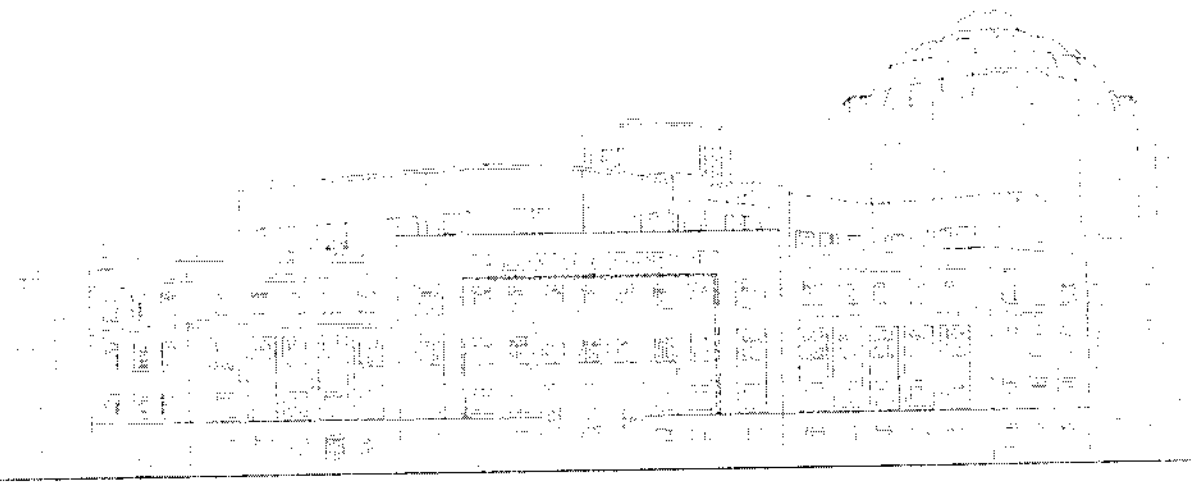
Plataforma Digital Transaccional

Licenciamiento para Software de Service Managment



Contenido

1. Objetivo

El objeto del presente llamado, es la contratación de un sistema de gestión de incidentes de IT en la modalidad SaaS (Software as a Servicie) para poder dar soporte a los organismos de estado, comercios adheridos y oficinas de atención al usuario final, que utilicen la Plataforma Digital Transaccional (PDT) que Sociedad del Estado Casa de Moneda en adelante ORGANISMO CONTRATANTE, implemento en el marco de la conformación de un ecosistema digital transaccional y financiero inclusivo, donde puedan convivir Usuarios bancarios y extra bancarios, conectándose a los diferentes medios de pagos, servicios transaccionales, bancos y servicios financieros, procesadores, referentes de la economía social, redes de puntos físicos y demás actuales y potenciales integrantes del nombrado ecosistema, utilizando una plataforma común.

2. Necesidades

Se requiere adquirir licenciamiento de uso de la plataforma para 50 agentes que brindaran soporte a incidentes ocurridos y reportados en la plataforma PDT

3. Alcance

El sistema de gestión de incidentes (ITSM) deberá proporcionar una interfaz que permita la creación, categorización y gestión de incidentes que serán reportados por usuarios de la solución PDT.

A continuación, se detallan las funcionalidades que el sistema deberá soportar para el uso que se dará al mismo.

4. Funcionalidades del Sistema

4.1. Generalidades

- El mismo deberá soportar multicanalidad, los que significa que los incidentes se podrán reportar vía múltiples canales como ser:
  - web
  - Aplicación móvil
  - Correo electrónico
- Los incidentes reportados deberán ser unívocamente identificables y contar con un ID autogenerado por cada incidente nuevo.
- El sistema deberá proporcionar una interfaz de login/registro de nuevo usuario cliente.
- El sistema deberá proporciona una interfaz de modificación de perfil de usuario logueado, permitiendo seleccionar
  - Lenguaje
  - Cambio de contraseña
  - Cambio de correo electrónico
  - Zona horaria
- El sistema deberá permitir la vista de los incidentes reportados propios de un cliente y los pertenecientes a la compañía del cliente logueado.
- El sistema deberá desconectar una sesión de un cliente logueado luego de cierto tiempo de inactividad o luego de un determinado lapso de tiempo preconfigurado.
- El sistema debe proporcionar una interfaz de gestión Administrativa para la gestión de usuarios (clientes y agentes), estadísticas, configuración de niveles de servicio (SLA), canales de comunicación, integración con sistemas de terceros, configuración de colas de atención.

4.2. Agentes y Clientes

El sistema debe contemplar la capacidad de generar 2 tipos de usuarios diferentes:

- Agentes
- Clientes

Los agentes serán los responsables de recepcionar los incidentes creados por los clientes y dar tratamiento a los problemas reportados, permitiendo informar cada acción realizada para la resolución del incidente, dejando una bitácora de trabajo que puede ser consultada por otro agente o por el cliente que reporto el incidente.

Los clientes serán usuarios del sistema, que no pertenecen a la SECM pero que harán uso de la herramienta o aplicación que la PDT ofrece a estos donde podrán informar fallas experimentadas en el uso de las aplicaciones ofrecidas.

La plataforma deberá contar con un menú de gestión de usuarios donde se puedan definir los roles y permisos asociados a cada usuario o tipo de usuario.

Agentes:

- Creación de casos

- Gestión de incidentes creados por clientes
- Escalamientos internos
- Gestión de usuarios clientes
- Gestión de estadísticas

Clientes:

- Creación de Casos
- Cierre de Casos

4.3. Generación de Incidentes (Cliente)

El sistema deberá exponer una web con un formulario de ingreso de incidentes donde el cliente que reporte un nuevo incidente ingresará a siguiente información:

- Producto
- Criticidad
  - Critico
  - Mayor
  - Menor
  - Consulta
- Asunto
- Detalle
- Archivo Adjunto (opcional)

Una vez completado los campos se debe enviar el formulario seleccionando el botón enviar y el sistema retorna con el ID del caso creado.

El sistema debe proporcionar una vista agrupadora de casos abiertos y/o cerrados por cliente y/o empresa para que los clientes puedan gestionar múltiples incidentes.

El cliente podrá generar incidentes utilizando el envió de un correo electrónico a una determinada cuenta de correo, utilizando tags identificatorios en asunto o cuerpo de mensaje y el sistema en forma autónoma deberá poder registrar el incidente en el sistema de gestión, de la misma forma que lo realiza en el punto definido anteriormente
También se deberá poder interactuar via correo electrónico para realizar updates bidireccionales al incidente reportado.

4.4. Gestion de Incidentes (Agente)

Cada incidente reportado por un cliente, deberá ser gestionado por un agente de la SECM encargado de dar solución al mismo.

El sistema deberá proveer una interfaz de gestión de incidentes que contemple los siguientes campos que identifiquen al incidente:

- Fecha de alta de incidente
- Id de Incidente
- Cliente

- Empresa
- Descripción del caso
- Descarga de adjuntos al caso

Al seleccionar el incidente se tiene que presentar la pantalla de respuesta al mismo donde se deberá insertar:

- Estado del incidente:
  - En análisis
  - Resuelto
  - Pendiente de respuesta
  - Cerrado
- Cuadro de texto para agregar información sobre el tratamiento del mismo
- Insertar archivos adjuntos (opcional)

El agente deberá contar con una vista generalizada de incidentes de todos los clientes, donde podrá seleccionar cualquiera de estos y poder dar gestión sobre el mismo.

El agente podrá generar incidentes con la misma vista de cliente y podrá asignarlos a otro agente o a una cola de producto definida para que otro agente la gestione de esa cola.

4.5. Service Level Agreement

El sistema deberá permitir definir diferentes Service Level Agreement (SLA) según criticidad definida en el incidente reportados, para poder tomar acciones y escalamiento en caso de no cumplimiento de estos.

Se debe contar con un tablero donde se visualice la matriz de incidentes en tratamiento ordenados por prioridades o SLA con el tiempo de tratamiento que lleva cada incidente reportado

4.6. Estadísticas y Reportes

El sistema deberá proveer un gestor que permita generar estadísticas y reportes de tratamiento de incidencias en tiempo real o bajo demanda

Los reportes bajo demanda se podrán parametrizar con valores de entrada que deberán ser los siguientes y no son mandatorios el ingreso de todos los definidos:

- Cliente
- Empresa
- Fecha desde
- Fecha Hasta
- Estado del incidente
- Agente
- Tiempo de resolución del incidente
- Criticidad

El resultado de la consulta será un reporte exportable en archivo csv o pdf.

El sistema deberá contar con un tablero de visualización grafica en tiempo real de incidencias generadas, en tratamiento, con el SLA de cada una de las incidencias y el tiempo de creación.

4.7. Base de Conocimiento

El sistema debe tener la capacidad de almacenamiento para repositorio de información o base de conocimiento (KB).

La misma debe contemplar las siguientes capacidades:

- Creación de articulos
- Indexación y búsqueda por palabras claves
- Creación de árboles temáticos
- Capacidad de vincular incidentes con documentación

5. Disponibilidad del sistema

El sistema a adquirir se ejecuta bajo la modalidad SaaS, por lo que no requiere despliegue de software en infraestructura on premise.

El proveedor del servicio deberá garantizar una disponibilidad del sistema en un 99.99% al año.

En caso de requerir ejecución de ventanas de mantenimiento de sus sistemas, el proveedor deberá avisar con 7 días de anticipación de las tareas a realizar, para que desde el área que utilice la herramienta contratada, pueda comunicar a sus clientes de la indisponibilidad de la misma en la fecha definida para la ventana.

El proveedor deberá garantizar la disponibilidad y la integridad de todos los datos almacenados en sus sistemas mediante respaldos periódicos de la información allí almacenada.

6. Soporte ante fallas del sistema

El proveedor deberá proporcionar soporte a los incidentes que se reporten como fallas en el sistema, deberá proporcionar una web de ticketing para informar de los incidentes, correo electrónico o línea de atención telefónica.

El soporte deberá responder según un SLA definido dependiendo de la criticidad del problema reportado según la siguiente tabla (Los valores manifestados son tiempos máximos de resolución)

Tipo de Falla	Tiempo de Respuesta	Solución Temporal	Solución Definitiva
Falla Total	15 minutos (7x24)	4hs	3 días
Falla Mayor	30 minutos (7x24)	8hs	7 días
Falla Menor	1 dia laboral	2 días laborables	15 días

Se requiere contar con una matriz de escalamiento para escalar los incidentes en caso de que los tiempos de resolución descriptos en la tabla anterior excedan a los definidos.

En caso de incumplimiento de los SLA definidos (Falla Total, Falla Mayor o Falla Menor), se aplicará una penalización del 1% del valor a pagar al momento de realizar la renovación del licenciamiento adquirido.

7. Licenciamiento

El licenciamiento a adquirir se define según la siguiente tabla

Descripción del Licenciamiento de Software Necesario	
Nombre de la Empresa	Atlassian
Software	Jira Service Management
Forma de Licenciamiento	Usuarios
Cantidad de licencias	50 Agentes
Modalidad de Pago	Anual
Fecha de Inicio del Servicio	7/2021
Plazo de vigencia del Servicio	Anual

8. Consideraciones adicionales

El sistema será de utilización por parte de un organismo perteneciente al Gobierno Nacional Argentino y el proveedor del SaaS a contratar deberá garantizar los siguientes puntos:

- Que en el manejo de la seguridad de los datos y el cumplimiento de normativas y leyes vigentes existe una responsabilidad compartida por el organismo y el proveedor. Las dos partes deben tomar las precauciones, realizar los controles y demás cuidados de su área de influencia. (ej. el proveedor responsable por la infraestructura, plataforma y servicios administrados y el organismo responsable por la información y su tratamiento que se utiliza con el servicio SaaS).
- Debe cumplir con Programas de cumplimiento y Certificaciones por Terceros de ISO 27001/2
- Adherencia a ley Protección de Datos Personales Argentina y normativa relacionada.
- Garantía de Propiedad de los Datos.

9. Formas de cotización de licencias

Se requiere la cotización discriminada por tipo de licencia, indicando los diferentes componentes funcionales que incluye cada una.