

**OBRA SOCIAL DEL PERSONAL DE LA SEGURIDAD PÚBLICA DE LA CIUDAD AUTÓNOMA DE  
BUENOS AIRES - O.S.PE.SE.**

*“Licitación Pública para la contratación de Servicio de Diseño, Desarrollo e Implementación del  
Ecosistema Digital Unificado y Plataforma de Gestión”*

**PLIEGO DE ESPECIFICACIONES TÉCNICAS**

Los oferentes deberán elaborar sus propuestas contemplando que a partir del presente procedimiento de contratación se solicita el servicio de horas de desarrollo de software para aplicativos de los sistemas de la Obra Social del Personal de Seguridad Pública de la Ciudad Autónoma de Buenos Aires (en adelante “OSPESE”) bajo la modalidad Software Factory, conteniendo todos los servicios necesarios para convertir un requerimiento en una pieza de desarrollo.

El dimensionamiento de esta licitación, expresado en horas de servicio, está calculado con relación a los consumos esperados desde las distintas áreas de OSPESE. La cantidad de horas es estimada y puede modificarse a causa de las variables que modifiquen la gestión de la demanda de las dependencias de la Obra Social.

Las funcionalidades que se incluyen dentro de las versiones de piezas de desarrollo deberán cumplir con el detalle de las historias de usuario.

Los entregables mensuales con la rendición de horas consumidas deberán presentarse de acuerdo con los consumos de horas y se certificarán de acuerdo a los esfuerzos previamente acordados.

## 1. RESUMEN DEL PRODUCTO

El sistema Padrón OSPESE constituye el núcleo del ecosistema digital de la Obra Social, consolidándose como una plataforma web integral orientada a la gestión unificada, confiable y trazable del padrón de afiliados. La solución centraliza la información de titulares y grupos familiares, digitaliza los procesos administrativos críticos y establece reglas de negocio robustas que garantizan la coherencia operativa y la integridad del dato a lo largo de todo su ciclo de vida

El producto fue diseñado y construido bajo un enfoque modular, escalable e interoperable, permitiendo que la gestión diaria del padrón —altas, bajas, modificaciones, transferencias, cambios de titularidad y programaciones futuras— se realice de manera controlada, auditada y alineada a la normativa vigente. Cada acción ejecutada dentro del sistema queda registrada mediante mecanismos de trazabilidad y auditoría, asegurando transparencia, responsabilidad operativa y capacidad de reconstrucción histórica ante inspecciones o análisis posteriores.

La plataforma no se limita a la administración estática de datos, sino que incorpora una lógica temporal avanzada, capaz de manejar estados presentes, pasados y futuros de los afiliados, incluyendo la programación de altas y bajas tanto de titulares como de familiares, con validaciones automáticas que preservan la consistencia del grupo familiar y evitan escenarios inválidos. Este enfoque permite reflejar con precisión situaciones reales del padrón, anticipando cambios y reduciendo la intervención manual correctiva

En términos de interoperabilidad, el sistema actúa como un orquestador de información entre OSPESE y actores externos clave. Integra procesos de intercambio con OSDE mediante la generación automática de novedades diarias y reportes estructurados, asegurando la sincronización de altas, bajas, cambios de cobertura y modificaciones relevantes del padrón. Asimismo, incorpora la integración con información del Ministerio, permitiendo la carga, procesamiento y validación de informes mensuales de aportes y situaciones de revista, transformando información externa en novedades operativas accionables dentro del sistema

A partir de esta integración, el producto incorpora un módulo de gestión de novedades, que presenta a los operadores y administradores las acciones sugeridas ante cambios detectados (licencias, vencimientos, falta de aportes, modificaciones de cobertura), habilitando su confirmación o descarte con impacto directo y controlado sobre el padrón. Este mecanismo reduce la discrecionalidad, estandariza criterios de decisión y fortalece el gobierno del dato.

Complementariamente, el sistema ofrece capacidades de análisis y visibilidad operativa, a través de métricas globales del padrón, reportes exportables y vistas consolidadas que facilitan la toma de decisiones tácticas y estratégicas. La posibilidad de realizar operaciones masivas, con validaciones previas y control de ejecución futura, refuerza la eficiencia operativa sin resignar control ni trazabilidad.

En conjunto, el Padrón OSPESE no se presenta como un sistema aislado, sino como una plataforma central de interoperabilidad y gestión, diseñada para sostener el crecimiento del ecosistema digital de la Obra Social. Su arquitectura y funcionalidades permiten la convivencia de procesos administrativos, atención al afiliado, intercambio institucional y análisis de datos, consolidando una

fuerza única de verdad, confiable y auditable, sobre la cual se apoyan las operaciones presentes y futuras de la organización.

El producto solicitado se estructura en CUATRO (4) módulos lógicos. Las siguientes especificaciones son excluyentes; el incumplimiento de cualquiera de ellas será causal de desestimación técnica, dado el carácter crítico de los datos de salud administrados.

#### A. Módulo de Autogestión

Este componente deberá operar como una plataforma de "Alta Seguridad y Autogestión", garantizando la identidad digital del afiliado.

- **Identidad y Acceso Robusto:** El sistema deberá implementar mecanismos de autenticación segura (OIDC/OAuth2) y validación de identidad contra el Padrón. No se aceptarán soluciones que no garanticen la encriptación de credenciales en tránsito y reposo.
- **Gestión Documental con Validación de Integridad:** La funcionalidad de carga de trámites (Partidas, DNI, CUD) deberá incluir repositorios seguros y pistas de auditoría que registren quién subió el documento y cuándo, para evitar fraudes documentales. El sistema debe asegurar que la documentación impacte en el Core Administrativo sin intervención humana innecesaria, pero manteniendo un log de transacciones inalterable.
- **Seguimiento de trámites:** Permitirá al afiliado visualizar de manera clara y en tiempo casi real el estado de todas las gestiones iniciadas a través del Portal de Afiliados o de otros canales digitales. Cada trámite contará con un identificador único, fecha de inicio, estado actual, así como un historial completo de eventos, cambios de estado y mensajes u observaciones relevantes asociados a la gestión. La información presentada deberá reflejar fielmente el estado real de los trámites en los sistemas internos de la organización (CRM y Core Administrativo), reduciendo la necesidad de consultas telefónicas o presenciales y aportando un mayor nivel de transparencia operativa y previsibilidad al proceso para el afiliado.
- **Portal de Afiliados:** El Portal de Afiliados funcionará como el canal digital unificado de interacción entre el afiliado y O.S.Pe.Se., operando bajo un esquema de Single Sign-On (SSO) que permita acceder, desde una única identidad, a todas las funcionalidades y servicios disponibles dentro del ecosistema.

El portal deberá estar disponible en versión web y móvil, y su arquitectura estará diseñada para interoperar con el sistema "Padrón OSPESE" y de terceros, permitiendo al afiliado resolver sus gestiones sin necesidad de navegar múltiples plataformas. A continuación, se listan las capacidades principales del Portal:

- Acceso centralizado a información personal y de grupo familiar.
- Consulta de estado de afiliación, cobertura y beneficios.
- Acceso a servicios integrados del ecosistema.
- Canal único de comunicación y notificaciones relevantes para el afiliado.

Se busca consolidar una experiencia digital continua, reduciendo la fragmentación de sistemas y mejorando la percepción de servicio.

- **Asistente Virtual (AI) Integrado:** El Agente Virtual deberá contar con una arquitectura de NLP capaz de interpretar intenciones y mantener el contexto de la conversación. Es mandatorio que el bot pueda discriminar consultas informativas de gestiones transaccionales, derivando estas últimas al flujo humano con todo el historial de interacción persistido.

## B. Módulo de Gestión Operativa

Este núcleo deberá funcionar como un sistema de misión crítica, soportando alta concurrencia y asegurando la integridad referencial de los datos bajo reglas de negocio estrictas.

- **Motor de Reglas de Negocio Configurable:** El sistema deberá disponer de un motor de reglas, que permita parametrizar validaciones (ej. vigencia de CUD, topes de edad, carencias) sin necesidad de nuevos despliegues de software. Esto es obligatorio para garantizar la mantenibilidad evolutiva.
- **Seguridad Granular:** La gestión de usuarios deberá extender la implementación del esquema de permisos granulares actual. El sistema debe impedir por diseño que un usuario visualice o modifique datos sensibles que no correspondan a su rol específico, bloqueando filtraciones de datos internas.
- **CRM:** Constituirá el eje operativo de la relación entre la Obra Social y sus afiliados, centralizando todas las interacciones, reclamos y trámites en un entorno único y controlado. El sistema deberá reemplazar los mecanismos informales de gestión por un modelo transaccional basado en casos, donde cada interacción se materializa en un ticket con trazabilidad completa desde su creación hasta su resolución definitiva. Dicho módulo deberá soportar una bandeja de entrada unificada y omnicanal, integrando consultas provenientes de distintos puntos de contacto en una única interfaz operativa. Asimismo, incorporará flujos de trabajo inter-áreas que automaticen la derivación de casos entre sectores internos, garantizando la continuidad del trámite, la conservación del historial completo de acciones y la eliminación de estados indefinidos o sin responsable asignado. Complementariamente, el CRM deberá incluir capacidades de gestión de campañas y comunicaciones masivas segmentadas, permitiendo la ejecución de acciones informativas o preventivas dirigidas a grupos específicos de afiliados, así como mecanismos de medición de calidad de servicio mediante encuestas de satisfacción automatizadas al cierre de casos o campañas, aportando indicadores objetivos para la mejora continua de la atención.

## C. Módulo de Integración

Este componente deberá proveer una capa de abstracción (Middleware) robusta para desacoplar el Core de los sistemas externos, garantizando la estabilidad operativa ante fallos de terceros.

- **Orquestación y Manejo de Fallos:** El módulo deberá incluir mecanismos de "encolamiento" y reintentos automáticos (Retry patterns). Si un ente externo (ej. Ministerio) no responde, el sistema no deberá colapsar ni perder el dato, sino encolarlo y procesarlo asincrónicamente.
- **Conectividad Agnóstica:** Respecto a las integraciones con otros servicios (ej. OSDE), el ADJUDICATARIO deberá entregar los conectores de software (API Clients) desarrollados y

documentados según los estándares de mercado (REST/SOAP), independientemente de la disponibilidad momentánea de la contraparte. El sistema debe quedar listo técnicamente para "encender" la conexión mediante configuración.

- **Conciliación Automática de Padrones:** El sistema deberá ejecutar procesos batch automatizados para cruzar masivamente la base local contra el Ministerio, reportando discrepancias a nivel de campo para depuración proactiva.

#### D. Módulo de Inteligencia

Este módulo deberá transformar los datos en activos estratégicos, bajo estricto cumplimiento del marco legal argentino vigente.

- **Protección de Datos Personales:** En cumplimiento de la Ley 25.326, el módulo de explotación de datos deberá aplicar técnicas de anonimización y disociación irreversible de datos sensibles cuando se utilicen para análisis estadísticos o poblacionales. El ADJUDICATARIO deberá garantizar por arquitectura que ningún dato médico sensible pueda ser asociado a la identidad del afiliado en las vistas analíticas generales.
- **Analítica Predictiva y Financiera:** Los tableros de control deberán permitir el "Drill-down" (desglose) desde el indicador macro hasta el detalle del registro que lo compone, para facilitar auditorías profundas de facturación y aportes.
- **Perfilado de Riesgo:** El sistema deberá ser capaz de categorizar la población en base a reglas de consumo prestacional para identificar cohortes de riesgo (Crónicos, Discapacidad), proveyendo insumos para la gestión médica sin vulnerar la privacidad del paciente.
- **Plan de resolución de contingencias:** Se debe definir y presentar un plan de acción ante contingencias del sistema.

## 2. TECNOLOGÍAS UTILIZADAS

El ecosistema digital de OSPES se apoya en un stack tecnológico basado en servicios administrados y herramientas ampliamente adoptadas en la industria, orientadas a garantizar escalabilidad, seguridad, mantenibilidad y eficiencia operativa.

Las tecnologías listadas a continuación constituyen el stack de referencia obligatorio para el desarrollo de nuevas versiones y módulos, debiendo ser utilizadas cuando resulte técnicamente pertinente según el tipo de componente a implementar (backend, frontend, procesamiento asincrónico, reporting, infraestructura).

La arquitectura admite distintos patrones de implementación (serverless, contenedores, procesos orquestados), siempre dentro del marco tecnológico definido, asegurando compatibilidad, performance y coherencia con el ecosistema existente.

#### Infraestructura Cloud y Servicios Administrados (AWS)

- AWS Lambda
- AWS Fargate
- AWS EventBridge / Scheduler

- AWS Step Functions
- AWS RDS
- AWS S3
- AWS SES
- AWS VPC
- AWS CloudWatch

#### Backend

- NestJS

#### Frontend

- Vite

#### Base de Datos

- PostgreSQL

#### DevOps, Infraestructura como Código y Control de Versiones

- Docker
- Terraform
- GitHub

#### Analítica, Reportes y Business Intelligence

- Metabase

#### Seguridad, Autenticación y Conectividad

- AWS Cognito
- Tailscale VPN

### 3. EQUIPO DE TRABAJO

El Adjudicatario deberá conformar un equipo de trabajo con experiencia comprobable en el stack tecnológico solicitado. Los roles mínimos requeridos son:

- **Director Médico Digital:** Profesional médico o de ciencias de la salud con experiencia comprobable en gestión hospitalaria y transformación digital. Responsable de asegurar alineamiento clínico, cumplimiento normativo (Ley 26.529, estándares del Ministerio de Salud), interoperabilidad y seguridad del dato asistencial. Ideal contar con posgrados en salud digital o certificaciones equivalentes.
- **PMO / Project Manager Senior & Tech Delivery Lead:** Responsable integral de planificación, PMBOK/Agile, control de riesgos, matriz RACI y gestión de costos. Lidera

roadmap, hitos y dependencias. Coordina equipos técnicos y clínicos. Experiencia comprobable en ejecución de proyectos complejos.

- **Ingeniero en Procesos Sanitarios y Gobernanza Clínica:** Responsable de relevar, rediseñar y optimizar procesos asistenciales y administrativos mediante metodologías Lean Healthcare, BPMN y modelos internacionales (HIMSS, JCI, ISO 9001). Define mapa de procesos, riesgos operativos e indicadores de desempeño clínico-administrativos. Se valoran las certificaciones HIMSS.
- **Ingeniero de Requerimientos / Product Specialist:** Traductor funcional-técnico entre las necesidades del negocio sanitario y las capacidades tecnológicas. Define requerimientos, historias de usuario, procesos target y criterios de aceptación.
- **Diseñador UX / UI:** Responsable de diseñar interfaces seguras, eficientes y centradas en el usuario. Diseño, ejecución y evaluación de test de usabilidad.
- **Arquitecto Cloud Senior:** Diseño de arquitectura de referencia de alta criticidad con alta disponibilidad, IaC y observabilidad. Especialista en AWS (LandingZone, WAF, EKS, S3, CloudTrail, CloudWatch), Terraform, seguridad infra-as-code y segregación de ambientes para sistemas de salud.
- **Tech Lead Backend Senior:** Arquitectura de microservicios, NestJS, Node, OpenAPI. Define patrones de diseño, performance y resiliencia.
- **Ingeniero Frontend:** Typescript, React/Vite, Chakra UI y test automáticos.
- **Ingeniero Backend:** Dominio avanzado de Typescript, NestJS, pruebas contractuales, CI/CD, y patrones de integración para sistemas satélites.
- **Arquitecto y Analista de Datos Senior / BI Lead:** Diseño de modelos para análisis de datos, lakehouse, gobierno de datos, interoperabilidad semántica y calidad.
- **Dev Sec Ops:** Diseño e implementación de pipeline seguro CI/CD, gestión de secretos, automatización, monitoreo y cumplimiento normativo: ISO 27001, RGPD. Responsable de auditorías de seguridad, vulnerabilidades y trazabilidad end-to-end.
- **QA Automation Lead:** Pruebas funcionales y no funcionales, automatización, validación de performance y stress para sistemas de misión crítica. Define estrategia de testing y validaciones de interoperabilidad.

#### 4. METODOLOGÍA DE TRABAJO

OSPESE notificará al ADJUDICATARIO a través de la emisión de Solicitudes de Provisión de Servicios (SPR) los requerimientos de servicios de desarrollo.

El ADJUDICATARIO deberá acordar, antes de iniciar el desarrollo, con OSPESE la especificación funcional, los esfuerzos a insumir, y la documentación de las entregas parciales y finales.

El ADJUDICATARIO generará una propuesta técnica dentro de los SIETE (7) días hábiles desde la solicitud de alguna pieza de desarrollo. En esta instancia la propuesta deberá incluir el orden de magnitud en tiempos y esfuerzos y se deberá acordar con el OSPESE los acuerdos específicos técnicos para cada desarrollo solicitado.

En los casos que el requerimiento no posea definición de la arquitectura del sistema, el ADJUDICATARIO deberá presentar la propuesta de arquitectura, que deberá ser validada y aceptada por OSPESE, incluyendo todas las integraciones con otros sistemas. Se planificarán y acordarán:

1. El número de sprints de dos o tres semanas, así como el alcance y entregable de cada uno de ellos.
2. La arquitectura del sistema validada y aceptada por OSPESE, incluyendo todas las integraciones con otros sistemas y cómo resolverlas.
3. Las funcionalidades clasificadas y priorizadas del producto con todos los elementos a implementar.

Luego de alcanzar estos acuerdos se comenzarán los servicios de desarrollo iniciando el sprint 1. Una vez definido el sprint, antes de comenzar el desarrollo de cada historia, el ADJUDICATARIO deberá especificar las tareas que serán desempeñadas para su resolución.

Esto permitirá entender la solución ofrecida y, además, mantener un registro de la operatoria de los desarrolladores. A cada historia se le deberá cargar una estimación en horas para su resolución completa. Esto permitirá la estimación de la cantidad de horas de desarrollo que serán dedicadas a cada una de las historias.

Una vez definidas las tareas, junto con sus estimaciones, el ADJUDICATARIO será responsable de ir cambiando los estados de estas a: ANÁLISIS, EN PROCESO, y RESUELTA, según corresponda. El ADJUDICATARIO además deberá cargar el consumo de horas por sprint, al finalizar el mismo.

Ningún miembro del equipo puede cambiar el estado de la historia a: RESUELTO. Sólo las tareas que la componen pueden cambiar a este estado. El cambio de estado a RESUELTO de la historia se realiza durante la etapa de UAT (Prueba de aceptación de usuario).

El ADJUDICATARIO, dispondrá de un entorno de trabajo de desarrollo y deberá de implementar las soluciones desarrolladas en ese entorno, previo a cada pedido de implementación en QA.

Para la implementación en QA deberá crear un ticket de deploy, indicando detalladamente el contenido del paquete a ser deployado, explicando tecnología, archivos de configuración, variables de configuraciones y todas las particularidades que se consideren para la implementación.

Las horas correspondientes al inciso 1.a serán ejecutadas conforme a los módulos, alcances y entregables previamente definidos en el esquema contractual, considerándose automáticamente aceptadas en la medida en que se cumpla con dicho alcance acordado. Por su parte, las horas correspondientes al inciso 1.b se consumirán únicamente a requerimiento expreso de la Obra Social, debiendo cada solicitud ser previamente validada y aprobada por las partes en cuanto a alcance y estimación. Considerándose aceptadas, serán ejecutadas y reportadas según el mecanismo de seguimiento acordado, sin que ello implique una modificación automática del alcance contractual original.



## 5. CALIDAD DEL CÓDIGO

OSPESE evaluará el código presentando, siendo su aprobación necesaria para su aceptación. El código debe cumplir con los siguientes requisitos técnicos:

- A. Test unitario automático, con un mínimo de 80% de cobertura, implementado con las herramientas de test unitarios adecuadas al lenguaje de programación (Junit, phpUnit, Jasmine, Mockito)
- B. No debe tener vulnerabilidades de seguridad, ni bugs mayores, críticos o bloqueantes.
- C. Debe evitar la duplicidad de código.
- D. Código comentando:
  - a. Nombre de la clase se debe indicar el Nombre de la clase, descripción general, número de versión, nombre de autores.
  - b. Documentación de cada constructor o método (especialmente los públicos) incluyendo: nombre del constructor o método, tipo de retorno, nombres y tipos de parámetros si los hay, descripción general, descripción de parámetros (si los hay) descripción del valor que devuelve.
  - c. Utilización de Swagger para la documentación de APIS.
- E. Utilización de patrones de diseño de software como patrones creacionales, estructurales y de comportamiento.
- F. Las bases de datos deben ser versionadas utilizando herramientas de migración.

OSPESE podrá utilizar diferentes herramientas para análisis del código como SonarQube y procesos como codeReview para validar la calidad del código presentando.

## 6. ENTREGABLES

Quien resulte ADJUDICATARIO deberá entregar las piezas de desarrollo que incluyan todos los servicios necesarios para que el requerimiento que solicite OSPESE se convierta en un desarrollo entregado por el ADJUDICATARIO. Los servicios contenidos en el proceso de desarrollo conforman una unidad de valor que es la hora de desarrollo.

La documentación mínima y obligatoria que el ADJUDICATARIO debe presentar en forma MENSUAL, en caso de consumo de horas, es un informe conteniendo:

- Datos de la Solicitud de Provisión de Servicios (SPR) a la que referencian las horas de desarrollo insumidas a certificar.
- Cantidad de horas de desarrollo a certificar. Estas deberán estar discriminadas por proyecto con el detalle de los esfuerzos estimados en la orden de magnitud acordada.

Adicionalmente toda la documentación que contenga evidencia del Servicio debe ser entregada a OSPESE como parte de este contrato.

En cada entrega puede variar la documentación según los servicios de desarrollo solicitados con el período informado y queda a criterio de OSPESE la validación de esta.

## 7. CRITERIOS DE ACEPTACIÓN DE PIEZAS DE DESARROLLO

OSPESE tendrá quince (15) días hábiles para verificar el cumplimiento de la calidad del producto de software entregado. Este plazo de verificación vale para todas las piezas de desarrollo requeridos, salvo para el Código.

En todos los casos el ADJUDICATARIO es responsable de brindar el soporte necesario para la instalación de la totalidad del software desarrollado, y de la totalidad de los procedimientos necesarios para su funcionamiento y puesta en marcha.

En cuanto a las condiciones generales de piezas de desarrollo previstos en el presente Pliego, se definen las siguientes pautas de trabajo:

- Toda observación a piezas de desarrollo derivará en, por lo menos, una reunión con el ADJUDICATARIO para comunicar los motivos de la observación y definirá los períodos de subsanación. En dicha reunión, OSPESE expondrá y explicará los motivos de la observación. OSPESE deberá levantar las observaciones dentro del período de subsanación establecido.
- Toda Revisión – Subsanación dispondrá de las iteraciones necesarias hasta la aceptación definitiva de la misma.
- Si el resultado de la revisión es satisfactorio, OSPESE otorgará la aceptación, de lo contrario, comunicará las razones de la no aceptación.

Una vez que OSPESE considere que el producto es válido (por cumplir con los estándares de calidad, ser completo y correcto, tanto desde el punto de vista formal como funcional), emitirá la aprobación del mismo.

Para las piezas de Código fuente, el ADJUDICATARIO deberá realizar sus pruebas de desarrollo y entregar el producto con calidad de aceptación. Esta calidad de aceptación se fija en base al porcentaje de errores u omisiones detectados de cada tipo de severidad.

Se define los tipos de severidad como:

- **Crítica:** Cuando los usuarios no pueden utilizar las funcionalidades principales del sistema. Cuando no es posible realizar algún trabajo productivo. Cuando no se puede prestar el servicio a los clientes.
- **Mayor:** Cuando el sistema está operando, pero con restricciones. Existe impacto en la prestación del servicio a los clientes. Existe impacto para los usuarios.

- **Menor:** Cuando los usuarios no pueden utilizar las funcionalidades secundarias del sistema. Cuando no se encuentran disponibles algunas funciones o componentes del Sistema, que generan un impacto mínimo para los clientes y para los usuarios. Cuando las limitaciones no son críticas para la operación. El impacto no genera un riesgo considerable, pero es necesario resolverlo.

Baja/Cosmética: El error se refiere a un mal funcionamiento de la interfaz de usuario, que no impide la correcta ejecución del sistema.

Por lo que, cada pieza de Código fuente será aceptado por OSPESE si presenta:

- A. 0% de errores de severidad crítica y mayor
- B. 30% de errores de severidad menor y
- C. 50% de errores de severidad baja.

Además de lo mencionado anteriormente, OSPESE se reserva el derecho de solicitar la corrección de incidencias particulares que considere de prioridad máxima independientemente de su severidad

## **8. CONDICIONES DE TRABAJO**

### **8.1. MEDIOS DE COMUNICACIÓN**

El ADJUDICATARIO deberá suministrar a OSPESE los datos de los recursos que cumplan el rol de referentes técnicos o líderes del servicio, con números de teléfonos celulares y mails.

En todos los casos se deberá establecer de común acuerdo entre el OSPESE y el ADJUDICATARIO los medios de comunicación que garanticen la completa y correcta prestación de los servicios en el nivel de calidad requerido en el Pliego de Bases y Condiciones Particulares y en el presente Pliego de Especificaciones Técnicas.

En ningún caso se reconocerán trabajos solicitados por medios de comunicación informales u Órdenes de Servicio / Órdenes de Trabajo cursadas de manera informal por parte de Usuarios involucrados en la Solución y/o Proyecto o por cualquier participante que no haya sido expresamente autorizado por OSPESE.

### **8.2. ENTORNO DE TRABAJO**

A los fines del desarrollo de las actividades previstas en el presente Pliego de Especificaciones Técnicas y el Pliego de Bases y Condiciones Particulares, el ADJUDICATARIO deberá contar con una oficina permanente en la ciudad de Buenos Aires, durante todo el tiempo de su ejecución.

Independientemente del lugar físico donde se efectúen las actividades, OSPESE dispondrá de un ambiente de desarrollo, prueba, homologación y producción los que se encuentran instalados y serán configurados en base a las premisas de operatividad necesarias que serán suministradas por el ADJUDICATARIO. Durante todo el período de prestación de los servicios y/o desarrollo de

Proyectos, OSPESPE tendrá acceso a versiones parciales de cualquier pieza de desarrollo, máximo en forma SEMANAL previo requerimiento de la misma.

### **8.3. HERRAMIENTAS**

El ADJUDICATARIO deberá poseer un correcto licenciamiento de las herramientas que utilice en los desarrollos, siendo su exclusiva responsabilidad. No obstante, el empleo de copias ilegales y/o de programas inconsistentes con las políticas de seguridad de OSPESPE será considerado falta grave y podrá dar lugar a la rescisión del contrato por culpa del adjudicatario, sin perjuicio de las acciones penales y/o civiles que pudiesen corresponder.

### **8.4. TRASLADOS Y GASTOS ASOCIADOS**

Todos los traslados del personal afectado del ADJUDICATARIO, así como los Tiempos de Traslado involucrados hacia o desde locaciones de OSPESPE o donde esta dispusiere, son a exclusivo cargo y expensa del ADJUDICATARIO no pudiendo exigirse reembolso alguno a OSPESPE.

NO VÁLIDO PARA INCLUIR EN LA OFERTA