

A. Desarrollo de software

I. El Ente Público: **Consejería Jurídica del Estado**

Introducción

En el marco de la implementación del nuevo Sistema de Justicia Penal, llevado a cabo en el año 2010, se adquirió e instaló un Sistema informático para la gestión y administración de los expedientes penales. Este sistema fue diseñado para facilitar la comunicación y el intercambio de información entre la anterior Procuraduría General de Justicia del Estado y la Defensoría Pública. Este sistema sigue operando de manera continua hasta la fecha.

Es importante destacar que la Defensoría Pública del Estado no tiene acceso al código fuente de este sistema, y que la base de datos está compartida con la Fiscalía General del Estado de Baja California. En atención a las mesas de trabajo realizadas con la participación de la Coordinación de Gabinete, la Secretaría de Hacienda, y los responsables del Sistema de Justicia Penal, se implementó el proyecto integral de "Audiencias Efectivas", cuyo objetivo es reducir el diferimiento de audiencias y asegurar la culminación de los procesos penales de una manera eficiente.

En tiempos recientes, se ha llevado a cabo una significativa inversión en la infraestructura tecnológica, lo que ha permitido una mejora sustancial en las capacidades operativas de la Defensoría Pública. Sin embargo, es importante señalar que el sistema actual encargado de gestionar los expedientes penales no responde completamente a las exigencias de comunicación interinstitucional con la Fiscalía General del Estado, la Comisión Estatal del Sistema Penitenciario y el Poder Judicial del Estado. Esto genera ciertos riesgos, limita la eficiencia y provoca el retraso de audiencias.

1. El objetivo del Software:

Ante la creciente demanda de modernización y eficiencia en los procesos de la Defensoría Pública, y con el objetivo de continuar fortaleciendo el proyecto transversal de "Audiencias Efectivas", resulta urgente la implementación de un nuevo sistema de información que permita asegurar un control riguroso y eficiente de la administración operativa en el ámbito penal.

Este sistema debe garantizar la gestión digitalizada de los expedientes, optimizando la carga administrativa mediante la automatización de procesos clave. Además, integrará de manera fluida los documentos audiovisuales correspondientes a las audiencias, contribuyendo a una reducción significativa en los tiempos de atención y mejora en la accesibilidad de la información. La implementación de esta herramienta no solo proporcionará agilidad y eficiencia operativa, sino que también garantizará una plataforma fácil de usar y accesible para los usuarios.

Asimismo, este nuevo sistema permitirá mejorar sustancialmente la eficiencia en el trabajo de los defensores públicos, disminuyendo sus cargas administrativas y facilitando la integración de los expedientes mediante flujos de trabajo más organizados, intuitivos y colaborativos. Incorporará de forma natural y segura el manejo de multimedia, permitiendo la visualización directa de fotografías, audios, videos y documentos, integrados en los expedientes electrónicos. Todo esto facilitará una administración ágil, clara y completa de la información, optimizando la toma de decisiones sin interrupciones, incluso cuando se requieran ajustes o mejoras al sistema.

Uno de los aspectos más relevantes del sistema será el fortalecimiento de la comunicación con los distintos operadores del sistema de justicia penal (Fiscalía General del Estado, el Poder Judicial y la Comisión Estatal del Sistema Penitenciario CESISPE), mediante interconexiones seguras que respeten los estándares de confidencialidad y permitan el intercambio ágil y continuo de información. Esta capacidad permitirá mantener operativas todas las funciones del sistema, incluso ante escenarios de alta demanda o modificaciones específicas, garantizando una colaboración más eficiente y disminuyendo los diferimientos de audiencias por falta de información oportuna.

El sistema será capaz de generar reportes ejecutivos, estadísticos y de carga de trabajo, lo que permitirá a los directivos y responsables del área contar con información clave para la administración, seguimiento y mejora continua de los procesos de defensa penal. Además, incluirá un módulo de archivo digital que integrará de forma fluida la nueva información generada de los expedientes, manteniéndolos actualizados mediante un modelo cooperativo que permita adaptarse de forma flexible a las necesidades cambiantes del servicio.

Otro punto importante es que el sistema será interoperable con las bases de datos actuales de la Defensoría Pública (MySQL, Oracle) y con la nueva base de datos SQL Server de Microsoft, logrando una transición fluida sin afectar la operación diaria. También se incorporará un módulo de Oficialía de Partes para la recepción de documentos y asignación de casos, además de funcionalidades especializadas para la etapa de ejecución, que permitirán dar seguimiento detallado y abogar por beneficios a los defendidos en esta fase, sin interrumpir el funcionamiento de otros componentes del sistema.

El sistema se integrará con la agenda institucional de correos electrónicos, permitiendo notificaciones automáticas, recordatorios y coordinación eficiente de audiencias y tareas. Asimismo, estará preparado para conectarse con el nuevo sistema de la Fiscalía, actualmente en su etapa final de desarrollo, permitiendo una administración estatal completa y sincronizada de expedientes, con capacidad de adaptación y crecimiento conforme a las nuevas demandas operativas.

Como se puede observar, la solución tecnológica que se estará contratando debe ser un sistema **flexible, escalable y seguro**, capaz de evolucionar conforme a las crecientes necesidades operativas de la Defensoría Pública del Estado de Baja California. Esta capacidad de crecimiento, adaptación y respuesta eficiente ante nuevas demandas solo puede lograrse mediante una arquitectura moderna que permita la integración ágil de nuevas funcionalidades, la mejora continua de procesos, y la alta disponibilidad de los servicios del sistema. Por ello, se ha determinado que la **arquitectura de microservicios** es la más adecuada para el desarrollo de este sistema, ya que **es la que cumple plenamente con estos requerimientos estratégicos y técnicos**, asegurando un rendimiento óptimo, una mayor eficiencia en el uso de recursos, y una base sólida para futuros desarrollos, como la implementación de aplicaciones móviles y nuevas integraciones interinstitucionales.

Nombre del sistema

Sistema Integral para el Control y Administración de la Defensoría Pública en Materia Penal

1.1 Actividades generales

1.1.1 Se deberá brindar los servicios profesionales, que le permitan especificar el

entendimiento de los procesos, necesidades de negocio e identificación de interesados en la operación de los módulos del sistema.

- 1.1.2 Definir enlaces por parte de la Defensoría Pública que apoye en la gestión y coordinación de reuniones, seguimiento a la información y documentación solicitada, además de facilitar el acceso a las instalaciones.
- 1.1.3 Identificar mediante el análisis los requerimientos funcionales y no funcionales, así como criterios de aceptación. Dicho análisis deberá enfocarse en una metodología ágil y para lograrlo como mínimo realizar las siguientes actividades:
 - 1.1.3.1 Realizar sesiones de trabajo con los usuarios o interesados clave para recabar información de los procesos y flujos de trabajo relacionados con los requerimientos y necesidades identificadas.
 - 1.1.3.2 Revisar en conjunto con los usuarios claves los sistemas, reportes, archivos y base de datos que utilizados actualmente en los procesos relacionados con los requerimientos y necesidades identificadas.
 - 1.1.3.3 Entrevistar a personal experto en la materia, tanto personal interno y externo a la organización.
- 1.1.4 Llevar a cabo presentaciones del sistema para mostrar avances a los usuarios de manera periódica, con motivo de identificar situaciones no consideradas en el análisis y tomar decisiones para solventarlas.
- 1.1.5 Dar seguimiento al proyecto a través de sesiones mensuales con la finalidad de revisar los avances del plan de trabajo del proyecto.
- 1.1.6 Definir y planificar procesos paralelos con el apoyo de los usuarios responsables de las operaciones.

2. Requerimientos de Funcionalidad del Sistema

2.1 Características Generales

Se requiere del desarrollo de un sistema integral para el control y administración de la defensoría pública en materia penal, que cumpla con las siguientes características:

- 2.1.1 Que se desarrollen los módulos y características solicitados en función de los requerimientos de la Defensoría Pública de Gobierno del Estado de Baja California.
- 2.1.2 Que se administre la información de forma histórica referente al contenido de los expedientes.
- 2.1.3 Que la información resida de forma centralizada en una base de datos.
- 2.1.4 El acceso a la información será de acuerdo a los roles de los usuarios.
- 2.1.5 El usuario administración será quien defina el control de accesos a módulos y usuarios del sistema.

- 2.1.6 Que se cuente con una consulta detallada de los expedientes y sus anexos.
- 2.1.7 El sistema deberá operar con una interfaz vía web.
- 2.1.8 El sistema manejará diferentes niveles de conexión con los operadores, favoreciendo los API REST y Web Services.
- 2.1.9 El sistema se conectará de manera simultánea a diferentes bases de datos de la Defensoría (MYSQL, ORACLE, SQL Server Microsoft).

2.2 Módulos que integran el Sistema

2.2.1 Módulo de Administración, Configuración y Mantenimiento

En este módulo se llevará a cabo la administración, mantenimiento y configuraciones al sistema para una correcta operación a través de las siguientes funcionalidades:

- 2.2.1.1 Catálogo para el mantenimiento y configuración de módulos y procesos.
- 2.2.1.2 Catálogo para el mantenimiento y configuración de Roles que serán asignados a los usuarios.
- 2.2.1.3 Catálogo para el mantenimiento y configuración de usuarios.
- 2.2.1.4 Mantenimiento a catálogo de Tipo de Oficina
- 2.2.1.5 Mantenimiento a catálogo de Oficinas.
- 2.2.1.6 Mantenimiento a catálogo de Áreas.
- 2.2.1.7 Mantenimiento a catálogo de Empleados.
- 2.2.1.8 Mantenimiento a catálogo de Estado del Caso Penal.
- 2.2.1.9 Mantenimiento a catálogo de Tipos de Actividad.
- 2.2.1.10 Mantenimiento a catálogo de Prioridad.
- 2.2.1.11 Mantenimiento a catálogo de Motivo de Reasignación.
- 2.2.1.12 Mantenimiento a catálogo de Motivo de Activación.
- 2.2.1.13 Mantenimiento a catálogo de Motivo de Baja.
- 2.2.1.14 Mantenimiento a catálogo de Motivo de Solicitud de Ficha.
- 2.2.1.15 Mantenimiento a catálogo de Motivo de Suspensión.
- 2.2.1.16 Mantenimiento a catálogo de Trámites y Servicios.
- 2.2.1.17 Catálogo para el mantenimiento y configuración de plantillas.

2.2.2 Módulo para la Etapa de Control

Modulo para llevar el seguimiento de las asesorías relacionadas con la etapa de control, y permitirá los siguientes procesos y funcionalidades:

- 2.2.2.1 Opción de oficialía de partes para dar ingreso a los casos y definir al defensor responsable y de seguimiento.
- 2.2.2.2 El sistema debe brindar la opción para reasignar defensores en cualquier etapa del proceso.
- 2.2.2.3 Se deberá contar con acceso a través de una consulta al sistema de la Fiscalía General del Estado.
- 2.2.2.4 Se deberá tener acceso a la agenda de las audiencias del Poder Judicial del Estado.
- 2.2.2.5 Se deberá habilitar acceso a la información del sistema penitenciario.
- 2.2.2.6 El sistema tendrá en este módulo un proceso para el registro de todas las actividades que se llevan a cabo en relación con el expediente, con opción para subir documentos digitales como evidencia de cada actividad.
- 2.2.2.7 Se contará con la visualización de una agenda para consultar las actividades programadas o ya realizadas de los defensores en los casos, por ejemplo, las audiencias o asesorías al imputado.
- 2.2.2.8 Se deberá brindar la opción para suspender, reactivar o cerrar definitivamente algún caso.
- 2.2.2.9 El sistema a través de este módulo ofrecerá un proceso para la generación, edición e impresión de documentos. Considerando las configuraciones referentes a las plantillas.
- 2.2.2.10 Se deberá contar con la funcionalidad para el escaneo de documentos e integrarlos al expediente.
- 2.2.2.11 Este módulo debe brindar una consulta para visualizar todos los archivos relacionados con el expediente.
- 2.2.2.12 El sistema permitirá consultar los videos relacionados con las audiencias requeridas.

2.2.3 Módulo de Archivo

A través de este módulo se llevará un adecuado control del archivo que resguarda las carpetas de investigación, involucrando las siguientes funcionalidades:

- 2.2.3.1 Este módulo deberá tener habilitado una consulta con acceso al Sistema del poder Judicial para verificar la agenda de las audiencias.
- 2.2.3.2 Contará con una consulta general a todo el expediente del imputado.
- 2.2.3.3 Dentro de este módulo se llevará un control para los préstamos de las carpetas de investigación, donde se identificará a quién, cuándo y cuánto tiempo se

prestará la carpeta. Además del seguimiento para su entrega.

2.2.3.4 Se contará con una opción para generar un formato de préstamo de la carpeta de investigación.

2.2.3.5 Se deberá contar con la funcionalidad para digitalizar documentos e integrarlos al expediente.

2.2.4 Módulo para la Etapa de Ejecución

Modulo para llevar el seguimiento de las asesorías relacionadas con la etapa de ejecución, y permitirá los siguientes procesos y funcionalidades:

2.2.4.1 Contará con una consulta general a todo el expediente del imputado.

2.2.4.2 A través de este módulo se deberá permitir el registro de todas las actividades que se llevan a cabo en relación con el expediente en la etapa de ejecución y habilitar una opción para subir documentos digitales como evidencia de cada actividad.

2.2.4.3 Este módulo deberá tener habilitado una consulta con acceso al Sistema del poder Judicial para verificar la agenda de las audiencias de la etapa de ejecución.

2.2.4.4 Este módulo permitirá consultar los videos relacionados con las audiencias requeridas.

2.2.4.5 El sistema a través de este módulo ofrecerá un proceso para la generación, edición e impresión de documentos para la etapa de ejecución. Debiendo considerar las configuraciones referentes a las plantillas.

2.2.4.6 Se deberá contar con la funcionalidad para digitalizar documentos e integrarlos al expediente identificando la etapa de ejecución.

2.2.5 Módulo de Reportes e Indicadores

Mediante este módulo se podrán emitir los diferentes reportes e indicadores de forma oportuna para la medición y toma de decisiones en materia penal.

2.2.5.1 Los reportes generados por el sistema serán: Reporte de audiencias, reporte de asignaciones de expedientes, reporte de notificaciones del poder judicial, reporte de expedientes por delito, reporte por genero del imputado, reporte etapas del expediente, reporte de tipos de audiencia.

2.2.5.2 Todos los reportes podrán ser sorteados o filtrados, por ejemplo, rangos de fecha, municipio, defensor, oficina, etc. Y además podrán ser visualizados en pantalla y/o generados en archivos con formato PDF y de Excel.

2.3 Seguridad

Las prácticas de seguridad estarán alineadas a estándares internacionales como ISO/IEC 27001 y marcos de referencia como el NIST Cybersecurity Framework (CSF), con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información, así como la protección integral de los datos y la continuidad operativa. Las medidas implementadas incluirán la aplicación de políticas y controles de acceso adecuados, la prevención de accesos no autorizados, y la trazabilidad

(bitácora) de las operaciones. Toda la comunicación entre los diferentes componentes del sistema, así como con sistemas externos autorizados, estará cifrada mediante el uso de certificados de seguridad válidos, garantizando la protección de los datos en tránsito. La autenticación y autorización se realizará mediante el uso de Web Tokens seguros, permitiendo que únicamente usuarios y microservicios autorizados puedan acceder a los recursos del sistema, reforzando así los mecanismos de seguridad en las integraciones internas y externas.

Como medida adicional de seguridad, se establece que las API REST no estarán expuestas directamente al exterior, sino que serán accesadas únicamente de forma interna por el servidor web (tales como Apache Tomcat, IIS u otro que se utilice), asegurando que solo se ejecuten mediante procesos controlados y dentro de la infraestructura autorizada. Esto refuerza los controles de acceso y minimiza los riesgos de ataques externos hacia los servicios internos del sistema. De igual forma, el proveedor deberá observar y aplicar estas buenas prácticas durante todo el proceso de desarrollo, implementación y puesta en marcha del sistema, integrando controles técnicos que respalden estos lineamientos conforme se describe a continuación:

2.3.1 El sistema contará con diferentes niveles de acceso y una administración de roles, usuarios, menús y opciones del sistema.

2.3.2 Se definirán roles específicos para limitar los accesos de acuerdo a las responsabilidades de cada usuario.

2.3.3 El sistema deberá contar con una administración para el control de accesos por horarios de trabajo, días laborales y accesos libre en cualquier momento de fecha y horario.

2.3.4 El sistema deberá permitir consultar de manera general o por usuario los accesos realizados en sistema (bitácora) por una fecha o rango de fechas.

3. Requerimientos No Funcionales del Sistema

3.1 Interfaces de Usuario

Las interfaces del sistema deberán conservar los requerimientos mínimos de diseño necesarios para cumplir con la imagen institucional del Gobierno del Estado de Baja California.

3.2 Interfaces de Software

La integración con otros sistemas deberá hacerse favoreciendo conexiones por medio de API REST y Web Services.

3.3 Confiabilidad

El sistema deberá garantizar la confiabilidad, seguridad y un desempeño estable para todos los usuarios, permitiendo que la información almacenada sea consultada y actualizada de manera permanente y simultánea, sin que las cargas de trabajo afecten los tiempos de respuesta ni la continuidad de las operaciones.

3.4 Confidencialidad

La información administrada por el sistema deberá tomar las medidas preventivas y reactivas para prevenir la divulgación de la información a personas o sistemas no autorizados.

3.5 Integridad

El sistema deberá ser construido de tal forma que se mantenga los datos libres de modificaciones no autorizadas.

3.6 Desempeño

Garantizar la confiabilidad, la seguridad y el desempeño del sistema a los diferentes usuarios. En este sentido la información almacenada podrá ser consultada y actualizada permanente y simultáneamente, sin que afecte el tiempo de respuesta.

3.7 Disponibilidad

Esta estará definida por la disponibilidad del servidor por lo que se asegura una disponibilidad del 100% en horario normal de oficina.

3.8 Escalabilidad

El sistema deberá ser construido sobre la base de un desarrollo evolutivo e incremental, que permita incorporar nuevas funcionalidades y atender futuros requerimientos con el menor impacto posible sobre el código existente. Para ello, se deberán considerar principios de modularidad y reutilización de componentes, permitiendo realizar ajustes específicos sin afectar la operación general del sistema.

La arquitectura del sistema deberá estar preparada para escalar de manera flexible y eficiente, tanto en capacidad operativa como en funcionalidad, permitiendo desarrollar, modificar o eliminar módulos de forma independiente incluso después de su implementación inicial. Esta capacidad de escalado y adaptación facilitará la atención oportuna a las necesidades cambiantes de la Defensoría Pública, asegurando la optimización de recursos y la continuidad operativa en todo momento.

3.9 Facilidad de uso e ingreso a la información

El sistema debe ser de fácil uso para los usuarios, además debe presentar mensajes de error que permitan al usuario identificar el tipo de error y comunicarse con el administrador del sistema, o solucionarlo el mismo de ser posible.

3.10 Sostenibilidad

Todo el sistema deberá estar documentado en cada uno de los componentes de software que forman parte de la solución propuesta.

4. Consideraciones especiales

4.1 Se deberá considerar realizar un traspaso inicial de los catálogos que contienen información de utilidad para la operación de la defensoría pública pertenecientes a los sistemas de Fiscalía General y del Poder Judicial, además de establecer mecanismos para la actualización de los datos.

4.2 La consulta del expediente se conformará por lo menos de los siguientes datos:

- Datos generales
- Datos de Fiscalía general
- Relación de actividades
- Visualización de documentos
- Visualización de audiencias
- Estatus
- Bitácora de movimientos
- Relación de defensores asignados
- Identificación de etapas

- 4.3 El sistema deberá llevar un registro histórico de los movimientos que se hacen sobre el expediente.
- 4.4 Todas las notificaciones dentro del sistema se manejarán vía correo electrónico.
- 4.5 El intercambio de información con los sistemas de Fiscalía General del Estado, el Poder Judicial del Estado y la Comisión Estatal del Sistema Penitenciario se realizará favoreciendo conexiones por medio de API REST y Web Services.
- 4.6 Se deberá considerar por parte del proveedor el suministro de 2 licencias correspondientes a SQL Server 2022 standard 2 Core tipo NCE Perpetuo, además de la instalación y puesta a punto.
- 4.7 Se deberá considerar por parte del proveedor el suministro del licenciamiento de un agente Veeam Platform para SQL Server, además de la instalación y puesta a punto.

5. Especificaciones Técnicas

Con la finalidad de asegurar el cumplimiento de los objetivos y necesidades de la Defensoría Pública, así como la del área de informática, el sistema deberá contener al menos las siguientes características:

- 5.1 Proporcionar un plan de trabajo del proyecto donde se identifique y desglosen las actividades y los tiempos necesarios para concluir cada una de las etapas del proyecto y siguiendo una metodología ágil de desarrollo.
- 5.2 Representar en un cronograma las fases de desarrollo del sistema bajo la metodología ágil de Scrum.
- 5.3 Proporcionar un sistema en línea para la solicitud de cambios y reportes de incidentes para la comunicación entre el equipo de trabajo de la DEFENSORIA PUBLICA y el proveedor.
- 5.4 Detallar el proceso de control de cambios y aceptación de etapas.
- 5.5 Diseñar un plan de entrenamiento y capacitación para Usuarios finales.
- 5.6 Desarrollar un plan de pruebas.
- 5.7 La Base de datos que utilizará el sistema deberá ser SQL Server versión 2022 y deberá ser desplegada en la infraestructura de la DEFENSORIA PUBLICA, además la base de datos deberá de estar normalizada.
- 5.8 Para el desarrollo del BACK y FRONT END se utilizará cualquier lenguaje de programación orientada a objetos como puede ser PHP 7 o superior, Java, JavaScript, HTML5, C#, Node.JS y cualquier lenguaje que sea óptimo para el microservicio que atiende el módulo del sistema.
- 5.9 El código deberá de estar comentado y documentado y el proveedor deberá utilizar un sistema de control de versiones como GitHub, en el cual se estará publicando y gestionando el código fuente del proyecto durante todas las fases de desarrollo.
- 5.10 El proyecto debe funcionar como mínimo en los siguientes exploradores de Internet: Google Chrome y Mozilla Firefox.

5.11 Cada microservicio deberá atender los estándares de nomenclatura de base de datos aplicables a su ámbito, incluyendo procedimientos, triggers, índices, llaves primarias y foráneas, según corresponda. Asimismo, se deberá respetar una estructura clara de programación modular y por capas internas, que contemple la separación lógica entre presentación, lógica de negocio y acceso a datos dentro de cada servicio. Esta organización garantizará la facilidad de mantenimiento, escalabilidad y claridad del código, alineándose con las buenas prácticas de desarrollo en arquitecturas distribuidas.

5.12 Los archivos multimedia que componen las carpetas electrónicas serán configurables con respecto a su ubicación.

5.13 El servidor web generará logs para identificar fallas.

5.14 El desarrollo y diseño del proyecto deberá estar basado en una arquitectura de microservicios, el cual permite una mayor flexibilidad en la implementación de nuevas funcionalidades, optimización del rendimiento y una gestión eficiente de los recursos.

El propósito de este esquema es que cada microservicio será responsable de una funcionalidad específica dentro del sistema. Estos microservicios se comunicarán entre sí a través de APIs REST o mediante un sistema de mensajería asíncrona, lo que garantizará una interacción eficiente y segura.

5.14.1 Cada microservicio será desarrollado de manera independiente y podrá ser desplegado en entornos distribuidos, lo que facilitará la actualización y evolución del sistema sin afectar su operatividad. Ofreciendo las siguientes ventajas:

5.14.1.1 Escalabilidad

- Cada microservicio puede escalarse de manera independiente según la demanda.
- Optimiza el uso de recursos y mejora el rendimiento del sistema.

5.14.1.2 Mantenibilidad

- Facilita la actualización, mejora y corrección de errores sin afectar todo el sistema.
- Permite a equipos de desarrollo a trabajar en diferentes microservicios sin interferencias.

5.14.1.3 Alta Disponibilidad

- Si un microservicio falla, el resto del sistema sigue funcionando.
- Permite implementar estrategias de redundancia y recuperación automática.

5.14.1.4 Flexibilidad Tecnológica

- Cada microservicio puede desarrollarse con la tecnología más adecuada para su función.
- Facilita la integración con otros sistemas y la adopción de nuevas tecnologías.

5.14.2 Los microservicios a desarrollar deberán estar clasificados según su función, por ejemplo:

Comunicaciones Operadores de Justicia

Fiscalía

- Microservicio para atender la solicitud de Defensor
- Microservicio para solicitar expediente

Poder Judicial

- Microservicio para recepción de notificación
- Microservicio para solicitud de audiencias
- Microservicio para envío de promociones

CESISPE

- Microservicio para solicitud de antecedentes penales
- Microservicio para solicitud de informe judicial

Defensoría

- Microservicio visualizar multimedia.
- Microservicio para mantenimiento a catálogos
- Microservicio para mantenimiento a expedientes
- Microservicio para asignación de carga de trabajo
- Microservicio para actualización de agenda
- Microservicio para conexión con escáner
- Microservicios para notificaciones
- Microservicio para visualización de videos

5.15 . En el desarrollo del sistema podrá considerar el uso total o parcial del framework BAJA STACK, promovido por la Agencia Digital del Estado de Baja California, siempre y cuando la tecnología sea compatible con la arquitectura de microservicios, así como los requerimientos funcionales y técnicos del sistema, y no represente costos adicionales ni afecte los tiempos de entrega establecidos en este Anexo Técnico.

5.16 Con motivo de asegurar un adecuado análisis y una correcta implementación del sistema, se requieren los siguientes documentos que avalen que proveedor cuenta experiencia y capacidad técnica.

- Certificado de Scrum Master
- Certificado de Scrum Product Owner
- Carta del fabricante Veeam, donde certifique al proveedor como canal autorizado para venta/distribuidor y los servicios de soporte y mantenimiento relacionados.

6. Entregables

Los aspectos que al menos se deben documentar y/o entregar son:

6.1 Minutas de reuniones.

Documentar la relación de minutas que se lleven a cabo durante la vida del proyecto.

6.2 Relación de Historias de Usuarios.

Documentar con detalle las historias de usuario definidas entre las partes interesadas.

6.3 Memoria técnica.

Documentar con la relación de herramientas y configuraciones necesarias para la instalación del sistema, para la correcta operación del sistema.

6.4 Manuales de usuario

Documentar las guías que permitan a las personas que utilizan el sistema su entendimiento y uso de las funcionalidades necesarias para la operación.

6.5 Modelo Relacional de Base de Datos

Se deberá documentar el tipo de relación entre las tablas y vistas, así como, los atributos y el tipo de dato de cada tabla de la base de datos.

6.6 Diccionario de Base de Datos

Se debe describir la información que se guarda en cada tabla de la base de datos. Asimismo, también se debe de describir a detalle cada campo del atributo de la tabla donde se pueda apreciar para qué es cada columna.

De igual manera se tiene que describir a detalle las vistas, triggers y funciones que se vayan a utilizar.

6.7 Código Fuente

Se requiere la entrega del código fuente. Con la información técnica y capacitación para el entendimiento completo del código fuente y el desarrollo del sistema.

6.8 Manual técnico del sistema.

El propósito de este documento es brindar una guía al personal del sistema para el área de Informática con el posible soporte que se valla presentado en la operación de cada día del sistema. Cada documento deberá de estar dividido en estos apartados:

6.8.1 Descripción general del proceso.

En este apartado se tiene que describir de manera general para que se usa la sección o pantalla del sistema.

6.8.2 Validaciones previas (Información en base de datos)

En esta sección se tiene que poner todas las tablas de la base de datos en las que tiene que existir información para poder realizar el proceso. Para esto, se requiere que se ponga en el documento, en una tabla con dos columnas la siguiente información, por renglón.

6.8.2.1 Nombre de la tabla

Se tiene que poner el nombre de la tabla, en dado caso de manejar más de una base de datos, se tiene que agregar el nombre de la base de datos.

6.8.2.2 Descripción de la validación

Se tiene que poner el nombre de cada columna de la tabla de la base de datos con el valor o la información que tiene que contener cada columna y por qué debe contener ese valor.

6.8.3 Descripción del proceso

En esta parte del proceso se tiene que describir paso a paso todo el proceso de inicio a fin, donde se pueda ir apreciando de que tablas se va obteniendo información para iniciar el proceso, validaciones que se tienen que ir cumpliendo, tablas donde debe de existir información y tablas donde se va guardando la información.

6.8.4 Programas

En este apartado se tienen que proporcionar de manera específica todos los archivos que intervienen de alguna manera en el proceso, en una tabla con la siguiente

información: nombre de las Clases ("cs"), Métodos, nombre de los archivos "cshtml","aspx", entre otros.

6.9 Catálogo de errores

El propósito de este documento es tener definidos los tipos de errores que pueden surgir en el intercambio de registros en cualquier parte de los procesos definidos del sistema. Como pueden ser errores lógicos, físicos y de transmisión de datos. El documento tiene que contener la siguiente información:

6.9.1 Atributo.

Nombre del atributo o campos que está causando el error.

6.9.2 Reglas de validación.

Regla de validación que no se está cumpliendo por la cual se está marcando el error.

6.9.3 Código de Error.

Código del error a mostrar en pantalla.

6.9.4 Descripción del Error.

Descripción general de la causa del error.

6.9.5 Archivo responsable.

Nombre y ruta del archivo que contiene mensaje del error

7. Plazo de entrega

El plazo de entrega no deberá exceder del día **15 de diciembre de 2025.**

8. Garantía y vicios ocultos

8.1 Tiempo de garantía

Los servicios de desarrollo del sistema deberán contar con una garantía contra fallas atribuibles al diseño, desarrollo y/o vicios ocultos, por un periodo de un año natural a partir de la fecha de firma del Documento de Aceptación Final.

8.2 Vicios ocultos

Los vicios ocultos para este contrato de servicios se definen como aquellos que reúnan las siguientes características:

- Haber existido al tiempo de la entrega final del desarrollo del sistema solicitado.
- Ser tales, que el desarrollo del sistema contratado no sirva para su uso natural o sirva imperfectamente, de acuerdo con lo solicitado y documentado por Defensoría Pública del Gobierno del Estado de Baja California.