferentes para los aplazamientos según la Ordenanza Fiscal de que se trate.

Realizará simulaciones de aplazamiento o fraccionamiento con posibilidad de impresión del resultado (fracciones a pagar).

Se podrá cancelar aplazamientos y fraccionamientos no atendidos o atendidos parcialmente, reponiendo los recibos a su estado original.

Se podrá realizar fraccionamientos por número de plazos y por importe (principal o total de fracción).

Se podrá realizar fraccionamientos por concepto tributario en recibos multi-concepto.

Se podrá domiciliar los aplazamientos y los fraccionamientos y también emitir cartas de pago con clave C60.

Gestionará el cálculo de intereses en aplazamientos y fraccionamientos distinguiendo entre intereses legales o intereses de demora en función de sí se aporta la correspondiente garantía.

Se podrán emitir informes de estado de situación del aplazamiento y fraccionamiento concedido con desglose de pago y pendiente de pago.

El aplazamiento o fraccionamiento del pago podrá afectar a un único recibo o considerarse un plan de pago de deuda global (Voluntaria y Ejecutiva - con o sin expediente). Además, si es concedido, condicionará el tratamiento del expediente ejecutivo, en caso de que haya; paralizando actuaciones posteriores.

Los fraccionamientos ejecutados sobre un concepto tributario, en voluntaria y sin intereses, se mantendrán para ese concepto y contribuyentes en ejercicios sucesivos hasta que se cancele.

Se podrá incluir en el mismo expediente de fraccionamiento deudas de un mismo sujeto pasivo pero de distinto municipio.

Se contempla la posibilidad de que en el mismo expediente de fraccionamiento se incluyan deudas de distintos conceptos con y sin intereses.

Contemplará la gestión de las garantías: presentación, importe, justificación para el contribuyente de su presentación, paralización de la deuda, control del tipo de garantía aportada.

Registrará un histórico de todos los aplazamientos y fraccionamientos, y las diferentes actuaciones llevadas a cabo incluso cuando se cancelen.

Gestionará las fracciones y aplazamientos de forma clara que no dificulte la operativa diaria.

2.1.2.4.2 Devoluciones de ingresos debidos e indebidos.

El registro y confirmación de cobros duplicados o excesivos deberá generar automáticamente en el sistema, derechos de devolución a favor del contribuyente. Estos se podrán tramitar de oficio o a instancia de parte. El sistema permitirá la configuración por entidad.

Se deberán generar tales derechos de devolución en el caso de liquidaciones complementarias o definitivas, de las que resulten importes a devolver a los contribuyentes.

Los derechos de devolución anteriores deberán quedar ligados tanto al contribuyente como a las operaciones de cobro registradas sobre los recibos y, en su caso, a las liquidaciones practicadas.

Los derechos de devolución anteriores deberán gestionarse mediante un expediente desde el que se deberá poder tramitar tanto el procedimiento de reconocimiento del derecho de devolución como el procedimiento de ejecución de dichos derechos. Opcionalmente, deberá ser posible la tramitación en un mismo acto del reconocimiento del derecho de devolución y la ejecución de las devoluciones.

Deberá permitir la creación automática de expedientes de devolución de ingresos para todos aquellos derechos de devolución existentes para los que todavía no se haya iniciado su tramitación.

También se deberán gestionar mediante estos expedientes la ejecución de los derechos de devolución que nazcan como consecuencia de la resolución de reclamaciones y recursos tributarios.

Permitirá devoluciones parciales de un recibo que incluya uno o varios conceptos y una o varias entidades a liquidar. También a uno o varios contribuyentes según su porcentaje de participación o importe pagado.

Tanto desde la consulta de un contribuyente como desde la consulta de un recibo o liquidación se deberá poder visualizar y acceder tanto a los derechos de devolución asociados como a los expedientes en los que se tramitan dichos derechos.

En el procedimiento de ejecución de los derechos de devolución se deberán poder calcular los intereses que correspondan, en función de la fecha del ingreso, el tipo de derecho de devolución y la fecha de propuesta de ejecución de la devolución, distinguiendo entre ingresos debidos e indebidos.

El procedimiento de ejecución de las devoluciones de ingresos incluirá la posibilidad de ejecutar dichas devoluciones mediante el pago por compensación de la deuda del destinatario de la devolución.

La ejecución de las devoluciones deberá generar información para la contabilidad y, en su caso, registrar el cobro de la deuda a compensar.

Cuando se disponga de la información del número de cuenta, bien por orden de domiciliación del contribuyente o bien por el procedimiento de embargo de cuentas, por defecto se tomará ésta para efectuar la devolución, aunque la decisión última corresponderá al usuario.

En el caso en que las devoluciones deban hacerse efectivas mediante cheque y/o transferencias bancarias, dichas devoluciones deberán poderse materializar mediante las especificaciones del Cuaderno 34 de la AEB.

En el caso del IVTM, cuando se tengan que tramitar devoluciones por prorrateo por baja del vehículo, la aplicación deberá inter-operar con la DGT para obtener e incorporar los datos y fecha de baja del mismo.

2.1.2.4.3 Suspensiones

Deberá dejar constancia de la situación de suspensión en el recibo en el cual está sujeto y el aval o garantía, en caso de tener (tipo de garantía, importe, fecha de presentación y fecha de devolución). Asimismo quedará registrado el motivo de la suspensión.

Se requerirá que los recibos suspendidos aparezcan a la pantalla de cobros, pero que no se incluyan en la selección de embargo.

2.1.2.4.4 Anulaciones

Admitirá propuestas de baja individuales y colectivas.

Admitirá propuestas de baja total o parcial de un recibo.

Debe existir una propuesta de baja con carácter previo a la anulación.

Quedará reflejada tanto la propuesta de baja como la anulación y la fecha de anulación efectiva.

La contabilización debe realizarse mediante un proceso automático transparente al usuario.

Incorporará la gestión de bajas por insolvencia y rehabilitación de éstos fallidos, siempre y cuando no sean anulaciones definitivas.

2.1.2.5 Recaudación ejecutiva

Podrá generar expedientes colectivos de apremio, que incluirán todas las deudas no satisfechas en periodo voluntario.

La providencia de apremio se generará por aquellas deudas no satisfechas en una fecha determinada permitiendo generar un modelo normalizado con la norma C60.

En el caso de deudas de organismos públicos, se obtendrá una certificación acreditativa de no pago a efectos de un nuevo requerimiento, y en caso de falta de pago permita realizar el correspondiente expediente de compensación de deudas.

Para el resto de contribuyentes la falta de pago de la providencia de apremio en los plazos establecidos, determinará la emisión de la providencia de embargo y el inicio del expediente ejecutivo.

Gestionará la realización de las diferentes fases del procedimiento ejecutivo establecidas en el Reglamento General de Recaudación hasta la declaración de crédito incobrable así como las posibles derivaciones de responsabilidad.

Dispondrá de opciones de tratamiento de relaciones de recibos o expedientes por actuaciones colectivas permitiendo la parametrización de las operaciones.

Dispondrá de un control de plazos y alertas para el seguimiento de prescripciones.

Dispondrá de la posibilidad de asignar bloques de expedientes concretos a diferentes unidades de tramitación, permitiendo un seguimiento y control de su ejecución.

Dispondrá de una gestión de compensación de deudas en ejecutiva. Generará y controlará, el expediente de compensación: propuesta, resolución, notificación y aplicación del impuesto compensado.

Dejará constancia de todos los intercambios de información a todos los organismos oficiales que se requieran en el procedimiento ejecutivo y con los que exista convenio de colaboración.

2.1.2.5.1 Procedimiento de apremio

El vencimiento del plazo de pago de las deudas en periodo voluntario, determinará que el sistema relacione las vencidas y no pagadas, anuladas y/o recurridas. Propondrá en primera instancia su aceptación, y posteriormente, una vez validada la propuesta, emitirá las relaciones pertinentes de providencia de apremio. También estará la posibilidad de dictar providencias de apremio individuales.

La emisión de las notificaciones de apremio, así como el resto de notificaciones y avisos de pago de la gestión de ejecutiva, se integrarán con el subsistema de gestión de notificaciones, aprovechando todas las funcionalidades propias de este módulo (control de costas de notificación, gestión SICER, control de direcciones desconocidas y del extranjero, concordancia de datos fiscales entre SICER y unidades fiscales, etc.)

Gestionará de forma diferenciada el procedimiento ejecutivo de las deudas de las Administraciones Públicas y “Grandes Deudores”.

Permitirá gestionar los avales y fianzas depositados y registrados en los expedientes con motivo de las cancelaciones de los procedimientos de fraccionamientos y/o aplazamientos.

Las diligencias de embargo, podrán ser individuales o colectivas y que permitirán la acumulación de deudas anteriores. Dispondrá de la posibilidad de emitir un documento de cobro C60 para permitir el ingreso mediante entidades colaboradoras.

Las deudas nuevas que se generen podrán incorporarse a los expedientes abiertos o bien generar la apertura de un nuevo expediente.

El sistema permitirá implementar la tramitación de los expedientes de embargo en todas sus fases. Los costes asociados a cada actuación queden documentados e incorporados en el expediente.

La selección de expedientes ejecutivos podrá realizarse por deudor, por sucesor o responsable, en su caso, por situación del expediente, por trámites, etc.

En cada expediente ejecutivo quedará reflejado el importe total del expediente y los importes cobrados totales por embargo de cada tipo de bienes. En los bienes objeto de embargo (cuentas corrientes, devoluciones fiscales, sueldos y salarios, etc.) aparecerán desglosados los importes embargados y las fechas de cobro para cada objeto embargado.

Permitirá la correcta gestión de los recibos de un expediente ejecutivo según sean las deudas tributarias o por otros conceptos no tributarios.

En los expedientes ejecutivos se desglosarán los interesados relacionados con el expediente y el tipo de relación. Permitirá relacionar expedientes.

Permitirá la posibilidad de listar los recibos y expedientes ejecutivos cuya fecha de prescripción esté comprendida en un periodo de tiempo concreto.

2.1.2.5.2 Embargo de bienes y cuentas bancarias

El sistema permitirá el embargo de cuentas siguiendo el sistema centralizado C63 AEB/CECA; aunque también admitirá el embargo colectivo sin C63 para aquellas Entidades Financieras que no estén adheridas.

En la gestión de embargo de cuentas basado en C63, las fases 3 y 4 puedan funcionar de manera autónoma e independiente de las fases 1 y 2.

La recepción de la información correspondiente a la fase 4 del procedimiento mecanizado de embargo de cuentas corrientes, según el cuaderno C63, liberará la deuda que no va a ser cubierta por las cantidades retenidas, dando así la posibilidad de ordenar inmediatamente nuevos embargos por dichas cantidades.

La posibilidad de hacer cuantos levantamientos parciales sean necesarios de importes retenidos en una misma entidad.

Una vez realizado el ingreso de las cantidades embargadas por el procedimiento anterior, el sistema deberá aplicar automáticamente dichos importes a la deuda para la que se emitieron las órdenes de embargo, siguiendo el criterio de antigüedad de la deuda.

Realización de una simulación de la fase 6 del C63 una vez efectuado el cobro de las cantidades retenidas para la detección en plazo de posibles descuadres.

El sistema permita el seguimiento del estado de la gestión en general y de uno o más expedientes en particular.

Este procedimiento esté automatizado en su mayor parte, dejando siempre opción a finalizar de modo manual esta tramitación para avanzar en el procedimiento ejecutivo.

Permitirá cuantos levantamientos parciales sean necesarios de importes retenidos en una misma entidad. Permitirá la inclusión en cualquier fase 3 del C63 de aquella deuda que no tenga vigente una referencia C60 valida.

Para el embargo de Sueldos, Salarios y Pensiones se podrá obtener información de la Tesorería General de la Seguridad Social, del Instituto Nacional de la Seguridad y otras entidades.

El sistema permitirá la gestión de expedientes para el embargo de bienes inmuebles, en todas sus fases e integrado con la gestión catastral.

Dispondrá de mecanismos para solicitar información en el Registro de la Propiedad, central o local.

La aplicación permitirá la realización, seguimiento y control del resto de los embargos previstos en la normativa.

Permitirá el embargo masivo de devoluciones tributarias a realizar por la Agencia Estatal de Administración Tributaría, en caso de que la Diputación suscriba los convenios correspondientes.

Dispondrá de los procesos necesarios para implantar el sistema de embargo de devoluciones tributarias de la AEAT utilizando el modelo 996. Se requerirá un proceso automático en el aplicativo para gestionar de forma automática estos cobros a partir del fichero AEB 43.

Permita hacer un seguimiento del expediente a efectos del embargo de otros bienes o la propuesta de la declaración de fallido.

2.1.2.5.3 Sucesiones y derivaciones de responsabilidad

El sistema incorporará un proceso de Sucesiones y Derivaciones que sustituya el deudor por el sucesor o derivado para tramitar embargos sucesivos. No obstante, el expediente ejecutivo en la pantalla de cobros podrá consultarse por el titular anterior y por el sucesor o derivado.

Las Sucesiones y Derivaciones se contemplarán como expedientes que pueden estar relacionados con expedientes ejecutivos y que seguirán diferentes circuitos según de qué tipo de Sucesión o Derivación Solidaria o Subsidiaria se trate.

El sistema podrá contemplar que un expediente de sucesión o derivación pueda llegar a comprender diferentes interesados relacionados con el contribuyente, objeto del expediente ejecutivo, en los cuales se les reclamará un porcentaje del expediente (en caso de cuotas de participación de cotitulares, socios de una sociedad, etc.).

2.1.2.5.4 Gestión de fallidos

El expediente contendrá una propuesta de declaración de fallido, por lo cual se comprobará la realización de las actuaciones necesarias, teniendo en cuenta en su caso el importe, la declaración de fallido del titular, la declaración de responsabilidad en su caso, la propuesta de declaración de crédito incobrable, la anulación de los créditos y la anotación para el registro mercantil.

Controlará las bajas por referencia.

Permitirá el seguimiento y control de fallidos y rehabilitación de los créditos en su caso.

2.1.2.6 Gestión de cobros

Se debe adecuar completamente a las especificaciones del cuaderno C60 de la AEB en su última versión permitiendo las modalidades de pago 1, 2 y 3 y todas las funcionalidades incluidas en el mismo.

Permitirá una gestión de cobros provisional y definitiva.

Se podrá gestionar deuda domiciliada según las especificaciones contempladas en el Cuaderno 19 de la AEB y la CECA, con cualquiera de sus procedimientos.

Permitirá la domiciliación de la deuda con posterioridad a la emisión de los padrones.

Dispondrá de la posibilidad de aplicar reducciones sobre la deuda mediante domiciliación en una cuenta bancaria.

Será posible el cobro de fracciones y aplazamientos domiciliados.

Se registrará el motivo de devolución en el proceso de carga de las devoluciones de la deuda domiciliada. En función de dicho motivo, en su caso, se darán de baja las domiciliaciones de las deudas periódicas.

Se podrá realizar cobros parciales, o a cuenta.

Se registrará los cobros realizados mediante transferencia bancaria, registrando la cuenta donde se han hecho efectivas.

Permitirá la obtención de informes detallados de los cobros efectuados con cualquiera de las modalidades anteriores.

Tanto los cobros duplicados como los indebidos (cobro de recibos anulados o propuestos de baja) quedarán registrados en los recibos correspondientes.

Se generará automáticamente para el deudor, los correspondientes derechos de devolución, que serán gestionados y tramitados mediante expedientes diseñados a tal efecto.

Permitirá la emisión de justificantes de pago por recibo o por persona o cotitular.

Se podrá cuadrar los procesos de cobro por los códigos de proceso. Estos códigos se asignarán de forma automática o manual al crear los distintos procesos de cobro y se asociarán a todas las operaciones relacionadas con cada proceso. Existirán dos formas de cuadrar los importes mediante: hojas de arqueo diarias para cuadrar dinero

cobrado en una fecha concreta; o mediante el cuadre de procesos de cobro, como cargas de C60, fase 4 del C63, etc., que se realizará por el código del proceso, indistintamente del día en que se pase la operación.

Deberá permitir una planificación de la carga de los ficheros bancarios que se reciban (incluyendo los cobros a través de fichero C43), de forma que se carguen y procesen de forma automática, y se emita un informe con los errores.

Dado que la información de los cobros a través de C60 es diaria, pero la recepción del importe total es quincenal, deberá permitir un control total de los ficheros, permitiendo conciliar los ficheros C60, con los correspondientes C43 y en todo momento, disponer de la situación de cada uno de los ficheros, a través de los códigos de proceso, con indicación de si se ha recibido el dinero, se ha contabilizado, se ha enviado a intervención etc.

2.1.2.7 Sanciones de Tráfico

El sistema proporcionará un módulo para gestión y recaudación completa de las sanciones de tráfico.

La creación de los expedientes y la introducción de los datos necesarios para ello podrán realizarse de forma manual mediante un frontal web, cargas de ficheros y desde dispositivos móviles.

A estos efectos, la aplicación, en la parte que corresponda, deberá poder ejecutarse en dichos dispositivos móviles y haber previsto el software y los medios técnicos necesarios para su conectividad tanto con el aplicativo como con la DGT para el intercambio de datos “on-line”.

Gestionará todo el procedimiento sancionador, del pase a la vía ejecutiva de las sanciones y de los recursos administrativos que se interpongan.

Estará orientada a procesos masivos desatendidos para agilizar al máximo la tramitación. Entre otros, permitirá:

- La identificación y resolución automática de los expedientes del art. 81.5 de la LSV
- La identificación y resolución automática de los expedientes que no son del art. 81.5 de la LSV en los que, además, ni se han hecho alegaciones ni se ha pagado la sanción en plazo de descuento

- La identificación y resolución automática de los expedientes por infracción de los artículos 65.5 j), 65.5 h) y 65.6 de la LSV, en los que no se presenten alegaciones
- El control de plazos para evitar prescripciones y caducidades, identificando automáticamente y avisando de los expedientes con riesgo de prescripción o caducidad.

Permitirá conocer el estado de tramitación de todos los expedientes, en todas y cada una de las fases del procedimiento. Incluirá utilidades para detectar expedientes que están siguiendo una tramitación irregular o no prevista.

Se podrá obtener información de la DGT mediante procesos individuales (por expediente) o colectivos (masivamente), incluyendo los datos del titular del vehículo a fecha de infracción, el dato de si el vehículo estaba, o no, dado de baja a fecha de infracción y tanto el domicilio del vehículo como el del titular del vehículo.

Gestionará las publicaciones en TESTRA y notificaciones en DEV (Dirección Electrónica Vial).

Generará documentos para efectuar el pago de la sanción, en cualquier momento del procedimiento, aunque legalmente no esté previsto, que incluyan, en su caso, notas informativas.

Calculará la sanción a aplicar y los puntos a detraer en el caso de las infracciones por exceso de velocidad, a partir del límite de velocidad vigente y la velocidad del vehículo.

Si el pago con boletín se registra en la aplicación antes de que el expediente haya sido creado, la aplicación no cerrará el expediente sin antes comprobar que la cantidad ingresada es correcta.

Caso de pago parcial de la sanción deberá ser posible continuar la tramitación del expediente por la parte pendiente de la sanción.

La generación automática Permitirá la impresión de los expedientes en papel (de todo el expediente o de una parte del mismo), con la opción de generar un índice.

Posibilitará de segundos envíos de notificaciones de denuncia y resoluciones sancionadores para subsanar defectos.

Permitirá la modificación del estado de tramitación del expediente y de la gravedad de las infracciones, con recalculo automático de fechas de prescripción, caducidad y demás información pertinente.

2.1.3 Requerimientos técnicos

Los requerimientos técnicos mínimos que debe cubrir el SIGRT, son los siguientes:

2.1.3.1 Características generales

La solución propuesta se basará en los siguientes conceptos:

- SIGTR deberá ser multi-idioma (al menos valenciano, castellano e inglés) y multiplataforma hardware y software.
- Cualquier producto software o hardware que incluya el adjudicatario como componente para proporcionar el servicio solicitado debe estar en producción en organismos multi-entidad o supramunicipales, dentro de mercado (no descatalogado), soportado por el fabricante, y actualizado periódicamente con el objeto de resolver errores (bug) y reducir vulnerabilidades.
- Los requisitos técnicos deberán cubrir los niveles de seguridad exigidos en el apartado “5.3 Confidencialidad y seguridad de la información y protección de datos de carácter personal” del presente pliego.
- La solución debe ser accesible por los usuarios a través de los sistemas operativos comunes (Windows, OS X, iOS, Linux) y navegadores web de uso común (IE, Firefox, Safari, Chrome). La presentación se llevará a cabo mediante un navegador basada en tecnología web HTML. Los usuarios de la Diputación de Valencia, EELL o el propio contribuyente podrán acceder al SIGTR mediante dispositivos heterogéneos a través de la red privada o accediendo a través de Internet de forma segura.
- El interfaz gráfico deberá respetar los criterios de accesibilidad web, siguiendo las pautas recomendadas por WCAG 2.0. La accesibilidad deberá estar en línea con las exigencias del Real Decreto 1.494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- El SIGTR estará desplegado bajo un modelo de nube privada (Private cloud) según definición de NIST (National Institute of Standards and Technology), con las características propias de nube que define NIST.
- El adjudicatario deberá proporcionar toda la documentación referente al Diccionario de Datos, que facilite la comprensión de la estructura de datos, de tal forma que IMELSA y/o la Diputación de Valencia podrá explotar los mencionados datos de forma independiente.

Teniendo en cuenta estas premisas, el licitador presentará la arquitectura tecnológica que posea la solución propuesta.

Para asegurar la disponibilidad del servicio y el mantenimiento correcto del SIGTR, se considera que al menos debe disponer de los siguientes entornos de trabajo:

- Migración de datos: debido a las características propias del Proyecto de implantación, será necesario durante las actividades de migración de un entorno especializado de migración con gran capacidad de datos y de procesamiento en el que se copiarán todos los datos a migrar, se realizarán las transformaciones y se generarán los ficheros de carga requeridos. El adjudicatario podrá crear además otros entornos que considere necesarios durante la implantación.
- Preproducción: una vez completadas las pruebas en el entorno de desarrollo del adjudicatario, serán desplegados en este entorno para realizar las pruebas de integración y formación necesaria. El adjudicatario propondrá mecanismos de copia de datos requeridos de forma periódica desde el entorno de producción a preproducción atendiendo a las necesidades regulatorias que le apliquen, de forma que se garanticen la semejanza de los entornos y confidencialidad de los datos.
- Producción: el entono de producción será el que accedan los usuarios de la Diputación de Valencia, EELL y ciudadanos. Solo serán desplegados a este entorno los cambios debidamente aprobados y autorizados por la Diputación de Valencia a través de IMELSA.

El entorno de Desarrollo queda fuera del alcance del pliego y será soportado por adjudicatario, disponiendo de las mismas características técnicas que el entorno de producción ofertado.

El sistema globalmente se estructurará en un conjunto de servidores virtuales y físicos que asumirán de forma modular los requerimientos y funciones necesarias que se describen en el presente pliego.

2.1.3.2 Sistema de generación de informes

SIGTR debe disponer de un sistema que pueda manejar el usuario final para la creación de consultas y cualquier tipo de informes, listados o documentos.

El sistema de generación de informes proporcionará capacidades de creación de informes de negocio para usuarios y aplicaciones web.

Los objetivos de este sistema será cubrir un amplio rango de necesidades de creación de informes, abarcando desde informes operativos de gestión, de análisis y documentación para los contribuyentes.

La herramienta permitirá la exportación de los resultados hacia aplicaciones de ofimática estándares o archivos de texto plano.

El sistema de generación de informes estará integrado con todos los módulos de la aplicación.

2.1.3.3 Planificador de procesos y trabajos

El sistema proporcionará herramientas específicas para planificar trabajos en diferido, de tal forma que se pueda programar procesos de tratamiento masivo en el SIGTR sobre los recibos, expedientes, carga de datos externos, generación de informes, o de cualquier otro tipo técnico y funcional.

2.1.3.4 Documentación, manuales y código fuente del SIGRT

Los manuales de usuario y toda la documentación del sistema se entregará en soporte digital, y en papel en caso de que IMELSA lo requiera, y se mantendrá actualizada permanentemente con las nuevas funcionalidades y modificaciones realizadas en la aplicación.

Todos los cambios sobre el sistema extremo-a-extremo, técnica o funcional, serán documentados, actualizados, entregados y aceptados por IMELSA, según los procedimientos que se establezcan durante el Proyecto de implantación.

De la misma forma, el Proyecto de implantación, así como el posterior servicio incluirá toda la documentación asociada a las actividades del mismo, incluyendo la planificación actualizada, actas de reuniones, informes, documentación técnica y funcional. Será necesario disponer de un repositorio único tanto para la documentación del proyecto como la del servicio. El licitador deberá indicar los entregables que proporcionará en el proyecto y durante el servicio.

Las empresas licitadoras tendrán que garantizar la disponibilidad del código fuente de la aplicación en caso de cierre de la empresa por cualquier motivo, fusión o absorción por otros o por cambio en la línea de negocio de la misma. Para garantizar el acceso al código fuente en los casos anteriormente descritos, deberá depositar una copia ante notario, que será actualizada al menos 2 veces al año.

2.1.3.5 Portabilidad e Interoperabilidad.

El adjudicatario deberá proporcionar mecanismos para apoyar:

- Portabilidad de datos: para copiar objetos de datos dentro o fuera de la nube. Entre otros, debe permitir la incorporación de los datos de nuevas delegación de EELL o cese de las actuales. La incorporación de nuevas delegaciones de EELL será un servicio ofrecido bajo petición, según se indica en el apartado 3.1.1.1. Los licitadores deberán detallar el procedimiento, tareas y formatos para la portabilidad de datos de EELL.
- Interoperabilidad de servicios: para usar los datos y servicios a través de múltiples proveedores, como por ejemplo, pero no únicamente:
  Requerido antes del periodo de transición al nuevo modelo de servicio:
  - Integración con la Plataforma de Administración Electrónica de EELL de la Comunitat Valenciana (PAECV en adelante).
  - SIGTR será accesible a los ciudadanos a través de las sedes electrónicas de sus ayuntamientos y desde la sede electrónica de la propia Diputación de Valencia.
  - El SIGTR deberá cumplir las Normas Técnicas de Interoperabilidad del Real Decreto 4/2010, de 8 de enero, para que sea capaz de interoperar con otros organismos como DG de Catastros, Agencia Tributaria, DG de Tráfico, Entidades Financieras, Colegio de notarios, u otros organismos y entidades que colaboran con la Diputación de Valencia.
  - Se dispondrá de la capacidad de interconectar con otras aplicaciones, como el Sistemas de Gestión Contable Municipal SICALWIN, registro electrónico, portafirmas y otros, así como capacidad para diseñar interfaces.

  No más tarde de 3 meses después del arranque:

  - Interoperabilidad con el Sistema de información Territorial SEGUEX de IMELSA. SEGUEX es un Sistema de Información Geográfica que funciona bajo entorno web, desarrollado en código abierto basado en tecnología MAPSERVER y biblioteca de JAVASCRIPT para mostrar mapas interactivos OPENLAYERS. El SIGTR deberá interoperar con SEGUEX para poder georeferenciar expedientes con información catastral en las bases de datos gráficas disponibles.

  El SIGTR deberá permitir la interoperabilidad con otros sistemas de la administración local, autonómica y de la administración general del estado,

mediante la provisión y consumo de servicios publicados en la Plataforma de Autonómica de Intermediación (PAI eSIRCA) de la Comunidad Valenciana.

- Portabilidad del sistema: para la migración de una instancia de máquina virtual o una imagen de máquina de un proveedor a otro proveedor, o migrar aplicaciones y servicios y sus contenidos de un proveedor de servicios a otro proveedor.

Cuando se requiera o finalice el servicio y sea devuelto a IMELSA según se indica en el apartado 5.2, se podrá exigir la obtención de los datos estructurados de la Diputación de Valencia y de las EELL que han usado el sistema, para posteriormente realizar la supresión completa y permanente de los datos en la infraestructura del adjudicatario saliente, así como la certificación de que el proceso fue realizado correctamente.

2.1.3.6 Comunicaciones.

La conexión con el SIGTR desde las instalaciones centrales de la Diputación de Valencia está incluida dentro del alcance del presente pliego. Se debe incluir en las propuestas modelos de redundancia de líneas de comunicaciones con diferentes proveedores de telecomunicaciones o al menos rutas alternativas del mismo proveedor.

Las EELL disponen de líneas de comunicaciones de salidas a Internet con distintos operadores. El licitador deberá describir las modalidades de conexión con el SIGRT y monitorización con las EELL.

Las propuestas deberán describir la arquitectura de comunicaciones que consideran más adecuada en función de los requerimientos descritos y requisitos de seguridad de IMELSA

2.2 Modelo de servicios

El objetivo principal que IMELSA tiene con la contratación de un modelo con orientación a servicios, es definir claramente qué necesita la Diputación de Valencia, las EELL y el contribuyente, y qué recibe IMELSA a través del adjudicatario como proveedor de los servicios. Además permitirá establecer acuerdos sobre los servicios que clarifiquen la relación entre los proveedores de servicios y los consumidores de servicio.

Para cubrir estás necesidades, los licitadores deberán detallar al menos los siguientes componentes del modelo de servicios: modelo de relación y modelo operativo.

2.2.1 Modelo de relación

El modelo de relación tiene como objetivo definir las funciones y responsabilidades del adjudicatario e IMELSA para asegurar el compromiso de cumplimiento de las respectivas obligaciones, tanto en el proyecto como en el servicio posterior.

El modelo de relación que proponga el licitador debe estar basado en los siguientes criterios:

- La Diputación de Valencia, a través de IMELSA, es el organismo responsable de definir, impulsar, contratar y ejecutar la estrategia para la provisión de servicios de la Gestión y Recaudación Tributaria de las EELL que delegan este servicio en la Diputación de Valencia.
- El adjudicatario del servicio será el responsable de **todos los servicios ofrecidos extremo a extremo**, con la mejor calidad al coste más competitivo, y entre sus responsabilidades se encuentran pero no se limitan a:
  - Adecuar el SIGTR a las necesidades de la Diputación de Valencia y EELL, migrando los datos actuales que se consideren en el Plan de Migración.
  - Cumplir los principios y medidas de seguridad requeridas.
  - Facilitar y garantizar la información de indicadores clave que se regulan en los ANS, mediante la monitorización de los servicios prestados, según se indica en el apartado 3.2.2.
  - Auditorías periódicas de cumplimiento de los servicios y de la seguridad de la información según se indican en los apartados 3.4 y 5.3.2 del presente pliego.
  - Mecanismos que garanticen el correcto funcionamiento de los servicios conforme a los niveles de servicio requeridos en el apartado 3.3 del presente pliego.
  - Separar la parte operativa del servicio de la parte de gestión, para lograr responsabilidades definidas, bien delimitadas y susceptibles de ser medidas.
  - Establecer los mecanismos de comunicación entre todos los equipos, proyecto de implantación y servicio posterior, para que se realimenten entre ellos.

2.2.2 Dirección y seguimiento del proyecto de implantación y el servicio posterior

El licitador debe incluir en la propuesta el modelo de relación asociado al modelo de servicios, teniendo en cuenta los criterios anteriores y las siguientes unidades en las que tendrán miembros IMELSA y Diputación de Valencia:

- **Unidad de Gobernanza** (UG), con el objetivo de garantizar la calidad de los servicios, medir el rendimiento, gestionar los riesgos y demostrar el valor entregado por el adjudicatario. Constituirá el máximo órgano de decisión y responsable último de la ejecución de los objetivos del proyecto y servicio.
- **Unidad de Gestión y Operación** (UGO), con el objetivo de realizar la toma de decisión de la operación y garantizar la ejecución de los procesos.

Se considera que los perfiles mínimos por parte del adjudicatario que deben interactuar y participarán en los distintos comités son:

- Director de contrato
- Responsable del Proyecto de implantación.
- Responsable del Servicio
- Responsable de Seguridad

Estos perfiles deberán tener el suficiente conocimiento y experiencia en gestión y recaudación tributaria, gestión de proyectos, gestión de servicios gestionados y provisión de servicios en la nube.

El licitador debe ampliar, mejorar y detallar, partiendo de las directrices aquí marcadas, la organización propuesta y el esquema específico de la relación con IMELSA y la Diputación de Valencia, así como otros modelos que considere. Además describirá la metodología que aplicará en la dirección y seguimiento del proyecto.

2.2.3 Modelo operativo

El modelo operativo definirá que hay que hacer y cómo hay que hacerlo, dentro del servicio solicitado SIGTR extremo-a-extremo. Las características de las necesidades del modelo operativo se detallan en el apartado 3.1.3 del presente pliego. El licitador incluirá el modelo operativo de servicios partiendo de las características indicadas y alienado con estándares del sector y con la mejor práctica en gestión y provisión de servicios de las Tecnologías de la Información, que ayuden a conseguir los objetivos de SGT, SIO e IMELSA.

3 Descripción de los servicios a contratar

3.1 Catálogo de Servicios

3.1.1 Sistema de Información de Gestión y Recaudación de Tributos

3.1.1.1 Servicio bajo petición y flexible.

El número de usuarios y EELL puede escalar o disminuir rápidamente. IMELSA podrá solicitar cuando lo requiera, la incorporación en el SIGTR de nuevas EELL, tributos, funcionalidades, o retirar los servicios delegados cuando finalice los acuerdos de delegación entre la Diputación de Valencia y las EELL.

IMELSA podrá requerir ampliar o reducir los servicios prestados, según sus necesidades por la incorporación de nuevas EELL, o la retirada de los mismos.

IMELSA podrá requerir de forma fácil y rápida, la creación o destrucción de los entornos de pruebas de aceptación y de formación de usuario, según las necesidades del momento.

Se desea por tanto, un servicio escalable, que gestione los cambios y configuración de la infraestructura tecnológica, e incorporación de nuevas delegaciones, de acuerdo con las necesidades de la Diputación de Valencia, EELL y de los acuerdos de nivel de servicio, y de pago bajo la modalidad “bajo petición”.

El licitador deberá indicar, dentro del ámbito del presente pliego y partiendo de los requeridos por IMELSA, el catálogo de servicios que ofrece bajo petición dentro del ámbito del presente pliego.

3.1.1.2 Modelo de estimación y de pago por uso.

Para los servicios bajo petición, el licitador deberá presentar el modelo de estimación para que IMELSA pueda valorar la ampliación o disminución económica. Este servicio canalizará las colaboraciones que no están reguladas en ninguno de los servicios prestados que se definen como requerimientos en el presente pliego. Las facturas asociadas a este tipo de servicios se calculan en base a la cantidad de recursos y consumidos por la Diputación de Valencia, basándose así en el modelo de pago por uso. El modelo de estimación se deberá definir sobre criterios objetivos y cuantificables.

3.1.1.3 Acceso a la red

Los usuarios del SIGTR podrán acceder al mismo a través de la red propia de la Diputación de Valencia o garantizado el acceso a través de una red privada mediante una conexión segura desde fuera de la red para el caso de EELL como se indica en el apartado 2.1.3.6. El licitador deberá incluir el detalle de la solución de las comunicaciones propuestas.

El acceso de los contribuyentes al SIGTR a través de Internet, soportará el uso de autenticación mediante certificado digital emitido por una autoridad de certificación reconocida y admitida por la Diputación de Valencia o mediante DNI electrónico.

3.1.2 Proyecto de implantación del SIGTR y establecimiento del servicio.

El proyecto de implantación del SIGTR y establecimiento del servicio se constituye para realizar la adecuación del nuevo SIGTR a las necesidades de la Diputación de Valencia, migración de los datos y transferencia de los servicios al adjudicatario, en términos de continuidad, cumplimiento y mejora de la calidad percibida, transformando un modelo de servicios de informática tributaria interno y tradicional, a un modelo de servicios en la nube y basado en ANS.

IMELSA entiende que esté es uno de los aspectos más importantes y críticos del servicio a contratar con el presente pliego que debe exigir la máxima diligencia por parte del adjudicatario para conseguir los objetivos planteados.

Las actividades mínimas que cubren los objetivos definidos dentro del alcance que deben incluirse en este proyecto, son las siguientes:

- Implantación del modelo de relación entre IMELSA, Diputación Valencia y el adjudicatario, así como los procedimientos del proyecto: gobierno, gestión y control.
- Aprovisionamiento e implantación del software y de la infraestructura tecnológica en la nube.
- Adecuar el nuevo SIGTR a los procesos y necesidades de la Diputación de Valencia, EELL y del contribuyente:
  - Análisis y Diseño de procesos según las necesidades del SGT.
  - Rediseño del sistema adaptándolo a las necesidades del SGT.
- Formar adecuadamente a los usuarios que usarán el SIGTR de la Diputación de Valencia y las EELL, migrar los datos del actual Sistema de Gestión Tributaria de la Diputación de Valencia al nuevo SIGTR detallado en el Plan de Migración, garantizando la calidad e integridad de los mismos.

- Garantizar el cambio de modelo de prestación de servicio sin afectar a las prestaciones que se ofrece actualmente a la Diputación de Valencia y EELL.
- Establecer y poner en marcha los métodos de trabajo, las herramientas y los procedimientos de medición, cálculo y entregables que se vayan a utilizar para medir el cumplimiento de los Niveles de Servicio, despliegue, arranque del nuevo sistema y transición hasta el servicio.

Basado en estas actividades u otras que pueda ampliar, el licitador propondrá en su Plan de Proyecto, cuales son las actividades e hitos que se compromete, junto con los mecanismos que aportará para garanticen el nivel de servicio reflejado en los ANS del apartado 3.3 del presente pliego y el éxito del proyecto. El licitador deberá presentar el Plan de Pruebas y aceptación por parte del usuario e IMELSA, tanto en la adecuación del sistema a las necesidades que requiere el SGT, como en la conversión o transformación y migración de los datos actuales al nuevo SIGTR, que incluirán los expedientes abiertos más los expedientes cerrados que se tengan que mantener por normativa legal. Se deberá obtener el 100% de los datos migrados con la calidad previamente definida. Se deberá garantizar la seguridad de la información existente de los ciudadanos, según el apartado 5.3. Asimismo, se incluirá algún proceso de corrección de posibles errores existentes

Se deberá incluir un Plan de Formación detallado que ayude a que los usuarios se sientan cómodos y confiados con el nuevo SIGTR, sobre todo, porque el interfaz de usuario y conjunto de características experimentan cambios significativos. Por ello, la capacitación del personal de IMELSA, de Informática y Organización de la Diputación de Valencia y los usuarios finales de la Diputación de Valencia y de EELL debe ser completa y en profundidad.

También incluirá un Plan de Comunicación al Contribuyente y a las EELL, donde se podrá contar con la colaboración del servicio de Atención al Contribuyente ACI que dispone IMELSA.

El licitador deberá presentar un Plan del Proyecto global, indicando claramente la estimación de tiempo y recursos, así como las fases, actividades, objetivos perseguidos en cada periodo y la medición de objetivos conseguidos. Se deberá indicar el modelo de despliegue de los módulos funcionales que no requieran migración de datos, los cuales podrían implantarse antes sin mucho esfuerzo y demostrando los primeros éxitos del proyecto. Además se deberá indicar todos los entregables que generara en este proyecto y el modelo de aceptación de los mismos por parte de IMELSA.

3.1.3 Servicios de soporte operativo

Los servicios de soporte operativo incluyen las siguientes actividades asociadas al servicio extremo-a-extremo del presente pliego de condiciones técnicas, es decir, cubrirán todos los servicios requeridos para la infraestructura tecnología, software y componentes necesarios para dar servicio completo al SIGTR. Estas actividades, enmarcadas como servicios de soporte operativo del SIGTR, se han estructurado en los siguientes procesos siguiendo estándares de mercado:

3.1.3.1 Gestión de la Capacidad y Disponibilidad.

Para gestionar el uso óptimo y el rendimiento del SIGRT extremo a extremo, de forma que se asegure que los requerimientos de disponibilidad y rendimiento se cumplen consistentemente y que la capacidad de los servicios proporcionados se corresponde a las necesidades descritas.

Tiene como objetivos, pero no se limitan:

- Garantizar que todos los servicios del SIGTR estén respaldados por una capacidad de proceso, rendimiento y almacenamiento suficiente, bien dimensionado y flexible para los usuarios funcionales y el contribuyente.
- Contribuir a diagnosticar problemas e incidencias relacionados con el rendimiento, capacidad y disponibilidad, así como proponer medidas proactivas para mejorar el rendimiento.
- Garantizar que los servicios del SIGTR están disponibles y funcionen dentro del marco de los ANS que se indican en el apartado 3.3.

3.1.3.2 Gestión de la Continuidad.

Para soportar la continuidad del Servicio de Gestión Tributaria, asegurando que el SIGRT puede ser recuperado en los plazos requeridos en los ANS del apartado 3.3.

Tiene como objetivos generales:

- Disponer de un Plan de Recuperación de Desastres destinado a restablecer la operativa del SIGTR y de los servicios proporcionados en un sitio alternativo. Será probado regularmente, al menos una vez cada seis meses y medido según los niveles del servicio requeridos en el del apartado 3.3. El Plan de Recuperación de Desastres puede ser parte de un Plan de Continuidad de Negocio del adjudicatario y estará basado en los normas BS25999 y BS25777 en la ejecución del contrato. Se deberá involucrar a personal de IMELSA y

Diputación dentro del comité de crisis que disponga el Plan, para las pruebas o en una posible activación del plan. El Plan deberá ser actualizado anualmente, y estarán sujetos al procedimiento de Gestión de Cambios que se definan.

3.1.3.3 Gestión de Cambios

Que asegure que los cambios propuestos del SIGTR se registran, evalúan, autorizan, se asigna prioridades, planifican, prueban, implantan y documentan, siguiendo los procedimientos establecidos y garantizando en todo momento la calidad y continuidad del servicio SIGTR. En el Proyecto de implantación del SIGTR y establecimiento del servicio, se deben definir el alcance de los cambios que aplicarán a cualquier elemento que conformen los servicios SIGTR en producción.

El adjudicatario deberá proponer los canales y procedimientos para estar informado de todas las peticiones de cambio solicitadas o propuestas por el adjudicatario, las cuales serán gestionadas por el órgano que se establezca. Asimismo, se definirá los criterios de cambio estándar frente a otros tipos de cambios menores y que no requieran la intervención del órgano responsable.

Se clasificará las peticiones de cambio de común acuerdo con IMELSA, en "*bajo petición*" o como consecuencia de la necesidad de corrección de un incidente o problema ("*correctivo*") en el SIGTR extremo a extremo. El adjudicatario tendrá que realizar el mantenimiento correctivo del SIGTR necesario para la correcta, eficaz y eficiente operativa diaria, sin coste alguno para IMELSA. La corrección de datos no válidos en el entorno productivo que se hayan provocado por errores en el SIGTR definidos como "correctivo", también será responsabilidad del adjudicatario. En este sentido, se incluyen como "correctivo" las adaptaciones resultantes de las acciones correctivas reflejadas en las auditorias.

El adjudicatario realizará la estimación de las peticiones de cambio *bajo petición* según se indica en el apartado 3.1.1. La petición se validará conjuntamente con el SGT para priorizar y planificar dentro del órgano responsable.

Al incluir en el alcance del proyecto la migración del sistema actual que debe cubrir los requerimientos funcionales, el licitador debe explicitar en la propuesta, cual es el modelo para los cambios y desde cuando se aplicará el modelo. Los cambios que vengan por necesidades normativas ajenas a la Diputación de Valencia o IMELSA, no serán considerados como bajo petición .

Todos los cambios generados bajo petición o correctivos tendrán su reflejo en la documentación técnica y funcional correspondiente.

3.1.3.4 Gestión de Versiones.

Entre otros objetivos del proceso se incluyen:

- Planificar y controlar la implantación de nuevas versiones del SIGRT y de componentes de los servicios extremo-a-extremo ya existentes.
- Asegurar que toda nueva versión puesta en producción y los cambios que se efectúen sean seguros y que sólo sean instalables versiones correctas, autorizadas y probadas bajo el proceso de la Gestión del Cambio anteriormente descrito
- Comunicar y gestionar las expectativas del SGT durante la planificación y puesta en producción de nuevas versiones.
- Transferir el conocimiento de las nuevas funcionalidades o correcciones que se incluyen en las nuevas versiones, a usuarios y a personal de IMELSA y la Diputación de Valencia.

3.1.3.5 Gestión de Incidencias y Problemas.

La Gestión de Incidencias deberá restaurar los niveles normales del servicio afectado tan pronto como sea posible, minimizando el impacto en el SGT, manteniendo los niveles de calidad y disponibilidad del servicio del SIGRT. El adjudicatario dispondrá de un punto único de contacto que registre todas las incidencias extremo-a-extremo, detectadas por procesos automáticos de monitorización y eventos o cualquier otra vía, y por incidencias escaladas por el personal gestor y de operaciones de IMELSA dedicado a ello.

Los licitadores deben indicar el protocolo de actuación para detectar y registrar los problemas en función de los incidentes reportados o identificando tendencias de los mismos, con el objetivo de llegar a la causa raíz de las incidencias, iniciar las acciones que corrigen el problema y reducen el impacto en el servicio del SIGTR extremo a extremo.

3.1.3.6 Gestión de los Niveles de Servicio.

Donde se agregan, componen, consolidan, monitorizan y se analizan las diferentes medidas de servicios y elaboración de los indicadores periódicos, extremo a extremo. Tiene como objetivo, mantener y mejorar la calidad de los servicios relacionados con el SIGTR y proporcionar la información necesaria sobre el grado de cumplimiento de los acuerdos en los servicios y otros indicadores clave de rendimiento que pueda proponer el adjudicatario.

3.1.3.7 Gestión de la Mejora Continua.

Buscará alinear los servicios ofrecidos a las necesidades cambiantes del SGT de la Diputación de Valencia y EELL, identificando e implementando mejoras. El esfuerzo de mejora se focaliza principalmente en el aumento de los parámetros de calidad, como entre otros, el tiempo dedicado; aumento de la eficacia, eficiencia y usabilidad.

Será un proceso constante, continuo y transversal al resto de procesos, que evalúe y optimice todos los procesos de soporte anteriores, y que mejoren los procesos del SGT de la Diputación de Valencia y EELL.

El licitador podrá incluir en la ejecución, otros procesos que considere necesarios para presentar el servicio solicitado de forma eficaz y eficiente.

3.2 Condiciones del servicio

3.2.1 Horarios.

El adjudicatario deberá proporcionar los servicios solicitados en los horarios especificados a continuación, en función de si el servicio se presta internamente o de cara al ciudadano y donde se aplicarán los niveles de servicio correspondientes:

- **Horario estándar** (12 horas x 5 días): días laborables según calendario laboral de la Comunitat Valenciana de 7:30 a 19:30h, excepto julio y agosto que será *de 7.30 a 16.00 hrs. Este horario está destinado al servicio prestado a usuarios* internos de la Diputación de Valencia y EELL.

- **Horario extendido**: días laborables según calendario laboral de la Comunitat Valenciana de 19:30 a 7:30h (12 horas x 5 días), más los fines de semana y festivos completos (24 horas x día). Este horario está destinado al servicio prestado al ciudadano y procesos internos del SIGTR descritos en el apartado 2.1.3.3 Planificador de procesos y trabajos del presente pliego.

3.2.2 Medición del Servicio y Herramientas.

Para el control y seguimiento de la calidad del servicio prestado, el adjudicatario proporcionará un sistema de información que facilite métricas e indicadores clave de rendimiento (KPLs) del servicio extremo-a-extremo, como se solicita en el apartado 3.3, y que servirá como mecanismo de seguimiento y evaluación del proyecto y posterior servicio. Estas herramientas deberán monitorizar la actividad del servicio en línea, con indicadores de evaluación y control de la infraestructura tecnológica y ANS relacionados, y que ayude a la Unidad de Gestión y Operación (UGO) a la

gobernabilidad del servicio. Incluirá un cuadro de mandos que ayude a la toma de decisiones y proporcione indicadores clave de rendimiento en tiempo real comparándolos con los indicadores objetivo.

IMELSA junto con la Diputación de Valencia se encuentra en un proceso de revisión y mejora continua de sus procesos de atención a usuarios que puede implicar la realización de cambios en lo referente a las herramientas internas que deberán integrarse con las herramientas de gestión del servicio proporcionados por el adjudicatario. Esta integración será asumida por el adjudicatario y deberá estar realizada antes del periodo de transición al nuevo modelo de servicio.

El licitador deberá especificar el conjunto de herramientas que afectan a la prestación de los diferentes servicios objeto de esta licitación, identificando la herramienta, el servicio o requerimiento aplicable y su finalidad.

El adjudicatario deberá adquirir y mantendrá las licencias de software de las herramientas que sean necesarias para la prestación del servicio.

3.2.3 Enfoque metodológico para el proyecto y el servicio.

Se requiere que los licitadores indiquen en su propuesta, el enfoque metodológico que aplicará en la ejecución del Proyecto de implantación del SIGTR y establecimiento del servicio, y de los restantes servicios objeto de esta contratación, en aras del aseguramiento de la calidad de los servicios propuestos.

3.3 Acuerdos de nivel de servicio

3.3.1 Descripción del Acuerdo de Nivel de Servicio

Se definen a continuación los ANS, (o en inglés SLA - Service Level Agreement) que deben cumplir los servicios descritos en el presente pliego. Los ANS aquí descritos representan la comprensión entre IMELSA y el adjudicatario sobre el nivel esperado del servicio que se va a entregar y la compensación disponible para IMELSA en el caso de que no se llegue al nivel especificado. En este caso, se aplicará las correspondientes penalizaciones económicas, definidas a continuación. La aplicación de las penalizaciones será acumulativa, excepto en los casos de que se indique lo contrario. Las penalizaciones se calcularán como porcentaje de la facturación mensual total y será aplicada como reducción del importe en la siguiente factura.

Los acuerdos de nivel de servicio se podrán mejorar anualmente, siempre y cuando exista un acuerdo mutuo entre el adjudicatario e IMELSA.

Los licitadores deberán describir cuáles son los mecanismos por los cuales garantiza el cumplimiento, validez y exactitud de los indicadores de nivel de servicio. Asimismo deberá describir los mecanismos de verificación de cumplimiento de niveles de servicio que pone a disposición de la Diputación de Valencia, como herramientas de monitorización de las actividades del servicio, como se indica en el apartado 3.2.2.

Los ANS se han elaborado teniendo en cuenta los siguientes criterios:

- Los ANS están relacionados con los requerimientos definidos en el pliego de condiciones técnicas y contractuales, y tienen como objeto establecer los parámetros de calidad “mínimos” para cubrir las expectativas del SGT. Se espera que los licitadores propongan complementarlos con otros que como mínimo debe incluir el ANS de Tiempo de Respuesta del SIGTR con las penalizaciones y mecanismos de control asociados, con el fin de conseguir los objetivos del servicio requeridos.
- Los ANS presentados se consideran extremo a extremo. Es decir, en el caso de que el adjudicatario subcontrate servicios a un tercero, los ANS se consideran tanto a un nivel de servicio único como a nivel agregado a través de los diferentes servicios, manteniendo un único punto de responsabilidad en el adjudicatario del contrato para los ANS.
- El licitador deberá detallar en la propuesta cómo se cumplirán los niveles de servicio requeridos y cuáles son los mecanismos que garantizan dichos niveles de servicio.

Todos los indicadores se medirán en periodos mensuales, excepto cuando se indique lo contrario en la definición del indicador. La penalización se aplicará a la facturación mensual del servicio.

A continuación se detallan los Indicadores que se han definido para medir la calidad mínima del servicio prestado por el adjudicatario:

3.3.1.1 Gestión de la disponibilidad

Código: S1-1

Indicador ANS: Disponibilidad[2] del SIGTR del entorno de producción en horario estándar del periodo.

[2] Definimos Disponibilidad, como el “*porcentaje de minutos mensuales en los que se encuentran operativos en el horario establecido, y con suficientes recursos, todos los elementos del SIGTR incluyendo la infraestructura (comunicaciones, hardware, datos y software de base), en el entorno de producción, para el funcionamiento adecuado del SIGTR*”.

Valor objetivo: 99,99% (incluyendo el tiempo de inactividad programado)

Formula:

$$((Tiempo\_Total\_HEstandar - Ttempo\_no\_disponible)/Ttempo\_Total\_HEstandar) * 100$$

Penalizaciones:

- Rango: entre 99,60% y 99,97%. Descuento: 5%
- Rango: menor 99,60%. Descuento: 10%

Código: S1-2

Indicador ANS: Disponibilidad* del SIGTR del entorno de producción en horario extendido del periodo.

Valor objetivo: 98,00% (no incluye el tiempo de inactividad programado)

Formula:

$$((Tiempo\_Total\_HExtendida - Tiempo\_no\_disponible)/Tiempo\_Total\_HExtendida) * 100$$

Penalizaciones:

- Rango: menor 98%. Descuento:5%

3.3.1.2 Gestión de Incidencias y problemas

Código: S2-1

Indicador ANS: Porcentaje de resolución de incidencias durante el periodo dentro de plazo máximo de resolución según prioridad. Las prioridades serán: **critica: 5 horas**; **media en 12 horas y baja en 48 horas**. Se definirán los criterios de asignación de prioridades durante el Proyecto de implantación del SIGTR y establecimiento del servicio.

Valor objetivo: 98% (para cada prioridad)

Formula:

$$(N^{a}Incidencias\_Resueltas/N^{a}TotalIncidencias\_Registradas) * 100$$

Penalizaciones:

- Rango: menor 98% en alguna prioridad. Descuento: 5%

Código: S2-2

Indicador ANS: Porcentaje de problemas resueltos (cierre) dentro del tiempo medio objetivo de resolución, durante el periodo.

Valor objetivo: 90% en menos de 30 días naturales (tiempo medio objetivo)

Formula:

$((Nº\_Problemas\_Resueltas\_en\ tiempo\ objetiva)) / (NºTotal\_Problemas\_Resueltas) * 100)$

Penalizaciones:

- Rango: menor 90%. Descuento: 5%

3.3.1.3 Gestión de cambios

Código: S3

Indicador ANS: Porcentaje de cambios estándares abiertos en periodo y enviados al Comité de Cambios. Se definirán los tipos de cambio durante el proyecto de implantación y establecimiento del servicio.

Valor objetivo: 99%

Formula:

$(NºCambtas\_Std\_EnviadasAlComite / NºTotalCambtas\_Std) * 100$

Penalizaciones:

- Rango: menor 99%. Descuento: 5%

3.3.1.4 Gestión de continuidad

Código: S4

Indicador ANS: Tiempo de recuperación objetivo o indisponibilidad admisible (RTO *Recovery Time Objective*) del SIGTR

Valor objetivo: 36 horas (tanto en horario estándar como extendido)

Formula:

Instante_tiempo_recupera_SIGTR - Instante_tiempo_produce_desastre

Penalizaciones:

- Rango: mayor 36 horas. Descuento: 10%

3.3.1.5 Gestión de la mejora continua

Código: S5

Indicador ANS: Iniciativas mensuales orientadas a la mejora continua, que serán realizadas en el próximo periodo

Valor objetivo: 2 iniciativas al mes

Penalizaciones:

- Rango: menor de 2 propuestas y realizadas al mes. Descuento: 5%

3.3.1.6 Gestión de la seguridad

Código: S6

Indicador ANS: Porcentaje de resolución (cierre) de recomendaciones y acciones correctivas, respecto a los plazos acordados al final de las auditorías.

Valor objetivo: 90% en plazo

Formula:

*((N°Recomendaciones_resueltas_en_plazo) / (N°Total_Recomendaciones)) * 100*

Penalizaciones:

- Rango: menor del 90%. Descuento: 10%

3.3.1.7 Gestión de la documentación

Código: SP1

Indicador ANS: Porcentaje de documentación completado y entregado en periodo. La documentación a entregar en el proyecto y el servicio será acordada entre el adjudicatario e IMELSA al inicio del proyecto.

Valor objetivo: 100%

Formula:

$(N^{a}DocumentaciónCompletadaYEntregada / N^{a}TotalDocumentación) * 100$

Penalizaciones:

- Rango: menor del 100%. Descuento: 5%

3.3.1.8 Proyecto de implantación del SIGTR y establecimiento del servicio.

Código: P1

Indicador ANS: Porcentaje de cumplimiento de los hitos especificados por actividades planificadas, que estén asociadas al proyecto de implantación del SIGTR, incluida la migración de datos, y establecimiento del servicio.

Valor objetivo: 90%

Formula:

$(N^{a}hitas\_cumplidas\_en\_Fertada / N^{a}TatalHitas\_en\_Fertada) * 100$

Penalizaciones:

- Rango: menor del 90%. Descuento: 10%

3.3.2 Consideraciones para el cálculo de Indicadores ANS y aplicación de penalizaciones

Todos los indicadores ANS miden desviaciones sobre actividades planificadas y realizadas.

El indicador P1 se medirá mensualmente durante el proyecto de implantación del SIGTR y establecimiento del servicio y hasta el final del periodo de transición. El indicador S6 solo será medido después de cada auditoria en cualquiera de sus modalidades.

El indicador S4 se medirá cada vez que se prueba el Plan de Recuperación de Desastres.

Los demás indicadores se medirán mensualmente desde el inicio del servicio después de un periodo de Transición, que no podrá superar los dos meses.

IMELSA tiene la potestad de decidir no aplicar las penalizaciones asociadas a incumplimientos de los indicadores cuando se den algunos de los siguientes supuestos:

- La razón de la desviación se deban a componentes que no están bajo la responsabilidad del adjudicatario.

- Existan situaciones extraordinarias que den lugar a alteraciones que desvirtúen la medida.

3.4 Auditoria del servicio.

El adjudicatario permitirá llevar a cabo, debiendo prestar su total colaboración, las inspecciones y auditorías que IMELSA considere necesarias para verificar el correcto cumplimiento de las obligaciones asumidas en la prestación de los servicios o dimanantes del contrato, y si fuese necesario, permitiendo el acceso a sus instalaciones relacionadas con la prestación de los servicios y a todos los elementos lógicos y físicos que conforman la prestación de los mismos.

Dichas inspecciones y auditorías podrán ser llevadas a cabo por IMELSA o bien por un tercero libremente designado por ésta. Concluida la auditoría y en función de las desviaciones detectadas, el adjudicatario deberá determinar las acciones correctivas para que las desviaciones y observaciones detectadas no vuelvan a tener lugar, así como designar a los responsables de la ejecución de dichas acciones y los plazos para su ejecución. El adjudicatario deberá presentar a la entidad, en el plazo máximo de 15 días naturales, el Plan de Acciones Correctivas, siendo su cumplimiento responsabilidad exclusiva del adjudicatario, según los niveles de servicios requeridos por la IMELSA.

4 Funcionalidades complementarias a las exigidas

Más allá de los requerimientos descritos hasta el momento, que deben ser cubiertos por las propuestas que se presenten, se describen a continuación otras funcionalidades por encima de los requerimientos mínimos y que los licitadores pueden optar a cubrir en sus propuestas sin que esto implique un aumento de las contraprestaciones económicas:

- Extensión de requisitos funcionales y técnicos a las requeridas.
- Ampliación de los Acuerdos de Nivel de Servicio (ANS) descritos en el apartado 3.3. Deberá incluir al menos un indicador de Tiempo de Respuesta
- Extensión de las herramientas requeridas para ofrecer los servicios.

Se invita a los licitadores a identificar y ofrecer funcionalidades no descritas en el pliego que encuentren de interés para cubrir los objetivos de la Diputación de Valencia.

En ningún caso las funcionalidades complementarias supondrán un incremento del precio, y no formarán parte de la valoración de la oferta.

5 Condiciones contractuales

5.1 Periodos en el Proyecto de Implantación y establecimiento del servicio

El contrato preverá la existencia del período del Proyecto de Implantación del SIGTR y el periodo de Transición al servicio regular posterior.

El período de Implantación tendrá una duración máxima de diez meses, a partir de la fecha de entrada en vigor del contrato del servicio.

Deberá existir un periodo de transición con una duración máxima de dos meses, a partir de la fecha de finalización del período de Implantación, es decir, en el momento que esté el SIGTR operativo en producción y la operativa normal del nuevo modelo de servicio. Durante este período, el adjudicatario pondrá en marcha los servicios, definirá los procedimientos operativos, designará los comités para la implementación del Modelo de Relación, y empezará con la medición de los indicadores de ANS del servicio. Al finalizar este período, el adjudicatario asumirá la responsabilidad completa sobre el cumplimiento de los niveles del servicio y calidad percibida acordado, pudiendo ser penalizado conforme a la LCSP.

Así pues el periodo máximo de implantación del SIGTR, transición y establecimiento operativo del nuevo modelo de servicios, será de 12 meses.

5.2 Plan de retorno de los servicios

Los licitadores deberán incluir en su oferta un Plan de Retorno de los servicios, el cual se acordará en caso de ejecución, quedando el adjudicatario obligado al traspaso de aquellos elementos afectos a la prestación de los Servicios a IMELSA, o a un tercero designado por esta, sin coste adicional alguno para IMELSA.

El proveedor saliente estará obligado a mantener el cumplimiento del modelo de medición del servicio durante el período acordado, así como a colaborar para facilitar la transferencia al Proveedor entrante, traspasando los medios y procedimientos necesarios para el Servicio. El equipo del Proveedor saliente encargado de realizar el traspaso deberá haber formado parte de la gestión del Servicio.

Durante este período, que será planificado por IMELSA y con una duración máxima de dos meses, el proveedor saliente no podrá incrementar los importes del servicio, vigentes en el momento de la finalización formal del contrato.

5.3 Confidencialidad y seguridad de la información y protección de datos de carácter personal.

5.3.1 Confidencialidad de la información

El adjudicatario deberá preservar la confidencialidad de toda aquella información a la que tenga acceso con ocasión del desarrollo de la prestación objeto del presente contrato, ya venga referida a la relación contractual entre las partes propiamente dicha o a cualquier otra consustancial a la prestación práctica del servicio. Abarca pues cualquier tipo de información personal, administrativa, técnica, informática y de seguridad.

Este deber de secreto se hace extensivo a los posibles terceros que puedan resultar cesionarios de los derechos y obligaciones dimanantes del presente contrato o a los subcontratistas, en virtud de lo dispuesto en los artículos 226 y 227 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público. El adjudicatario será responsable de trasladar esta obligación a dichos terceros y de actuar diligentemente para velar por su cumplimiento. De los posibles incumplimientos de este deber de secreto y de los perjuicios que ello pudiese reportar responderá el incumplidor y, de forma solidaria, el adjudicatario.

La obligación de confidencialidad persistirá incluso después de finalizar la relación contractual.

Cualquier estudio o publicación por el adjudicatario relacionada con el contenido del contrato o con cualquiera de sus aspectos, requerirá la previa autorización, por escrito, de la Unidad de Gobernanza (UG).

El adjudicatario tendrá la obligación de comunicar cualquier alteración, pérdida, sustracción, acceso, revelación o divulgación de información no autorizada, o incidencia relacionada con la misma, de la que tenga o pueda llegar a tener conocimiento, ya sea producida por la infidelidad de las personas que hayan accedido a la información o por cualquier otra causa, bien entendido que esa comunicación no eximirá al adjudicatario de los compromisos de secreto y confidencialidad y de las responsabilidades que se deriven de dicha omisión.

5.3.2 Seguridad de la información

En el marco del presente contrato, la seguridad de la información se contempla desde la doble incidencia de la normativa reguladora de la materia en el ámbito de la administración electrónica y de la propia de la protección de datos de carácter personal. Por ello, las exigencias de seguridad al adjudicatario se dirigen fundamentalmente al cumplimiento del conjunto de garantías que resultan de aplicación al SIGTR en virtud de ambos segmentos normativos. En este sentido, y a título meramente informativo, se hace constar que el sistema de información SIGTR ha sido catalogado de nivel Medio, conforme a las especificaciones del RD 3/2010, por el que se aprueba el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS), y de nivel Medio según lo establecido por el RD 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999 (RDLOPD).

No obstante, las condiciones sobre seguridad de la información se formulan también en atención al Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia (RPSyPDP), aprobado por el Pleno de la Corporación en sesión de 18 de junio de 2013 (BOP nº 159, de 6 de julio) y a la importancia que la Diputación otorga al objetivo a cumplir por el sistema de información afectado.

En el presente apartado se establecen las condiciones de seguridad que deberán ser implementadas por el adjudicatario en el entorno de la prestación del servicio. Forman parte inseparable también de estas condiciones de seguridad las medidas especificadas en los ANEXOS I y II, obedeciendo su inclusión en dichos anexos a una mera cuestión metodológica para facilitar su implantación.

En el **ANEXO I** se contemplan un conjunto de medidas encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

En el **ANEXO II**, se contienen aquellas medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

En virtud del principio de mayor protección (art. 10 RPSyPDP) cuando sobre un mismo elemento, activo o aspecto del sistema de información deban aplicarse simultáneamente las medidas de seguridad del ANEXO I y del ANEXO II, serán de aplicación las medidas que ofrezcan mayor nivel de protección o de exigencia.

5.3.2.1 Subcontratación

Todas las condiciones de seguridad exigidas al adjudicatario en el marco del presente contrato de servicios lo son con independencia de que todo o parte de los servicios sean objeto de subcontratación. Por tanto, las citadas condiciones de seguridad son exigibles tanto al adjudicatario como a los posibles subcontratistas. El hecho de producirse la subcontratación tampoco supone en ningún caso que se inicien nuevos plazos, ni se interrumpan ni se prorroguen, en los casos en que éstos se establezcan, para el cumplimiento de requisitos de seguridad por parte del subcontratista diferentes a los inicialmente establecidos.

En caso de subcontratación de los servicios por parte del adjudicatario, y a los únicos efectos de los requerimientos de seguridad, éste deberá comunicar a IMELSA y a la Diputación de Valencia antes de proceder a la subcontratación los datos de identificación del subcontratista, el alcance de la subcontratación y el instrumento contractual en el que figuren las obligaciones adquiridas por el subcontratista. De igual modo, se acompañará acreditación suficiente de que el subcontratista cumple los requerimientos de seguridad establecidos para el adjudicatario en el presente pliego técnico, en la medida que le resulten de aplicación en virtud del servicio que se subcontrata.

IMELSA, tras las comprobaciones oportunas, autorizará o no la subcontratación pretendida.

Lo previsto en este apartado lo es sin perjuicio de lo dispuesto en el apartado 5.3.2.9 en materia de protección de datos personales.

5.3.2.2 Análisis inicial de riesgos

Con independencia de lo indicado en el apartado “I.4 Gestión de riesgos” del ANEXO I, el adjudicatario deberá proceder a un análisis de riesgos previo a la puesta en servicio. Dicho análisis de riesgos se efectuará aplicando la metodología MAGERIT v2 o superior y podrá hacer uso de cualquier herramienta reconocida que integre dicha metodología.

El citado análisis contendrá, como mínimo:

- Una identificación de los activos más valiosos del sistema y una valoración cualitativa de los mismos.
- Una identificación y cuantificación de las amenazas posibles.
- Una identificación de las vulnerabilidades habilitantes de dichas amenazas.
- Una identificación y valoración de las salvaguardas adecuadas.
- La identificación y valoración del riesgo residual.

Con independencia de las amenazas identificadas, se incluirán en todo caso las amenazas que se detallan a continuación:

- (E.2) Errores del administrador del sistema/ de la seguridad
- (E.3) Errores de monitorización
- (E.4) Errores de configuración
- (E.15) Alteración de la información
- (E.18) Destrucción de la información
- (E.19) Fugas de información
- (E.20) Vulnerabilidades de los programas
- (E.23) Errores de mantenimiento de los programas (software)
- (E.24) Caída del sistema por agotamiento de recursos
- (A.3) Manipulación de los registros de actividad (log)
- (A.4) Manipulación de los ficheros de configuración
- (A.5) Suplantación de la identidad del usuario
- (A.6) Abuso de privilegios de acceso
- (A.11) Acceso no autorizado
- (A.12) Análisis de tráfico
- (A.13) Repudio (negación de actuaciones)

- (A.14) Interceptación de información
- (A.15) Modificación de la información
- (A.18) Destrucción de la información
- (A.19) Revelación de la información
- (A.22) Manipulación de programas
- (A.24) Denegación de servicio

El informe del análisis de riesgos se trasladará a la Unidad de Gobernanza. Tras su correspondiente estudio, la Unidad de Gobernanza comunicará al adjudicatario su conformidad o disconformidad con el análisis, pudiendo reclamar una revisión del mismo. En última instancia, la Diputación comunicará al adjudicatario las salvaguardas concretas que considere de aplicación y la asunción del posible riesgo residual.

Las salvaguardas concretas podrán coincidir con las medidas establecidas en el ANEXO I o requerir otras complementarias, atendiendo a los riesgos específicos resultantes del proceso de análisis.

El adjudicatario dispondrá de un plazo máximo que coincidirá con el plazo de implantación del SIGTR y establecimiento del servicio definido en el apartado 5.1, para llevar a cabo el análisis de riesgos y, en su caso, la implementación de las salvaguardas requeridas.

5.3.2.3 Auditoría inicial de seguridad

Sin perjuicio de lo indicado en el apartado “I.16 Auditoría de la seguridad” del ANEXO I, y una vez implantadas las salvaguardas concretas que resultasen del análisis inicial de riesgos citado en el apartado anterior, el adjudicatario vendrá obligado a realizar una auditoría que se ajustará a las siguientes indicaciones:

La auditoría será llevada a cabo por un equipo auditor externo al adjudicatario y que, en cualquier caso, no tenga ni haya tenido ningún tipo de vínculo con el adjudicatario que pueda generar dudas sobre su objetividad e independencia.

El equipo auditor estará compuesto por profesionales de la auditoría de seguridad de sistemas de información, con experiencia contrastada y acreditaciones reconocidas (ISACA, ISC, etc).

En la realización de la auditoría se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocida, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información.

El equipo auditor verificará el nivel de cumplimiento de las condiciones de seguridad que debe implementar el adjudicatario (apartado 5.3 y anexos del presente pliego).

El equipo auditor elaborará un informe de auditoría, detallando el grado de cumplimiento, identificando las posibles deficiencias y realizando una propuesta de las medidas correctoras o complementarias que estime necesarias, así como las recomendaciones que crea convenientes. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en se basen las conclusiones formuladas.

A la vista del informe de auditoría, el adjudicatario elaborará un documento en el que se plasme una propuesta de acciones cronológicamente planificadas para, en su caso, subsanar las deficiencias o desviaciones evidenciadas por el equipo auditor; así como todas aquellas cuestiones que considere oportunas en relación con los resultados de la auditoría. Del informe de auditoría elaborado por el equipo auditor y del documento elaborado por el adjudicatario se dará traslado a la Unidad de Gobernanza, que comunicará al adjudicatario su conformidad o introducirá los cambios que considere oportunos.

El adjudicatario dispondrá de un plazo máximo que coincidirá con el plazo de implantación del SIGTR y establecimiento del servicio definido en el apartado 5.1, para llevar a cabo las obligaciones contenidas en el presente apartado incluida, en su caso, la implementación de las acciones correctoras, salvo que, en este último caso, y con carácter extraordinario, la Unidad de Gobernanza otorgará un plazo mayor atendiendo a medidas muy específicas.

La realización de esta auditoria determinará la fecha de cómputo para el cálculo de los dos años establecidos para la realización de la siguiente auditoría regular ordinaria, tal como se contempla en el apartado “I.16 Auditoría de la seguridad” del ANEXO I.

5.3.2.4 Coordinación y supervisión de la seguridad.

La Diputación de Valencia como titular del sistema de información e IMELSA como responsable y gestor técnico del contrato, son responsables de que se cumplan todos los requisitos de seguridad en la prestación de los servicios. La seguridad del sistema de información requiere por tanto, de una correcta coordinación entre la Diputación de Valencia, IMELSA y el adjudicatario.

IMELSA y la Diputación de Valencia se reservan el derecho de supervisar el entorno físico y lógico de la prestación del servicio, en el marco de la seguridad de la información y de la protección de datos personales. El adjudicatario y los posibles terceros que puedan resultar cesionarios de los derechos y obligaciones dimanantes del presente contrato o los subcontratistas, están obligados a facilitar este derecho de supervisión y disponer todo lo necesario para su pleno ejercicio.

Todo tipo de documentación: informes, normativas, procedimientos, documentos requeridos legal o contractualmente, etc., que se generen por el adjudicatario en cumplimiento de los requisitos de seguridad que le impone el presente pliego técnico, pasaran a ser documentación de seguridad del sistema de información y, por tanto, deberán ponerse a disposición de la Diputación de Valencia e IMELSA.

En virtud del Reglamento de Política de Seguridad y de la Protección de Datos de Carácter Personal de la Diputación de Valencia (RPSyPDP) se designa al Jefe de la Unidad Técnica de Protección de Datos, adscrito al Servicio de Informática y Organización, como Responsable de Seguridad de los Sistemas de Información en el ámbito de la Diputación de Valencia.

En el marco del presente contrato de servicios, el interlocutor de la Diputación de Valencia para las cuestiones relacionadas con la seguridad del sistema de información y la protección de datos personales será el referido Responsable de Seguridad de los Sistemas de Información de la Diputación de Valencia.

Cada vez que en las presentes condiciones de seguridad –incluidas las medidas del ANEXO I y II- se requiera el traslado de información, comunicaciones, autorizaciones, etc. a la Diputación de Valencia, se procederá a su cumplimiento mediante su traslado tanto a la Unidad de Gobernanza, como al citado Responsable de Seguridad de los Sistemas de Información de la Diputación de Valencia.

Con carácter específico, se canalizará a través del Responsable de Seguridad:

- Las dudas o interpretaciones que puedan suscitarse en relación con las condiciones de seguridad y de protección de datos personales.

- El acceso por la Diputación a los diferentes registros relacionados con la seguridad y protección de datos personales: incidencias, auditorias, logs de acceso, de actividad, etc.

- La supervisión del entorno físico y lógico de la prestación del servicio en el marco de la seguridad de la información y de la protección de datos personales.

El responsable de seguridad del adjudicatario, designado conforme a lo dispuesto en el apartado “I.6 Competencias de seguridad” del ANEXO I y, en su caso, el apartado “II.2 Responsable de Seguridad” del ANEXO II, será también el interlocutor del adjudicatario en materia de seguridad con el Responsable de Seguridad de los Sistemas de Información de la Diputación de Valencia. En caso de subcontratación, el adjudicatario dispondrá lo necesario para que sólo exista como único interlocutor el responsable de seguridad designado por él.

Los canales de comunicación serán preferiblemente electrónicos, con las debidas garantías de seguridad.

El adjudicatario entregará un informe mensual de seguimiento de los controles de seguridad, cuanto menos sobre los siguientes aspectos:

- Gestión de incidentes de seguridad

- Controles de acceso

- Cumplimiento normativo y legislativo

- Mecanismos de comprobación periódica de los controles de seguridad

5.3.2.5 Prohibición de uso.

El adjudicatario no podrá hacer uso, en el entorno de la prestación del servicio, de dispositivos móviles (ordenadores portátiles, pda’s, tabletas, etc) susceptibles de almacenar información. Si con carácter excepcional, y por circunstancias justificadas, el adjudicatario necesitase de la utilización puntual de alguno de estos dispositivos, deberá recabar previamente su autorización.

Se excluyen, pues, estos dispositivos de la categoría genérica de “soportes de información” cuando se hable de éstos últimos en las condiciones de seguridad –ANEXO I y II- del presente Pliego técnico.

5.3.2.6 Ubicación de la infraestructura tecnológica y de la información.

Los centros de procesamiento de datos, infraestructura y plataforma asociada a los servicios, incluso los alternativos, deberán ser alojados dentro del territorio de la Unión Europea, preferiblemente en la Península Ibérica, por razones horarias y de mayores facilidades para ejercer los controles y auditorías definidas. Ello permite identificar el marco legal aplicable, garantizar en mayor medida su cumplimiento y reducir los riesgos asociados.

El adjudicatario deberá informar en todo momento a la Unidad de Gobernanza de la ubicación de la infraestructura tecnológica y de la información, incluyendo la posible intervención de subcontratistas en la prestación del servicio.

5.3.2.7 Proceso de mejora continua.

El proceso integral de seguridad del que forma parte el sistema de información implicado debe ser objeto de actualización y mejora continua. El adjudicatario colaborará en el ámbito de la prestación del servicio mediante la evaluación, actualización y mejora de las medidas de seguridad implantadas, haciendo uso de herramientas de monitorización y recopilación de información a partir del establecimiento de objetivos de control, aplicando criterios y métodos reconocidos en el ámbito de la gestión de tecnologías de la información.

El adjudicatario informará sobre los procesos de evaluación y mejora citados, y reportará la información obtenida tras su implantación al menos una vez al año.

Sin perjuicio de lo anterior, el adjudicatario establecerá un conjunto de indicadores que midan el desempeño real del sistema en materia de seguridad en los siguientes aspectos:

- Grado de implantación de las medidas de seguridad.
- Eficacia y eficiencia de las medidas de seguridad.
- Impacto de los incidentes de seguridad.

5.3.2.8 Certificaciones sobre productos de seguridad.

El licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, equipos, sistemas, aplicaciones o sus componentes han sido previamente certificados por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

En caso de que no exista la certificación indicada en el párrafo anterior, o esté en proceso, se incluirá, igualmente, referencia precisa, documentada y acreditativa de que son los más idóneos.

5.3.2.9 Protección de datos de carácter personal

Las siguientes condiciones se incorporan en cumplimiento del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD). La Diputación Provincial de Valencia es la responsable de los datos de carácter personal y el adjudicatario, en los términos del artículo 3.g) de dicha norma, ocupa la posición de encargado del tratamiento de dichos datos personales. En este contexto, el tratamiento de datos de carácter personal derivado de la prestación llevada a cabo por el adjudicatario se regirá por lo siguiente:

En principio, queda prohibido con carácter general el acceso por parte del adjudicatario a los datos de carácter personal albergados o tratados en el sistema de información afectado por la prestación de servicios, por no considerarse dicho acceso necesario para el desarrollo de la prestación, salvo en los siguientes supuestos específicos:

A los datos referentes a usuarios internos del sistema (Diputación, EELL, etc) necesarios para el cumplimiento de una obligación recogida en el presente pliego técnico (p.ej. registro de actividad, traslado de información, etc.)

A los datos referentes a cualesquiera usuarios del sistema o de titulares de la información gestionada en general por el sistema de información, para la solución de problemas de carácter técnico que, de forma ineludible, requiera dicho acceso para una rápida y efectiva solución de dicho problema.

A los citados datos personales cuando se produzcan incidencias graves que puedan afectar a la seguridad del sistema o de la información propiamente dicha.

Se prohíbe igualmente al adjudicatario el almacenamiento de datos de carácter personal en soportes portátiles, salvo en los supuestos de copias de respaldo o cuando le sea solicitado por la Diputación de Valencia.

El tratamiento por el adjudicatario de los datos de carácter personal que sea necesario para llevar a buen fin la prestación del servicio objeto del presente contrato a la Diputación de Valencia se ajustará a las instrucciones dadas por esta última, como responsable de dicho tratamiento según lo establecido por el artículo 3.d) de la LOPD.

El adjudicatario se compromete a no aplicar o utilizar con finalidad distinta a la que constituye el objeto del presente contrato los datos de carácter personal aludidos en el apartado anterior y a no comunicar dichos datos a terceros, ni siquiera para su conservación, salvo en los casos de subcontratación recogidos en el presente apartado.

El adjudicatario adoptará las medidas de seguridad contenidas en el ANEXO II del presente pliego técnico, en los términos expresados en el apartado 5.3.2.

A la finalización de la prestación de servicios, el adjudicatario pondrá a disposición de la Diputación de Valencia los datos de carácter personal obrantes en su poder y procederá al borrado físico o destrucción de cuantos soportes los contengan. No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos, garantizando la Diputación, como responsable del fichero, dicha conservación. Esta obligación del adjudicatario abarca los datos personales que se encuentren en poder de terceros, en virtud de los supuestos de subcontratación recogidos en el presente apartado.

En el caso de devengarse la subcontratación prevista en el artículo 227 del texto refundido de la Ley de Contratos del Sector Público, la Diputación de Valencia autorizará el acceso y tratamiento de los datos de carácter personal implicados en los mismos términos y condiciones que los establecidos para el adjudicatario.

En los supuestos anteriores, se entenderá que dichos subcontratistas actúan también como encargados del tratamiento, debiendo asegurarse el adjudicatario de la formalización de los requisitos del artículo 12 de la LOPD respecto de la citada prestación de servicios o subcontratación, así como del cumplimiento por los subcontratistas de todas las obligaciones establecidas por la LOPD, especialmente de las contenidas en citado artículo 12, así como todas aquellas establecidas en el presente apartado que les sean inherentes.

En dichos supuestos, y con carácter previo a facilitar el acceso y/o tratamiento de los datos, el adjudicatario dará cuenta a la Diputación de Valencia de esta circunstancia, facilitando los datos del tercero, el alcance de la prestación y el instrumento contractual en el que figuren las obligaciones adquiridas en materia de protección de datos personales, especialmente las contenidas en el susodicho artículo 12 de la LOPD. El incumplimiento de estos requisitos por parte del adjudicatario conllevará, con independencia de las correspondientes responsabilidades, la no autorización implícita de la Diputación al acceso y/o tratamiento de los datos a dichos terceros.

El adjudicatario y, en su caso, los terceros subcontratistas citados en el punto anterior, deberán guardar secreto profesional respecto de los citados datos de carácter personal. Esta obligación se establece en los mismos términos, en cuanto a desarrollo, responsabilidades y plazos, que lo determinado en el apartado 5.3.1 del presente Pliego técnico.

En la utilización de cualquier tipo de software destinado al tratamiento de datos de carácter personal, el adjudicatario vendrá obligado a incluir en la descripción técnica de dicho software el nivel de seguridad –básico, medio o alto- que permita alcanzar de acuerdo con lo establecido en el Título VIII del RD 1720/2007 (RDLOPD), en cumplimiento de lo dispuesto en la Disposición Adicional Única de dicha norma. El adjudicatario no podrá hacer uso de un software que no permita alcanzar las condiciones de seguridad requeridas en el presente Pliego técnico.

Cualquier modificación legislativa que pudiera afectar a las garantías expuestas anteriormente implicará, tras el pertinente requerimiento de la Diputación de Valencia, la automática adaptación por parte del adjudicatario y los posibles subcontratistas para darle debido cumplimiento.

5.3.3 Cumplimiento regulatorio

El adjudicatario garantiza que los sistemas y servicios contratados cumplen todos los requerimientos regulatorios y contractuales exigidos en la actualidad, y se obliga a realizar las actualizaciones que resulten necesarias en lo sucesivo para permitir el cumplimiento de cualquier nuevo requerimiento legal que resulte de aplicación en el futuro, especialmente en materia tributario, administración electrónica, seguridad, privacidad, interoperabilidad y servicios de sociedad de la información.

La adecuación del adjudicatario, sus actividades y servicios a la normativa nacional vigente que le resulte de aplicación es responsabilidad exclusiva del mismo, al igual que es igualmente responsabilidad exclusiva de éste la falta de cumplimiento de las

obligaciones legales impuestas en materia de seguridad, privacidad y servicios de la Sociedad de la Información.

Los servicios y sistemas incluirán en su ciclo de vida y descripción las especificaciones de seguridad, acompañadas de los correspondientes procedimientos de control.

5.3.4 Formación

El adjudicatario deberá mantener permanentemente informado y formado a su personal implicado en la gestión de los sistemas y servicios contratados sobre las políticas, procedimientos, normas y medidas aplicables a los mismos. La incorporación y adscripción de cualquier nuevo recurso a la gestión de los sistemas y servicios contratados exigirá su concienciación y formación previa sobre todo ello. Asimismo, el adjudicatario se compromete a organizar, preparar e impartir un programa formativo inicial (Plan de Formación) y otro periódico cuando se requiera, sobre el uso de los sistemas y servicios contratados tanto a su propio personal usuario de la Diputación de Valencia y EELL.

6 Contenido de la propuesta a presentar por los licitadores.

El licitador puede adjuntar a su oferta toda la información complementaría que considere de interés, sin embargo tendrá que presentar unos contenidos con una extensión máxima de 80 páginas y estar obligatoriamente estructurada de la forma siguiente:

1. Características Generales
   - Identificación de la oferta
   - Acatamiento con carácter general a las condiciones del pliego
   - Datos de la empresa

2. Conformidad funcional, técnica y condiciones contractuales
3. Solución técnica propuesta:
   - Adecuación de los requerimientos funcionales
   - Adecuación de los requerimientos técnicos
   - Adecuación del modelo de servicio
   - Proyecto de implantación del SIGTR y establecimiento del servicio
   - Detalle del equipo técnico propuesto para la ejecución del contrato

Los Anexos no tendrán limitación en cuanto a extensión, recogerán la información complementaria que se considere de interés.

Todas las ofertas se presentarán en soporte papel y en soporte electrónico

ANEXO I

MEDIDAS DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN

I.1 NORMATIVA DE SEGURIDAD

El adjudicatario dispondrá de uno o varios documentos aprobados por la dirección de la empresa en los que se describa, como mínimo:

- el uso correcto de equipos, servicios, instalaciones e información.
- lo que se considera uso indebido o inapropiado de los equipos, servicios, instalaciones e información.
- los derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente

Este conjunto de documentos que comprende la normativa de seguridad deberá estar en armonía con las condiciones de seguridad recogidas en el presente Pliego técnico.

En dicha normativa se indicará que la misma es de obligado cumplimiento y cómo localizar los procedimientos relacionados. Deberá existir un procedimiento para su revisión y firma regular.

La Diputación de Valencia podrá en cualquier momento instar al adjudicatario a la incorporación o modificación de contenidos de su normativa de seguridad, al objeto de que sea lo más coherente posible con la normativa de seguridad de la Diputación.

La normativa de seguridad y cualquier actualización de la misma será difundida al personal afectado.

I.2 PROCEDIMIENTOS DE SEGURIDAD

El adjudicatario dispondrá de uno o varios documentos aprobados por la dirección de la empresa en los que se detalle de forma clara y precisa:

- cómo deben llevarse a cabo las tareas habituales.
- quién debe realizar cada tarea y con qué frecuencia.
- cómo identificar y reportar comportamientos anómalos

Deben existir procedimientos para aproximadamente el 80% de las actividades rutinarias (p.ej: sobre el inventariado de activos, la modificación de reglas en el firewall, las tareas de backup, etc.). No obstante, se incorporarán también a estos procedimientos de seguridad aquéllos que puedan ser citados de forma expresa en las condiciones de seguridad recogidas en el presente Pliego técnico.

La Diputación de Valencia podrá en cualquier momento instar al adjudicatario a la incorporación o modificación de contenidos de sus procedimientos de seguridad, al objeto de que sean lo más coherentes posibles con los procedimientos de seguridad de la Diputación.

Los procedimientos de seguridad y cualquier actualización de los mismos serán difundidos al personal afectado.

I.3 ARQUITECTURA DE SEGURIDAD

El adjudicatario dispondrá de un conjunto de documentos aprobados por la dirección de la empresa, referidos al planteamiento integral de la seguridad del sistema. La documentación elaborada a estos efectos será, como mínimo, la siguiente:

a) Documentación de las instalaciones. Se detallarán las instalaciones (p.ej: número de instalaciones, su ubicación, etc.). Se precisarán:

• Las áreas existentes (p.ej: CPD, zona de acceso público, zona de carga y descarga, zona de operadores, etc.)

• Los puntos de acceso (p.ej: puerta principal, salida de emergencia, etc.).

b) Documentación del sistema. Se dispondrá de un inventario actualizado del sistema de información. El inventario contendrá una descripción:

• De los equipos (p.ej: servidor de Internet, robot de backup, etc.)

• De las redes internas existentes (p.ej: red local con direccionamiento 92.168.0.0/24, DMZ con direccionamiento 172.16.0.0/24, etc.), y los elementos de conexión al exterior (p.ej: la red local está separada de Internet mediante un firewall, etc.).

• De los puntos de acceso al sistema (p.ej: puestos de trabajo, consolas de administración, web de la intranet, etc).

• De los responsables de los elementos; entendiendo como responsable a la persona que es responsable de las decisiones relativas a cada elemento (p.ej: el responsable del router es el responsable de comunicaciones).

c) Documentación de líneas de defensa. Se dispondrá de un inventario con un esquema de los sistemas de seguridad del sistema de información (p.ej: firewalls, antivirus, antispam, antiphishing, etc.). El inventario contendrá una descripción:

• De los elementos de interconexión a otras redes (p.ej: la conexión con Internet se realiza a través de un router, la conexión con otras oficinas se realiza mediante un

túnel VPN IPSec, la conexión desde portátiles remotos se realiza mediante VPN SSL, etc.).

• De los elementos de defensa en las conexiones a otras redes (p.ej: la conexión con Internet se realiza a través de un firewall, etc.).

• De las posibles tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa (p.ej: el antivirus del firewall es diferente del antivirus del servidor de correo, el sistema operativo del router es diferente del sistema operativo del firewall, etc.).

d) Documentación del sistema de identificación y autenticación de usuarios. Se detallarán los sistemas de identificación y autenticación de usuarios para cada sistema o servicio. Se precisarán:

• El mecanismo de autenticación a cada sistema o servicio (claves concertadas, contraseñas, tarjetas de identificación, etc.).

• Dónde se almacenan las contraseñas (p.ej: las claves se almacenan cifradas en el fichero /etc/shadow en Linux, Active Directory en Windows, etc.).

e) Documentación de los controles técnicos internos. Se detallará cómo se controlan los datos una vez en los sistemas (p.ej: el intercambio de información con otros sistemas va acompañado de hashes para evitar su alteración, etc.). Se describirá la validación de datos de entrada, salida y datos intermedios (p.ej: validación de rangos en los datos, bloqueo de caracteres no autorizados, etc.)

f) Documentación del sistema de gestión con actualización y aprobación periódica. Se detallará cómo se gestionan los elementos antes enumerados (p.ej: cómo se da de alta un nuevo usuario, cómo se autoriza la conexión con un sistema externo, cómo se autoriza el acceso a un área restringida, etc.), con qué frecuencia se revisan (bien explícitamente o implícitamente en los documentos de gestión de cambios), quién es el encargado de la tarea y quién es el responsable de su aprobación.

I.4 GESTIÓN DE RIESGOS

El adjudicatario deberá llevar a cabo una gestión de riesgos que permita el mantenimiento de un entorno controlado, minimizando dichos riesgos hasta niveles aceptables. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que esté expuesto el sistema.

El análisis de riesgos, entendido como la utilización sistemática de la información disponible para identificar peligros y estimar los riesgos, deberá tener carácter formal y

se ceñirá a lo indicado en el apartado 5.3.2.2 del presente Pliego técnico en lo referente a la metodología, herramienta, contenido mínimo y procedimiento para el traslado del informe, aprobación por la Unidad de Gobernanza y asunción del riesgo residual.

Se realizará un análisis de riesgos ordinario de forma anual, que será revisado sistemática y periódicamente al objeto de considerar cualesquiera situaciones que puedan modificar en el tiempo sus parámetros de riesgo. Se llevará a cabo también un análisis de riesgos específico en todos aquellos supuestos en que así se indique en las condiciones de seguridad que son de aplicación al presente contrato y, de igual forma, cuando la Diputación de Valencia o IMELSA lo requiera puntualmente del adjudicatario en base a circunstancias especiales. En todo caso, deberá realizarse un análisis de riesgos en los siguientes supuestos:

- cuando cambie la información manejada.
- cuando cambien los servicios prestados.
- cuando ocurra un incidente grave de seguridad.
- cuando se reporten vulnerabilidades graves.

El adjudicatario deberá presentar trimestralmente los resultados de análisis de vulnerabilidades de las siguientes áreas:

- escaneo de vulnerabilidad de la infraestructura de electrónica de red y comunicaciones.
- escaneo de vulnerabilidades de las bases de datos.
- escaneo de vulnerabilidades de las aplicaciones web.

I.5 GESTIÓN DEL PERSONAL

El adjudicatario deberá observar las siguientes medidas en relación con el personal que intervenga en la provisión del servicio.

a) Deberá disponer de una política o normativa documentada donde se caracterice cada puesto de trabajo en materia de seguridad. Dicha caracterización comprenderá:

- la definición de las responsabilidades relacionadas con cada puesto de trabajo, basándose en el análisis de riesgos en la medida en que afecta a cada puesto de trabajo.

- la definición de los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular en términos de confidencialidad.

- la obligación de tener en cuenta los requisitos del puesto de trabajo en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias..

b) Deberá informar a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, así como recabar de cada persona su aceptación, expresa y por escrito, de dichos deberes y responsabilidades. A tales efectos, se dispondrá de un documento para cada perfil con sus deberes y responsabilidades, las medidas disciplinarias a que haya lugar, el apercibimiento de que las obligaciones, especialmente la de confidencialidad, se mantienen tanto en el período durante el cual se desempeña el puesto como posteriormente, en caso de traslado a otro puesto de trabajo o cese, y la aceptación del trabajador.

c) Deberá disponer de un procedimiento documentado que especifique la forma de informar y documentar recogidas en el apartado anterior.

d) Deberá disponer de un plan de concienciación al personal que, de forma regular, recuerde los deberes y obligaciones en materia de seguridad, especialmente en relación con la normativa sobre el buen uso del sistema, la identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado, y el procedimiento de reporte de incidencias de seguridad, sean reales o falsas alarmas. Se habilitará un registro que deje constancia de que cada persona ha recibido y seguido el plan de concienciación.

e) De igual forma, deberá confeccionarse un plan de formación en el que se identifiquen las necesidades formativas de cada puesto de trabajo, la planificación en la impartición de la formación necesaria y la frecuencia con la que se debe actualizar la formación. En particular, los contenidos de la formación abarcarán la configuración del sistema, la detección y reacción a incidentes, y la gestión de la información en cualquier soporte en que ésta se encuentre (almacenamiento, transferencia, copias, distribución y destrucción). Se habilitará un registro que deje constancia de la recepción de la formación que estaba planificada por parte del personal, así como la valoración de la misma.

f) Al objeto de corregir o, en su caso, exigir responsabilidades, el personal con acceso al sistema estará sujeto a las mismas condiciones que las establecidas

en el apartado “Autorización y control de acceso” (I.7) del presente ANEXO para los usuarios del sistema de información.

I.6 COMPETENCIAS DE SEGURIDAD

El adjudicatario debe garantizar en el ámbito de la prestación del servicio que la seguridad del sistema de información esté encomendada a personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

Entre el personal con competencias de seguridad, el adjudicatario deberá designar uno o varios administradores de seguridad, que serán los responsables de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información. Deberá designar también un responsable de seguridad, que tendrá como cometido fundamental supervisar la correcta implementación de las medidas de seguridad y su cumplimiento

El adjudicatario deberá proporcionar al responsable de seguridad designado las atribuciones y el entorno de independencia requeridos para el óptimo desarrollo de sus competencias. En ningún caso podrán recaer en una misma persona las competencias de administrador de seguridad y responsable de seguridad. Tampoco podrán asignársele al responsable de seguridad otras funciones que entren en conflicto con sus competencias de seguridad.

En caso de desastre, el responsable de seguridad del adjudicatario se incorporará al comité de crisis y coordinará todas las actuaciones relacionadas con cualquier aspecto de la seguridad en el sistema de información.

I.7 AUTORIZACIÓN, CONTROL DE ACCESO Y REGISTROS DE ACTIVIDAD

A) El adjudicatario dispondrá de un proceso formal de autorizaciones, contenido en la normativa de seguridad que se indica en el punto I.1, y que cubra los siguientes elementos del sistema de información:

• el acceso de una entidad (usuario o proceso) al sistema de información.

• la utilización de instalaciones, tanto habituales como alternativas.

•la entrada de equipos en producción, en particular, equipos que involucren criptografía.

- la instalación en el sistema de cualquier elemento físico o lógico.
- la entrada de aplicaciones en producción.
- el establecimiento de enlaces de comunicaciones con otros sistemas.
- la utilización de medios de comunicación, habituales y alternativos.
- la utilización de soportes de información.
- la utilización de equipos móviles.

Las autorizaciones serán realizadas por las personas debidamente habilitadas para ello. La citada normativa de seguridad contemplará, para cada tipo de componente o actuación, la persona o punto de contacto para su autorización. Deberá existir un modelo de solicitud (formulario) que contenga la descripción del elemento (componente) o actuación para la que se solicita la autorización, las actividades para las que se requiere el nuevo componente (motivación), el tiempo para el que se solicita la autorización (que puede ser temporal o permanente), justificación de que no afecta a otras funcionalidades del sistema, un análisis de riesgo conforme a la categoría del sistema (si el nuevo componente introduce posibles vulnerabilidades), justificación de que no viola ninguna normativa de seguridad, información de los procedimientos que son de aplicación, así como de la necesidad de desarrollar nuevos si fuese necesario.

B) El acceso al sistema de información por una determinada entidad (usuario o proceso) deberá estar previamente autorizado conforme a las especificaciones establecidas por la Diputación de Valencia. Los accesos al sistema que sean requeridos para la adecuada prestación del servicio en el entorno del adjudicatario respetarán, en cualquier caso, los siguientes principios:

a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones.

b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable.

El adjudicatario dispondrá de mecanismos para el control de todos los accesos (usuarios o procesos) al sistema de información, sean locales o remotos. Estos mecanismos deberán garantizar:

• que se protegen los recursos del sistema, de forma que se impida su utilización salvo a las entidades que disfruten de derechos de acceso suficientes. Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.

• que cada entidad (usuario o proceso) que accede al sistema tiene un identificador singular, que permita saber quién ha hecho algo y qué ha hecho.

• la existencia de un registro de las entidades responsables de cada identificador, que permita saber a quién corresponde cada identificador y los permisos o derechos que tiene.

• la inhabilitación del identificador cuando el usuario deja la organización, cesa en la función para la cual se requería la cuenta de usuario o cuando la persona que la autorizó da orden en sentido contrario.

• que, no obstante la inhabilitación anterior, el identificador se mantiene durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a los mismos (período de retención).

• la segregación de funciones y tareas críticas, de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita. Como mínimo serán incompatibles: desarrollo con operación del sistema, configuración y mantenimiento del sistema con operación del sistema, auditoría o supervisión del sistema con cualquier otra función.

• la utilización de mecanismos de autenticación dotados de las siguientes características:

- el mecanismo de autenticación en cada recurso se encontrará identificado (p.ej: mediante un listado de los recursos que requieren autenticación y su mecanismo de autenticación correspondiente)

- no se admitirá el uso de claves concertadas, salvo supuestos justificados y bajo indicación expresa de la Unidad de Gestión y Operación.

- se utilizarán preferentemente dispositivos de tipo físico (tokens) o componentes lógicos (certificados software, biométricos o equivalentes)

- en el caso de utilizar contraseñas, la calidad y renovación de las mismas se ajustará a las instrucciones dadas por la Unidad de Gestión y Operación.

- los autenticadores solo se activarán cuando se encuentren bajo el control efectivo del usuario y se mantendrán bajo su control exclusivo mientras se encuentren activos. La periodicidad de su renovación será la que decida la Unidad de Gestión y Operación.

- La retirada y deshabilitación de los autenticadores se producirá cuando la entidad (persona, equipo o proceso) que autentican finalice su relación con el sistema.

- para los usuarios del entorno del adjudicatario se dejará constancia de la recepción del autenticador, del conocimiento y aceptación de las obligaciones que implica su tenencia, en particular el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.

• en los accesos locales (se considera acceso local al realizado desde puestos de trabajo dentro de las propias instalaciones de la organización):

- el sistema se configurará de forma que no se revele información del sistema antes de un acceso autorizado. Los diálogos de acceso (al puesto local dentro de la propia instalación de la organización, al servidor, al dominio de red, etc.) no revelarán información sobre el sistema al que se está accediendo, salvo la que resulte indispensable.

- los intentos de acceso fallidos estará limitado al número que establezca la Diputación de Valencia, bloqueándose la cuenta si se supera el límite de intentos. Existirá un registro que recoja tanto los accesos con éxito como fallidos.

- una vez efectuado el acceso, el sistema mostrará un aviso con las obligaciones fundamentales del usuario, así como información del último acceso efectuado con éxito con su identidad (por ej. fecha y hora de la conexión).

• en los accesos remotos (se considera acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros):

- se observarán las mismas condiciones que las señaladas para el acceso local.

- se protegerá el canal de acceso remoto con las medidas indicadas en el presente ANEXO para la Protección de las comunicaciones.

C) El adjudicatario habilitará un registro o registros con las actividades de los usuarios en el sistema, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, tanto a nivel operativo como de administración, permitiendo identificar en cada momento a la persona que actúa. Considerando la incidencia que esta medida puede tener en los derechos individuales de los usuarios, lo cual requiere de una valoración jurídica previa a la determinación de la información necesaria y a las condiciones para su obtención, el adjudicatario deberá acordar con la Unidad de Gestión y Operación la concreción de la información que será objeto de registro y los requisitos para su obtención.

Sin perjuicio de lo anterior, las características mínimas que deberán cumplir los citados registros de actividad son las siguientes:

• indicará quién realiza la actividad, cuándo la realiza y sobre qué información, sea cual sea el usuario.

• incluirá la actividad de los operadores y administradores del sistema. Se configurará el sistema de forma que los propios operadores y administradores no puedan modificarlos o eliminarlos.

• se registrará tanto las actividades llevadas a cabo con éxito como los intentos fracasados.

• la determinación de las actividades a registrar y su nivel de detalle se realizará en base al análisis de riesgos del sistema.

• la determinación de las actividades a registrar y su nivel de detalle se realizará en base al análisis de riesgos del sistema.

• se configurará el sistema de forma que el contenido de dichos registros no puedan modificarse, así como la garantía de protección ante la eliminación por personas no autorizadas.

El adjudicatario dispondrá de un inventario de los registros de actividad, donde además se indicará el personal autorizado a su acceso o eliminación. Y el período de retención de los mismos.

El adjudicatario acordará con la Unidad de Gestión y Operación los períodos de retención específicos de los registros de actividad.

Las únicas personas con permiso para la administración de los registros de actividad son el Responsable de Seguridad de los Sistemas de Información de la Diputación de Valencia y el Responsable de Seguridad, designado por el adjudicatario conforme a lo establecido en el apartado I.6 del presente ANEXO, con las siguientes atribuciones:

- ambos responsables de seguridad serán, en principio, los únicos que tendrán acceso a los registros de actividad.

- la supervisión y garantía de la eliminación de dichos registros, conforme a los períodos de retención establecidos, corresponde al Responsable de Seguridad del adjudicatario.

- el Responsable de Seguridad de los Sistemas de Información de la Diputación de Valencia autorizará, previa petición, el acceso de otras personas a los registros de actividad cuando dicho acceso se justifique debidamente en razón de una función en el sistema que así lo requiera o por circunstancias concretas o de fuerza mayor, pudiendo establecer en la autorización límites temporales o funcionales.

- el Responsable de Seguridad del adjudicatario revisará sistemática y periódicamente los registros de actividad, reportando un informe mensual de carácter estadístico al Responsable de Seguridad de los Sistemas de Información de la Diputación de Valencia.

- el Responsable de Seguridad del adjudicatario pondrá en conocimiento del Responsable de Seguridad de los Sistemas de Información de la Diputación de Valencia de forma inmediata cualquier hecho -evidente, indiciario o sospechoso- que, tras la revisión de los registros de actividad, pudiese ser constitutivo de la realización de actividades indebidas o no autorizadas.

El adjudicatario dispondrá de un plan para garantizar la capacidad de almacenamiento de registros atendiendo a su volumen y política de retención, así como de un procedimiento para la eliminación de los registros tras el periodo estipulado de retención, incluyendo las copias de seguridad (si existen).

Las copias de seguridad, si existen, se ajustarán a los mismos requisitos establecidos a los registros en vivo.

La normativa y procedimientos de seguridad (apartados I.1 y I.2) deberán contener las necesarias especificaciones para el cumplimiento efectivo de lo indicado en el presente apartado.

I.8 PROTECCIÓN DE LAS INSTALACIONES E INFRAESTRUCTURAS

El equipamiento será instalado en áreas separadas específicas para su función. A estas áreas separadas solo se podrá acceder por las entradas previstas y vigiladas. Únicamente tendrán acceso al área las personas debidamente autorizadas. Se habilitarán dispositivos que impidan el acceso no autorizado. El control de acceso a dichas áreas se efectuará mediante mecanismos que permitan identificar inequívocamente a la persona que accede, así como la fecha y hora de entrada y salida. Se llevará un registro en el que conste toda la información de acceso anterior. Cuando el registro no se encuentre automatizado (p.ej: se lleva un listado en soporte papel) deberá hacerse constar también la persona que efectúa el registro. Los datos del registro de accesos se mantendrán, como mínimo, durante un período de seis meses.

Los locales donde se ubiquen los sistemas de información y sus componentes dispondrán de las adecuadas condiciones de temperatura y humedad, atendiendo a las especificaciones de los fabricantes de los equipos. Se instalarán mecanismos que permitan el control de los valores recomendados. Los locales contarán con las protecciones adecuadas frente a las amenazas identificadas en el análisis de riesgos, tanto de índole natural como derivadas del entorno o con origen humano, accidental o deliberado. Estará prohibida la existencia de material innecesario en el local, en particular material inflamable (papel, cajas, etc.) o que pueda ser causa de otros incidentes (fuentes de agua, plantas, etc.), y evitando que el propio local sea una amenaza o atractor de otras amenazas. El cableado contará con la protección adecuada, mediante su etiquetado (para poder determinar las conexiones de cada cable físico), protección (para evitar tropiezos) y control (para evitar la existencia de cableado fuera de uso). Se dispondrá de un plano del cableado que incluya el etiquetado de los cables.

Los locales deben contar con la potencia eléctrica necesaria. Se dispondrá de un análisis de la potencia eléctrica requerida, que se actualizará antes de la adquisición de nuevos componentes. Deberá contarse con las tomas eléctricas necesarias (p.ej: enchufes con toma de tierra, cantidad de enchufes suficiente para no tener que recurrir a multiplicadores en cascada que superen los W máximos recomendados, etc.). De igual modo, se garantizará el correcto funcionamiento de las luces de emergencia, mediante la revisión periódica de las mismas. Se incorporarán mecanismos que garanticen el suministro de potencia eléctrica en caso de fallo del suministro general (compuesto por SAI y, en caso de ser necesario, grupo electrógeno), de forma que se cuente con tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información

Se protegerán los locales frente a incendios, fortuitos o deliberados, conforme a la normativa industrial pertinente (p.ej: disponer de carteles para evacuación, extintores, materiales no inflamables, etc.). Del mismo modo, se protegerán los locales frente a incidentes fortuitos o deliberados causados por el agua (p.ej: que el CPD no sea recorrido por tuberías de agua, que existan sumideros de agua en el CPD, etc.) conforme al nivel de riesgo identificado, lo que comporta la realización de un estudio

de la ubicación física del local para conocer el riesgo real de problemas por causa natural o por el entorno.

Deberá mantenerse un registro pormenorizado de toda entrada y salida de equipamiento. El registro debe reflejar: fecha y hora, identificación inequívoca del equipamiento, persona que realiza la entrada o salida, persona que autoriza la entrada o salida y persona que realiza el registro. Los datos del registro de entradas y salidas de equipamiento se mantendrán, como mínimo, durante un período de doce meses.

La normativa y procedimientos de seguridad (apartados I.1 y I.2) deberán contener las necesarias especificaciones para el cumplimiento efectivo de lo indicado en el presente apartado.

I.9 CONFIGURACIÓN DE SEGURIDAD POR DEFECTO

Deberá realizarse una fortificación o bastionado del sistema de información previo a su entrada en operación de manera que se implemente una configuración segura por defecto; para esto deberán seguirse las guías CCN-STIC correspondientes, cubriendo al menos los siguientes aspectos:

a) Se retirarán las cuentas y contraseñas estándar (p.ej: los servidores Linux no deben tener la cuenta “root”, los servidores Windows no deben tener la cuenta “administrador” ni “invitado”, etc.)

b) Se desactivarán las funcionalidades técnicas no requeridas, ni necesarias, ni de interés o inadecuadas, ya sean gratuitas, de operación, administración o auditoría (p.ej: si se adquiere un firewall para proteger el perímetro y este proporciona la funcionalidad de acceso remoto mediante VPN IPSec, si dicha funcionalidad añadida no es necesaria ni ha sido solicitada por el responsable deberá haber sido deshabilitada). Dichas funcionalidades quedarán documentadas y constará el motivo por el que se hayan deshabilitado.

c) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

d) Dispondrá de mecanismos que garanticen la corrección de la hora a la que se realiza el registro (de actividad, de incidencias, etc).

e) Se establecerán bloqueos de sesión por tiempo de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

f) Se habilitarán mecanismos de prevención y reacción frente a código dañino (virus, gusanos, troyanos, programas espía y “malware” en general) dañino para todos los equipos (servidores y puestos de trabajo) Las opciones de configuración serán las recomendadas por el fabricante, así como las referentes a frecuencia de actualización; en caso contrario estará documentado el motivo.

g) El uso ordinario del sistema por los usuarios deberá ser sencillo y seguro. En caso de existir situaciones que puedan poner en riesgo la seguridad, y siempre que se trate de supuestos en que la organización la consienta bajo la responsabilidad del usuario, el sistema indicará esa posibilidad y las consecuencias al usuario, de forma que éste sea consciente de su exposición a un riesgo, debiendo el usuario dar su consentimiento expreso asumiendo el riesgo (p.ej: debe aparecerle al usuario una ventana de advertencia, que por defecto tendrá marcada la opción de “no continuar”, informando de esto al usuario y solicitándole la aceptación de las condiciones). De estos consentimientos informados de los usuarios quedará constancia en un registro.

El adjudicatario dispondrá de un procedimiento documentado que indique la frecuencia y motivos por los que se debe modificar la configuración del sistema e incluirá: la aprobación del responsable, la documentación del cambio, las pruebas de seguridad del sistema bajo la nueva configuración, y la retención de la configuración previa por un tiempo preestablecido.

I.10 INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

El adjudicatario dispondrá de un plan de mantenimiento del equipamiento físico y lógico que indique la frecuencia, componentes a revisar, responsable de la revisión y evidencias a generar. Respecto a dicho plan de mantenimiento:

• atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.

• contemplará mecanismos para el seguimiento continuo de los anuncios de defectos (p.ej: suscripción a lista de correo de avisos de defectos por parte del fabricante o un proveedor de este tipo de anuncios) y un procedimiento documentado que indique quién y con qué frecuencia debe monitorizar esos anuncios, así como el procedimiento para analizar, priorizar (en función del cambio en el riesgo derivado por la aplicación o no de la recomendación) y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.

I.11 GESTIÓN DE CAMBIOS

Deberá mantenerse un control continuo de cambios realizados en el sistema. En tal sentido, el adjudicatario contará con un procedimiento de gestión de cambios, que indicará la frecuencia y motivos por los que se debe cambiar un componente del sistema e incluirá: la aprobación del responsable, la documentación del cambio, las pruebas de seguridad del sistema tras el cambio, y la retención de una copia del componente previo por un tiempo preestablecido.

Respecto a dicho control de cambios:

• analizará todos los cambios anunciados por el fabricante o proveedor para determinar su conveniencia para ser incorporados o no.

• antes de poner en producción una nueva versión o una versión parcheada se comprobará en un equipo que no esté en producción (equivalente al de producción en los aspectos que se comprueban) que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

• se planificarán los cambios para reducir el impacto sobre la prestación de los servicios afectados.

• se determinará mediante análisis de riesgos si los cambios son relevantes para la seguridad del sistema. En caso de que el cambio implique una situación de riesgo de nivel alto deberá ser aprobado explícitamente de forma previa a su implantación.

I.12 GESTIÓN DE INCIDENCIAS

El adjudicatario dispondrá de un proceso integral para hacer frente a incidentes que puedan tener un impacto en la seguridad del sistema. Dicho proceso estará conformado por una serie de procedimientos que, como mínimo, serán los siguientes:

a) Procedimiento de reporte de incidentes reales o sucesos sospechosos (p.ej: aumento considerable de logs de error, ralentización del servicio, etc) bien sean internos o provenientes de servicios prestados por terceras partes, así como el detalle del proceso de escalado de la notificación (p.ej: un usuario final debe comunicar el incidente al centro de soporte, este analiza si es un incidente de seguridad, en cuyo caso lo reporta al técnico responsable de estos incidentes, etc.).

b) Procedimiento de toma de medidas urgentes, contemplando la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros (según convenga al caso). Dicho procedimiento deberá contemplar la toma de medidas urgentes en base a un procedimiento

de valoración de la urgencia, y quién debe tomar estas decisiones. Como resultado de dicha valoración se contemplan las medidas a tomar (detención de los servicios, aislamiento del sistema, etc).

c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

d) Procedimiento para avisar a las partes interesadas tanto internas (p.ej: avisar a los usuarios de la organización de la indisponibilidad o degradación de un servicio y el tiempo estimado de resolución) como externas (p.ej: avisar a los ciudadanos u otros organismos relacionados con la organización de la indisponibilidad o degradación de un servicio y el tiempo estimado de resolución). Cuando el incidente se deba a defectos en el equipamiento que pudieran causar problemas similares en otras organizaciones, el procedimiento contemplará la notificación de los mismos al CERT.

e) Procedimiento para prevenir que se repita el incidente. Dicho procedimiento contemplará, dentro de la investigación de las causas, las medidas necesarias para evitar que el incidente vuelva a producirse.

f) Procedimiento para incluir en los procedimientos de usuario la identificación y forma de tratar el incidente. Dicho procedimiento para la gestión de incidencias estará orientado al usuario final que corresponda, de forma que éste sepa identificar y resolver los incidentes más comunes.

g) Procedimiento para actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidencias.

El adjudicatario dispondrá de sistemas de notificación automatizada de incidencias. De igual modo, deberá mantener un registro de todas las actuaciones relacionadas con la gestión de las mismas. Dicho registro se ajustará, como mínimo, a lo siguiente:

• se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

• se registrarán aquellas evidencias que puedan, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos. La composición y detalle de estas evidencias implica criterios jurídicos especializados, por lo que el adjudicatario deberá acordar con la Diputación de Valencia las concretas evidencias que serán objeto de registro.

• se revisará la determinación de los eventos auditables en base al análisis de las incidencias.

I.13 PROTECCIÓN DE LA INFORMACIÓN ALMACENADA Y EN TRÁNSITO

A) El adjudicatario dispondrá de un sistema de cortafuegos que separe la red interna del exterior, de modo que todo el tráfico con el exterior pase a través del cortafuegos. Sólo se permitirá el tráfico que haya sido previamente autorizado. El perímetro concreto, delimitado y acotado, estará reflejado en la arquitectura del sistema (ver apartado I.3).

Las comunicaciones que discurran por redes fuera del propio dominio de seguridad utilizarán VPN, empleando protocolos estándar como IPSEC, SSL o TLS. En cualquier caso, el cifrado de las comunicaciones deberá ajustarse, como mínimo, a los siguientes parámetros:

TIPO DE CIFRADO	LONGITUD DE CLAVE
Cifrado simétrico TDEA y AES	112 bits
Cifrado basado en curvas elípticas	224 – 255 bits
Cifrado RSA, clave pública	2048 bits

La protección de las claves de cifrado, independientemente de la seguridad que ofrezcan, cumplirá los siguientes requisitos:

• la protección abarcará todo el ciclo de vida de las claves: su generación, transporte al punto de explotación (p.ej: entrega en mano, uso de contenedores físicos seguros o criptográficos, doble canal – clave y datos de activación por separado-), custodia durante la explotación, archivo posterior a su retirada de explotación activa y destrucción final (p.ej: eliminación de original y copias)

• los medios de generación deben estar aislados de los medios de explotación.

• las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación (p.ej. en contenedores físicos seguros o en contenedores criptográficos).

• se utilizarán medios de generación y custodia en explotación evaluados o dispositivos criptográficos certificados. Dichos medios emplearán algoritmos acreditados por el CCN.

• los medios de custodia en explotación deberán emplear tarjeta inteligente protegida por contraseña.

• existirá un registro que indique las actuaciones realizadas sobre cada clave en el sistema a lo largo de su ciclo de vida.

Se dispondrá de mecanismos para la prevención de ataques activos, garantizando que al menos serán detectados y, en caso de ocurrir, la consiguiente activación de los procedimientos previstos de tratamiento del incidente. Se consideran ataques activos (por contraposición a los ataques pasivos, en los que sólo se monitoriza la comunicación con el fin de obtener información de la misma o de lo intercambiado en ella) a aquellos ataques en los que se altere la información transmitida, se inserte información engañosa, o se secuestre la comunicación por una tercera parte.

B) Los soportes de información, tanto los que permanecen en los locales de la organización como los que salen a otros destinos, deberán ser etiquetados. Dicho etiquetado se realizará bajo las siguientes premisas:

• el etiquetado no debe revelar el contenido (p.ej: la etiqueta no contendrá palabras tipo “datos tributarios”, “datos padrón IBI”, etc. sino un código no interpretable por personal ajeno al procedimiento), pero debe indicar el nivel de seguridad de la información contenida de mayor calificación, de forma que no sea comprensible para alguien ajeno al sistema (p.ej: la etiqueta no contiene palabras tipo “confidencial”, “reservado”, “secreto”, etc. sino un código no interpretable por personal ajeno al procedimiento).

• los usuarios deben entender el significado de las etiquetas, bien mediante simple inspección, bien recurriendo a un repositorio que lo explique.

• los usuarios deben entender el significado de las etiquetas, bien mediante simple inspección, bien recurriendo a un repositorio que lo explique.

A los citados soportes de información se les aplicarán mecanismos criptográficos que garanticen la confidencialidad e integridad de la información contenida. Para su transporte se utilizarán los medios de protección criptográfica correspondientes al nivel de calificación de la información contenida de mayor nivel. Las claves se gestionan conforme a lo especificado en el apartado I.13.A).

Se dispondrá de un inventario de todos los soportes de información en uso, indicando su etiqueta, contenido actual, ubicación física y quién es el responsable del mismo. Se

aplicará la debida diligencia y control de los soportes de información mediante las siguientes actuaciones:

• se garantizará el control de acceso con medidas físicas, lógicas o ambas (ver I.8)

• se respetarán las exigencias de mantenimiento del fabricante, en especial en lo referente a temperatura, humedad y otros agresores medioambientales.

• se mantendrá la historia de cada dispositivo, desde su primer uso hasta la terminación de su vida útil y/o destrucción del mismo

Se dispondrá de un registro de entrada y salida de soportes donde se identifique la etiqueta del soporte, al transportista que efectúa su entrega y el que recibe el soporte para su traslado, respectivamente. De igual modo, se dispondrá de un procedimiento rutinario que coteja las salidas con las llegadas y levanta las alarmas pertinentes cuando se detecte algún incidente.

Se dispondrá de medidas que garanticen el borrado y destrucción seguros de los soportes de información, sean o no electrónicos. Se dispondrá de un procedimiento documentado que especificará en qué circunstancia se debe proceder al borrado, quién debe realizarlo y el método de borrado seguro de los soportes. Serán objeto de borrado seguro los soportes que vayan a ser reutilizados para otra información o liberados a otra organización. Se destruirán de forma segura los soportes cuando la naturaleza del soporte no permita un borrado seguro o cuando así lo requiera el procedimiento asociado al tipo de información contenida. En el borrado y destrucción de soportes se emplearán, preferentemente, productos certificados.

C) Se dispondrá de un procedimiento para limpiar (retirar la información contenida en campos ocultos, meta-datos, comentarios o revisiones) todos los documentos que vayan a ser transferidos a otro dominio de seguridad o publicados electrónicamente, salvo cuando dicha información sea pertinente para el receptor del documento. El procedimiento indicará el destino del documento, y, si va a ser transferido a otro dominio de seguridad o publicado electrónicamente, señalará cómo limpiar el documento. Se dispondrá de herramientas evaluadas para limpiar los documentos.

I.14 RESPALDO Y RECUPERACIÓN DE DATOS

El adjudicatario dispondrá de un procedimiento de copias de respaldo que garantice la restauración de la información frente a supuestos de pérdida de datos accidentales o intencionados. El procedimiento especificará la frecuencia con la que deben realizarse las copias y el periodo de retención durante el que mantenerlas. De igual modo, contendrá el plan para realizar regularmente el backup y su eliminación. Los periodos de realización y eliminación de las copias y respaldo se ajustarán a lo que establezca la Unidad de Gestión y Operación.

Se dispondrá de mecanismos de backup (p.ej: robot, unidad de cinta, cintas, disco duro para almacenamiento de copias, aplicación de backup, etc.) y de eliminación segura (p.ej: software de eliminación segura, desmagnetizador, etc.).

Las citadas copias de seguridad deberán abarcar:

• la información de trabajo de la organización.

• las aplicaciones en explotación, incluyendo los sistemas operativos.

• los datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.

• las claves utilizadas para preservar la confidencialidad de la información.

Las copias de respaldo disfrutarán de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad tanto en su acceso, almacenamiento como transporte, así como de la necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad, todo ello de conformidad con el apartado I.13.B).

Se verificará regularmente que la información respaldada está correctamente dispuesta para ser recuperada en caso de necesidad, para lo cual se dispondrá de un procedimiento para la realización de pruebas de restauración del backup, que indique quién debe hacerlo y la frecuencia; manteniendo los requisitos de seguridad establecidos para la información original restaurada. El plan de pruebas de respaldo cubrirá, a lo largo del tiempo, todos los ámbitos de los que se realizan backups.

Se dispondrá igualmente de un procedimiento para la solicitud de recuperación de un backup, la identificación del responsable de la información y su autorización por escrito.

Las copias de respaldo se conservarán en lugares lo suficientemente independientes de la ubicación normal de la información en explotación como para que los incidentes previstos en el análisis de riesgos no se den simultáneamente en ambos lugares y que permita cumplir con el plan de continuidad establecido.

I.15 CONTINUIDAD DE LA ACTIVIDAD

El adjudicatario garantizará la existencia y disponibilidad de medios alternativos (instalaciones alternativas, comunicaciones alternativas, equipamiento alternativo, personal alternativo, etc) para poder seguir manteniendo los servicios prestados en idénticas condiciones en caso de que los medios habituales no estén disponibles por cualquier causa. Los medios alternativas disfrutarán de las mismas garantías técnicas

y de seguridad que los medios habituales. El adjudicatario presentará a la Diputación de Valencia una planificación de los citados medios alternativos.

El adjudicatario elaborará un plan de continuidad que establecerá las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará su revisión periódica o actualización tras cambios en los sistemas, los servicios y su calidad. Los niveles de disponibilidad y los tiempos de recuperación en la prestación de los servicios son los establecidos en los acuerdos de nivel de servicio del presente pliego técnico.

El adjudicatario deberá designar un comité de crisis que tome la decisión de aplicar el plan de continuidad tras analizar el desastre y evaluar las consecuencias, encargándose de la comunicación con las partes afectadas en caso de crisis y llevando a cabo las actuaciones para reconstruir el sistema de información (recuperación del desastre)

El citado plan de continuidad contendrá, como mínimo, los siguientes aspectos:

• la Identificación de funciones, responsabilidades y actividades a realizar.

• la identificación de los medios alternativos que serán necesarios para poder seguir prestando los servicios (instalaciones alternativas, comunicaciones alternativas, equipamiento alternativo, personal alternativo, etc) y la recuperación de la información con una antigüedad no superior a un tope determinado a la luz del análisis de impacto.

• la planificación de la formación específica que las personas afectadas por el plan recibirán.

I.16 AUDITORIA DE LA SEGURIDAD

El adjudicatario vendrá obligado a realizar una auditoría de seguridad cuyo objeto será el diagnostico del cumplimiento de todas las condiciones de seguridad que debe cumplimentar el adjudicatario. El objetivo final de la auditoría es sustentar la confianza que merece el sistema auditado en materia de seguridad; es decir, calibrar su capacidad para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida, habida cuenta de que es la Diputación de Valencia, en última instancia, quien resulta responsable de todos los requisitos de seguridad del sistema.

La citada auditoría se ceñirá a lo indicado en el apartado 5.3.2.3 del presente Pliego técnico en lo referente al equipo auditor, metodología, contenido y procedimiento para

el traslado del informe de auditoría, propuesta de acciones planificadas para, en su caso, la subsanación de deficiencias, y conformidad por la Diputación de Valencia.

La auditoría de seguridad deberá llevarse a cabo:

• de forma regular, cada dos años.

• con carácter extraordinario, siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas.

La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años establecidos para la realización de la siguiente auditoría regular.

I.17 PROTECCIÓN DE LAS APLICACIONES INFORMÁTICAS

El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción (p.ej: no hay compiladores en los sistemas de producción).

Deberá aplicarse una metodología de desarrollo reconocida, la cual:

- tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
- trate específicamente los datos usados en pruebas.
- permita la inspección del código fuente.

Deberán formar parte integral del diseño del sistema los mecanismos de identificación y autenticación, los mecanismos de la información tratada y la generación y tratamiento de pistas de auditoría.

Las pruebas anteriores a la implantación o modificación del sistema de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente. El adjudicatario dispondrá de un plan de pruebas para comprobar el correcto funcionamiento de la aplicación antes de pasar a producción. A través de dichas pruebas se comprobará que se cumplen los criterios de aceptación en materia de seguridad y que no se deteriora la seguridad de otros componentes del servicio.

Las pruebas se realizarán en un entorno aislado (pre-producción). Las pruebas de aceptación tampoco se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Previamente a la entrada en servicio se realizará un análisis de vulnerabilidades y se resolverán las posibles vulnerabilidades detectadas, así como una prueba de penetración.

La entrada en servicio de las aplicaciones requerirá la autorización de la Unidad de Gestión y Operación, una vez acreditadas todas las garantías previstas en el presente apartado.

ANEXO II

MEDIDAS DE SEGURIDAD DE LOS DATOS DE CARÁCTER PERSONAL

II.1 DOCUMENTO DE SEGURIDAD

El adjudicatario dispondrá de un documento de seguridad que deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado, con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable (Diputación de Valencia) y del período de vigencia del encargo.

Esta obligación del adjudicatario no supone delegación de la Diputación de Valencia para la llevanza del documento de seguridad de ésta en relación con los ficheros y tratamientos afectados por la prestación del servicio.

El documento de seguridad del adjudicatario se ajustará en su contenido y previsiones a lo dispuesto en el artículo 88 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RDLOPD), en la medida de la prestación del servicio.

II.2 RESPONSABLE DE SEGURIDAD

Se aplicará lo dispuesto en el artículo 95 RDLOPD. El responsable de seguridad designado por el adjudicatario podrá ser el mismo que el citado en el apartado “I.6 Competencias de seguridad” del ANEXO I.

II.3 ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES

Se aplicará lo dispuesto en el artículo 85 RDLOPD.

II.4 RÉGIMEN DE TRABAJO FUERA DE LOS LOCALES DEL ENCARGADO DEL TRATAMIENTO

Se aplicará lo dispuesto en el artículo 86 RDLOPD.

II.5 FICHEROS TEMPORALES O COPIAS DE TRABAJO DE DOCUMENTOS

Se aplicará lo dispuesto en el artículo 87 RDLOPD.

II.6 FUNCIONES Y OBLIGACIONES DEL PERSONAL

Se aplicará lo dispuesto en el artículo 89 RDLOPD. Esta obligación del adjudicatario se integrará en las medidas recogidas en el apartado “I.5 Gestión del Personal” del ANEXO I y se complementará con lo establecido en los apartados “I.1 Normativa de Seguridad” y “I.2 Procedimientos de Seguridad” del citado ANEXO.

II.7 REGISTRO DE INCIDENCIAS

Se aplicará lo dispuesto en los artículos 90 y 100 RDLOPD. Esta obligación del adjudicatario se integrará en las medidas recogidas en el apartado "I.12 Gestión de Incidencias" del ANEXO I.

II.8 CONTROL DE ACCESOS

Se aplicará lo dispuesto en el artículo 91 RDLOPD.

II.9 GESTIÓN DE SOPORTES Y DOCUMENTOS

Se aplicará lo dispuesto en los artículos 92 y 97 RDLOPD. Esta obligación del adjudicatario se integrará en las medidas recogidas en el apartado "I.13 Protección de la información almacenada y en tránsito" del ANEXO I.

II.10 IDENTIFICACIÓN Y AUTENTICACIÓN

Se aplicará lo dispuesto en los artículos 93 Y 98 RDLOPD.

II.11 COPIAS DE RESPALDO Y RECUPERACIÓN

Se aplicará lo dispuesto en el artículo 94 RDLOPD.

II.12 AUDITORÍA

Se aplicará lo dispuesto en el artículo 96 RDLOPD. Esta obligación del adjudicatario se integrará en las medidas recogidas en el apartado "I.16 Auditoría de la Seguridad" del ANEXO I.

II.13 CONTROL DE ACCESO FÍSICO

Se aplicará lo dispuesto en el artículo 99 RDLOPD.

SALVADOR FRANCISCO|
DEUSA|IBANCO
2013.10.10 11:23:16
+02'00'

Salvador Deusa Ibanco

Jefe de Evaluación y Planificación