Plan Ceibal

Concurso público de precios

Horas de desarrollo y mantenimiento para plataforma de desarrollo profesional para docentes

PLIEGO ESPECÍFICO

ÍNDICE

1 OBJETIVO

Centro Ceibal llama a Concurso público de precios para contratar horas de desarrollo de software en modalidad remota o in situ para el desarrollo a medida de una plataforma de desarrollo profesional para docentes.

Este llamado tiene como objeto la adquisición de horas de desarrollo para tecnologías web (Ítem 1 y 2), a ser ejecutadas en un plazo de hasta dos años, según las necesidades de Centro Ceibal.

Ítem 1	Ítem 2
20 horas mensuales de soporte, desarrollo y mantenimiento a ser distribuidas entre mantenimiento correctivo y evolutivo (computado en horas mensuales). Las horas no ejecutadas podrán ser acumuladas hasta el mes siguiente.	La adquisición de **hasta 1600 horas de desarrollo y mantenimiento** para a ser ejecutadas en un plazo de hasta dos años, según las necesidades de Centro Ceibal, en modalidad bajo demanda.

Cada oferente deberá ofertar ambos ítems.

ITEM 1

Las 20 horas mensuales de desarrollo y mantenimiento serán utilizadas fundamentalmente para mantenimiento evolutivo al inicio del proyecto y luego, una vez puesta en producción la plataforma, se utilizarán tanto para mantenimiento correctivo como evolutivo, (las horas no ejecutadas podrán ser acumuladas hasta el mes siguiente).

Se utilizará una herramienta de gestión provista por Ceibal para el seguimiento de incidentes, donde se realizará el control de horas de cada mes. El oferente deberá brindar un resumen mensual en base al SLA propuesto.

La oferta deberá incluir una descripción del nivel del servicio propuesto, según los diferentes niveles de criticidad. A modo de ejemplo, tiempo de respuesta a incidentes, resolución y recuperación ante fallos, considerando un horario de atención de Lunes a Viernes de 9:00 a 17:00 horas (días hábiles) (Ver Anexo 5.2.3).

ITEM 2

Las 1600 horas a demanda podrán ejecutarse dentro las oficinas de Ceibal (in situ) o de forma remota.

Para el mantenimiento evolutivo, Centro Ceibal gestionará el proyecto, dividiendo los requerimientos en fases, con una metodología ágil a acordar con el proveedor.

Para cada fase, se entregarán los requerimientos a la empresa adjudicada, quien deberá estimar el esfuerzo de desarrollo necesario. Para cada fase o etapa, se requerirá la elaboración de entregables, como por ej. documentación relativa al proyecto. Una vez acordado con Centro Ceibal las horas que insumirá el desarrollo de cada fase, documentación requerida, período de garantía y la fecha de entrega de la misma, la empresa adjudicataria realizará el desarrollo.

Una vez informada la necesidad y los requerimientos de las tareas a realizar, el proyecto de mantenimiento evolutivo deberá comenzar como máximo en un plazo de 7 días calendario. Las horas consumidas no pueden superar la estimación aprobada para la fase, salvo razones fundadas con aprobación del Centro Ceibal.

Las partes acordarán un período de garantía para cada entregable definido durante la etapa de ejecución del proyecto, considerando 30 días como una pauta general.

Para los proyectos solicitados, los roles para la conformación del equipo podrán ser: Project Manager, Arquitecto de Software, Diseñador Web, Desarrollador, Tester y Técnico de infraestructura.

Cualquier modificación en el equipo de trabajo deberá ser notificada previamente (mínimo una semana) por escrito al Centro Ceibal, y su integración al equipo quedará sujeta a la aprobación del Centro Ceibal.

Se acordarán con el proveedor las etapas de transferencias de conocimiento y auditorías de desarrollo durante el transcurso del proyecto, las mismas podrán ser de forma presencial en Ceibal. Se podrán coordinar reuniones presenciales o por videoconferencia de forma periódica, según lo requiera el proyecto.

Para el mantenimiento evolutivo, en modalidad horas, Centro Ceibal podrá solicitar horas de desarrollo de un perfil Desarrollador, el que trabajará en los días y horario habitual del Centro Ceibal (lunes a viernes de 9 a 17 hs). Esto podrá ser tanto en modalidad remota como in situ, dependiendo de las necesidades por parte del cliente.

2 CARACTERÍSTICAS DEL SERVICIO

2.1 ESPECIFICACIONES OBLIGATORIAS

El oferente deberá contar con sólidos conocimientos de:

Especificaciones obligatorias	
Excluyentes	No excluyentes
● Base de datos MySQL ● Express Node JS ● React	● October CMS ● Laravel PHP ● Java EE ● Sequalizer ● Herramientas de extracción de datos como Pentaho ● Open Badges

2.2 SISTEMA INVOLUCRADO

El sistema involucrado trata de una **plataforma de desarrollo profesional docente** que se compondrá fundamentalmente de los siguientes módulos:

- **Módulo de gestión de instancias formativas** donde se presenta la oferta, se habilita la inscripción y se realiza el seguimiento de las distintas instancias formativas. Integración con diferentes LMSs para la sincronización de datos (primera integración: Schoology).

- **Módulo de desarrollo profesional docente,** su principal funcionalidad se basa en la oferta, gestión y seguimiento de las trayectorias formativas basadas en el desarrollo de competencias. Posible integración con un sistema de evaluación docente.

- **Módulo de micro acreditaciones certificadas por Ceibal,** cuya funcionalidad es emitir certificados digitales que cumplen con el estándar Open Badges para aquellos docentes que finalizan una instancia formativa.

La lista de módulos es orientativa y por tanto no taxativa, pudiendo modificarse durante la extensión del contrato.

2.3 FORMA DE TRABAJO

La empresa adjudicada deberá seguir las pautas de desarrollo y seguridad definidas por Ceibal.

Se utilizará Git como repositorio de código fuente utilizando la metodología git-flow. El repositorio Git será provisto por Ceibal.

Los servicios podrán ser prestados en forma remota así como in situ en las oficinas de Centro Ceibal por su característica o urgencia, según Centro Ceibal considere conveniente. En el caso de la modalidad in situ, Centro Ceibal proporcionará el espacio físico, licencias y accesos que correspondan. En caso de ser necesario se podrá brindar un PC.

La empresa oferente deberá contar con ambientes de desarrollo, mientras que Ceibal proporcionará los ambientes de testing, preproducción y producción. Si bien estos serán hosteados y administrados por parte de Ceibal, se podrá requerir realizar tareas de pasaje a producción por parte del proveedor.

3 OFERTA

3.1 MODALIDAD DE COTIZACIÓN

El oferente deberá cotizar las horas de desarrollo en el siguiente cuadro:

Horas de desarrollo y mantenimiento - Pesos uruguayos	
	Completar todas las celdas en blanco
	Costo (imp. incl.)
Cotizar **por el total de 20 horas mensuales -** Item 1	
Cotizar **por hora** [1] **-** Item 2 (hasta 1600 horas)	
Trabajos fuera de Horario de oficina[2] - Cotizar **por hora** (hasta 200 horas)	

Todos los costos necesarios para brindar el servicio (conexión a internet, computadoras, teléfono, equipamiento necesario para desarrollar), viáticos y horas de transferencia son de cargo del proveedor.

Centro Ceibal se reserva el derecho de pre-calificar al segundo mejor proveedor, a quien podría contratarle horas a los precios cotizados, sólo en caso de que el adjudicatario manifieste que no cuenta con capacidad operativa ante determinado requerimiento concreto.

[1] Cotización que contemple todos los roles: Project Manager, Arquitecto de Software, Diseñador Web, Desarrollador, Tester y Técnico de infraestructura, tanto en modalidad remota como in situ.

[2] Horario de oficina: 9:00 a 17:00 días hábiles.

3.2 PRESENTACIÓN DE LA OFERTA

La oferta debe incluir en forma obligatoria los siguientes elementos:

✓ **Antecedentes** relativos a experiencias en proyectos en sistemas y tecnologías similares a las que son objeto del presente llamado:

a. Sección 2.1 - Especificaciones **obligatorias excluyentes**: como requisito excluyente, el oferente deberá tener al menos 5.000 horas (acumuladas) de dedicación para la tecnología con antigüedad no mayor a 3 años (Base de datos MySQL, Express Node JS, React).

b. Sección 2.1 - Se valorará tener experiencia acreditada en proyectos en las tecnologías descrita en las especificaciones **obligatorias no excluyentes**.

c. Sección 2.2 - Se valorará tener experiencia acreditada en proyectos de desarrollo de sistemas orientados a la educación de alcance nacional. Especialmente aquellos orientados al público objetivo de la plataforma, contemplando aspectos de interfaz de usuario, interoperabilidad con otras plataformas y capacidad de explotación de datos.

El oferente deberá presentar carta de recomendación, licitaciones similares adjudicadas o datos de contacto de clientes para corroboración de antecedentes.

El oferente se podrá asociar con otras firmas en forma de asociación en participación (Joint Venture) o subcontratistas conforme se menciona en el Pliego General con el fin de mejorar sus calificaciones de antecedentes.

✓ **Presentación del equipo de trabajo**, incluyendo currículums del personal que será responsable de prestar el servicio. Deberán incluir formación y experiencia relevante en desarrollo, con su respectiva dedicación horaria al objeto del llamado.

✓ **Oferta económica** (3.1 - Modalidad de cotización)

✓ **Oferta técnica:**. El proveedor deberá entregar al menos una propuesta arquitectónica de manera de abordar los requerimientos detallados en el Anexo 5.5. Tener en cuenta que la lista de módulos es orientativa y por tanto no taxativa, pudiendo modificarse durante la extensión del contrato.

- ✓ **Propuesta de SLA para mantenimiento correctivo** (Ver Anexo 5.2.3)
- ✓ **Tabla de Cumplimiento de Seguridad** de la Información: disponible en el Anexo 5.4

3.3 EVALUACIÓN

El criterio de evaluación técnica de los oferentes será en base al cumplimiento de las especificaciones obligatorias para la prestación del servicio (sección 3.2), sumado a un análisis de los curriculums de los técnicos presentados por las empresas oferentes, antecedentes y SLA presentado.
Se procederá a estudiar la oferta económica de aquellas propuestas que hayan superado el 60% de los puntos totales correspondientes a la evaluación técnica. Para la evaluación económica, se tomará en consideración el escenario máximo de horas para los ítems 1, 2 y 3.

Evaluación	
	% Evaluación máximo
Antecedentes	20
Cvs	20
SLA	6
Consideraciones de seguridad	4
Oferta económica	30
Oferta técnica	20
TOTAL	**100**

4 PROPIEDAD INTELECTUAL

Todos los trabajos realizados a raíz de la contratación de este servicio serán de propiedad exclusiva de Centro Ceibal, debiendo la empresa adjudicada transferir los códigos y la información que Ceibal requiera.

El oferente garantizará que no infringirá derechos de autor, de propiedad industrial e intelectual de terceros y que mantendrá indemne al Centro Ceibal ante cualquier reclamo derivado de violaciones de derechos de propiedad intelectual y/o derechos de autor.

5 ANEXO

5.1 PRESENTACIÓN DE ANTECEDENTES

Tecnología utilizada	Nº de proyecto/s (1)	Nombre/s del proyecto (2)	Total horas por tecnología	Total de horas acumuladas (últimos 3 años) >= 5.000
Especificaciones obligatorias excluyentes				
Express Node JS	1.. 2... 3..			
React				
Proyectos que se realizaron en Base de datos MySQL				
Especificaciones obligatorias no excluyentes				
October CMS				
Laravel PHP				
Java EE				
Sequalizer				

Herramientas de extracción de datos como Pentaho				
Open Badges				
Especificar proyectos vinculados a Educación				
Otros				
Otros (que se considere relevante en proyectos de mantenimiento como tecnología recomendada)				

Ordenar del más reciente al más antiguo, por tecnología. Se valorarán sólo antecedentes de los últimos 3 años.

N° proyecto (1)	Nombre del proyecto (2)	Institución contratante	Contacto responsable de dicha institución, cargo, télefono, mail	Descripción y alcance del proyecto	Período en el que fue realizado Duración en meses	Cantidad de integrantes del equipo de trabajo Nombres y roles de los responsables	Proyectos derivados (si los hubiera) tomado como insumo lo realizado por el proyecto	Horas dedicadas en total	Lenguajes y Base de datos (incluir versiones usadas)	Hipervínculo a la carta de recomendación (si hubiere)

Para proyectos vinculados a Educación detallar interoperabilidad con distintos LMSs, experiencia con público docente y manejo de datos de estudiantes

5.2 ACUERDOS DE CALIDAD DEL SERVICIO

5.2.1 CALIDAD DEL SERVICIO

En cada proyecto asignado, el proveedor será responsable de realizar todas las pruebas que considere pertinentes para garantizar el funcionamiento correcto de la aplicación o sistema bajo prueba, tanto en requerimientos funcionales como no funcionales definidos en cada proyecto.

Ceibal auditará la calidad de cada entregable, así como también el detalle de casos de prueba definidos, planes, estimación y documentación pertinente en cada etapa del proyecto. En caso que Ceibal detecte incidentes de prioridad Urgente o Inmediata que hubieran podido detectarse durante el proceso de testing del proveedor adjudicado, deberá ejecutarse nuevamente el ciclo de pruebas diseñado sin costo extra.

5.2.2 ACUERDOS DE NIVEL DE SERVICIO

Se establecerán previamente un conjunto de parámetros para medir la calidad mínima y aceptable de los servicios prestados durante la vigencia de la relación entre las partes que se mencionan continuación.

5.2.2.1 PARÁMETROS DE EVALUACIÓN

1. Cumplimiento del plazo: se busca determinar si la provisión del producto (bien o servicio) fue entregado por el proveedor en el plazo acordado. Para ello se considerará:

- a. Cumplimiento de plazos acordados. Para mantenimiento correctivo, el SLA presentado en la sección 5.2.3.
- b. Seguimiento de pendientes
- c. Notificación oportuna de posibles retrasos

2. Calidad del producto o servicio recibido: se busca medir si el producto (bien o servicio) alcanzó el estándar de calidad que le fue exigido. En este atributo se concentran todas aquellas mediciones que permitan evaluar los aspectos técnicos debidamente especificados, ya sea mediante Especificaciones Técnicas propias, Normas, Instructivos, incluso cualquier otro régimen regulatorio o documento, que contractualmente los proveedores están obligados a cumplir. Para ellos considerar los siguientes aspectos:

- a. Calidad del equipo / obra suministrada (incluye calidad de materiales usados)
- b. Trabaja según los procedimientos acordados con Ceibal
- c. Calidad de la documentación provista
- d. Idoneidad del personal clave
- e. Seguridad de la solución

3. Servicio de post-venta: se busca medir el grado de respuesta del proveedor en pro de satisfacer necesidades vinculadas con el producto (bien o servicio) adquirido posterior a la entrega. Se busca medir si la respuesta del proveedor contribuye a la Calidad de la institución y si demuestra que lo suministrado es confiable. Al momento de evaluar, considerar los siguientes aspectos:

- a. Relacionamiento y comunicación post venta
- b. Respuesta ante reclamos luego de la prestación del servicio o entrega del bien.
- c. Aceptación / rechazo de trabajos (p.ej. en casos particulares de un contrato)
- d. Capacidad de trabajo
- e. Cumplimiento de garantías
- f. Coherencia de facturación
- g. Gestión de incidentes de seguridad

El incumplimiento de los acuerdos del nivel de servicio o plazos comprometidos sobre cualquiera de los parámetros para cada fase o sprint, según su impacto y gravedad, podrá ser objeto de un Reclamo o No conformidad ocasionando penalidades al proveedor. .

Se entiende como Reclamo aquellos incumplimientos sobre cualquiera de los parámetros descritos anteriormente (sección 5.2.2.1 anterior) que impacten de forma negativa sobre la continuidad del proyecto.

Se considera una No conformidad cuando se incumplen los plazos acordados con el Centro Ceibal de cualquiera de los hitos descritos en la sección 5.2.2.2, cuando se acumulen 5 Reclamos, o ante otros

incumplimientos a los términos acordados y obligaciones asumidas, según la gravedad e impacto de dicho incumplimiento.

La sumatoria de 3 No conformidades, se considera incumplimiento grave, lo que podría habilitar la rescisión del contrato por incumplimiento, ejecución de la garantía de cumplimiento de contrato y aplicación de las penalidades correspondientes según sección 5.2.2.3

Fuera de estos casos, ante incumplimiento grave de parte de la Empresa, Centro Ceibal podrá rescindir el contrato inmediatamente sin responsabilidad, ejecutar la garantía de cumplimiento de contrato y aplicación de las penalidades correspondientes, según sección 5.2.2.3.

5.2.2.2 HITOS

- Inicio de Proyecto

Hito comprometido	Retraso Aceptable
Cronograma de trabajo con hitos identificados con responsables	Una semana desde la fecha acordada

- Análisis y Diseño

Hito comprometido	Retraso Aceptable
Entrega de documentos de Plan de Pruebas incluyendo Estrategias de testing adoptada	Una semana desde la fecha acordada
Entrega de Diseño de Casos de Prueba	Una semana desde la fecha acordada

- Ejecución

Hito comprometido	Retraso Aceptable
Entrega de evidencia de pruebas ejecutadas / Reporte de errores detectados	Una semana desde la fecha acordada
Documentación de Liberación de proyecto con instructivo de instalación	Una semana desde la fecha acordada
Documentación técnica actualizada	Una semana desde la fecha acordada
Código Fuente	Una semana desde la fecha acordada
Transferencia de conocimiento a Ceibal realizada (en caso de ser requerida)	Una semana desde la fecha acordada

En busca de llevar adelante una modalidad ágil de trabajo, se requiere que los retrasos aceptables para los hitos comprometidos para las etapas de Análisis y diseño y ejecución se cumplan en cada una de las fases o sprints acordadas.

5.2.2.3 PENALIZACIÓN

El ingreso de una No conformidad podrá determinar la aplicación de una penalidad equivalente al 10% del precio acordado para esa fase, o sprint, la que se podrá incrementar según la gravedad del incumplimiento, hasta un máximo del 50%.

Centro Ceibal podrá retener la penalidad/es del importe facturado.

5.2.3 SLA - NIVEL DE SERVICIO

TIEMPO DE RESPUESTA

Urgencia del incidente	SLA (Tiempo de Respuesta en horas)	Observaciones
Urgente		Son aquellos incidentes[3] presentados en producción sobre el aplicativo que detienen o afectan la operación, colocando en riesgo la operación de CEIBAL o el servicio brindado por CEIBAL a sus usuarios
Alta		Son aquellos incidentes presentados en producción sobre el aplicativo que no detienen la operación, pero sí impiden que algunos recursos cumplan con su función básica.
Media /Baja		Son aquellos incidentes presentados en producción sobre el aplicativo que no impiden que cumpla con su función básica, pero sí les dificulta la operación.

[3] Incidencias: corresponden a cualquier evento que cause una interrupción del servicio o una reducción de la calidad del mismo

TIEMPO DE RESOLUCIÓN

Las partes acordarán para cada incidente el tiempo de solución del mismo. Especificar indicadores de resolución de incidentes mensual según nivel de urgencia.

Ejemplo: Porcentaje de incidentes resueltos en el plazo comprometido, en el mes y según nivel de criticidad.

El oferente puede añadir información que le parezca relevante en su propuesta de SLA.

El oferente deberá enviar mensualmente el informe con los indicadores definidos del SLA.

5.3 PRESENTACIÓN DE CVS

Ordenar la información de la más reciente a la más antigua.

Cuadro Resumen

Roles: Project Manager, Arquitecto de Software, Diseñador Web, Desarrollador, Tester y Técnico de infraestructura.

Rol	Nombre y Apellido	Dedicación (parcial o completa)

Cuadro por integrante

Cargo propuesto			
Perfil			
Educación			
Certificaciones/ Cursos relevantes			
Cantidad de años de experiencia en el perfil presentado			
Experiencia relevante para el llamado	Tecnología	Tiempo de experiencia: Proyectos URL (si corresponde)	
Historia Laboral	Desde	Hasta	Empresa/Rol/Principales actividades
Certificados (si corresponde)			

5.4 REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA COMPRA DE SISTEMAS INFORMÁTICOS Y HORAS DE DESARROLLO

Se establecen los requisitos a incluir al momento de realizar llamados para la compra de soluciones informáticas.

Requisitos obligatorios Estos requisitos son obligatorios para todas las soluciones informáticas, así como herramientas de hardware, a ser adquiridas por Centro Ceibal. Podrán haber excepciones que deberán estar justificadas y aprobadas por quien corresponda.

Requisitos deseados Estos requisitos no son obligatorios pero serán valorados al momento de adjudicar la compra.

Descripción de requisitos:

- **Diseño y arquitectura**

La solución deberá tener incorporada la seguridad en su diseño mediante el uso de buenas prácticas y la incorporación de la seguridad desde el diseño como parte de todo el proceso del ciclo de desarrollo de la solución.

Deberá cumplir los siguientes requisitos:

- Desarrollo por capas (presentación, lógica de negocio y datos).
- Solución modular con separación y agrupación de funcionalidades por categorías o módulos que permita la escalabilidad de la solución y facilite la integración y compatibilidad con otras soluciones.
- Arquitectura confiable que incorpore una visión de la seguridad integral cubriendo los aspectos de confidencialidad, disponibilidad, integridad, no repudio y privacidad a través de métricas e indicadores cualitativos como cuantitativos.

- **Autenticación**

La solución deberá cumplir con métodos de autenticación seguros que permitan verificar la identidad de los usuarios y protejan la confidencialidad de la información.

Deberá incorporar los siguientes requisitos:

- Autenticación con usuario y contraseña que cumpla las políticas de contraseñas del Centro Ceibal.
- Compatibilidad con los sistemas de autenticación centralizados (SSO) usados por Centro Ceibal según corresponda:
- Sistema de Login único para beneficiarios. (protocolo CAS - ver Anexo)
- Compatibilidad para autenticación con alguno de los siguientes proveedores de identidades (Google, Active Directory) detallando protocolos y configuraciones usados.
- Posibilidad de autenticación con múltiples factores (MFA) para cuentas privilegiadas.

- **Gestión de sesiones**

La solución deberá proveer una adecuada gestión de sesiones de usuarios permitiendo conocer el estado actual del usuario o el dispositivo conectado.

Para esto deberá:

- Mantener sesiones únicas para cada usuario que no podrán ser adivinadas o compartidas.
- Las sesiones serán desconectadas cuando ya no sean necesarias o durante un período de inactividad (en lo posible parametrizable).

- **Control de acceso**

La solución deberá proveer una adecuada gestión del control de acceso de manera de autorizar el acceso a las funcionalidades y datos en concordancia con los perfiles y roles que se definan.

Para esto deberá cumplir que::

- Los usuarios que quieren acceder a determinados recursos posean las credenciales correctas.
- Los usuarios estén asociados a un conjunto adecuado de roles y privilegios de acuerdo a las funcionalidades brindadas por la solución y a los recursos accesibles.
- Los metadatos de los roles y permisos deberán estar protegidos de manipulaciones y reutilizaciones.
- La asignación del control de acceso sigue el principio de menor privilegio.

- **Codificación y validación**

Las debilidades más comunes en aplicaciones web modernas, son los fallos en validar correctamente las entradas de datos que provienen de los usuarios y el entorno, previo al uso de esta información. Estas

debilidades generan la mayoría de las vulnerabilidades y ataques conocidos como por ejemplo Cross-Site Scripting (XSS), Inyección SQL, ataques al sistema de archivos, ataques Unicode y desbordamiento de buffers.

La solución deberá cumplir con:

- Asegurar la validación de entradas y salidas mediante una arquitectura de codificación y flujos seguros de la información que prevengan la inyección.
- Los datos de entrada sean robustamente ingresados y validados o en el peor de los casos filtrados y depurados.
- Asegurar una codificación de salida robusta que tome en cuenta el contexto de la información y sea lo más cercana al intérprete externo.

- **Manejo de errores y verificación de logs**

La solución deberá generar información de calidad en los logs y gestionar adecuadamente los mensajes de error, evitando en lo posible la publicación de información sensible.

Para lograr esto la solución deberá:

- No recolectar información sensible en los logs a menos que sea necesario o específicamente requerido.
- Asegurar que la información contenida en los logs es gestionada de acuerdo al nivel de clasificación de la misma (por ej. tomar en cuenta el ciclo de vida de la información y la caducidad de la misma).
- Incluir información útil para la auditoría y la solución de problemas que incluya como mínimo fecha, hora y detalle de los eventos, cambios en las configuraciones, intentos de acceso al sistema (exitosos y rechazados).

- **Confidencialidad y Protección de datos**

La solución deberá asegurar la confidencialidad, integridad y disponibilidad de la información y datos personales. Para implementar una adecuada protección de datos, la solución deberá asegurar la: legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva, y responsabilidad. Para esto la solución deberá:

- Cumplir con la normativa vigente uruguaya en materia de datos personales (Ley Nº 18.331, de 11 de agosto de 2008 y Decreto Nº 414/2009, de 31 de agosto de 2009). Se considera dato personal la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, a modo enunciativo, cualquier información numérica,

alfabética, gráfica, fotográfica, registro de voz e imagen, acústica o de cualquier otro tipo que refiera a ellas directa o indirectamente, conforme con lo dispuesto en el artículo 4 de la Ley Nº 18.331 y artículos 1 y 4 del Decreto Nº 414/009.

- Adoptar las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de los datos y evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información.
- Proteger la información y datos creada, editada, borrada o accedida sin las autorizaciones correspondientes, en particular en cantidades masivas de datos.
- Tomar las precauciones y controles necesarios para que la información y los datos personales no queden disponibles en navegadores, balanceadores de carga, copias temporales, cookies y otras estructuras donde no sea necesario.
- Asegurar la confidencialidad de toda la información que se procese o utilice. La Información Confidencial comprende, entre otros y a vía de ejemplo, la siguiente información: toda estrategia, plan y procedimiento comercial, información propietaria, software, herramienta, proceso, imágenes, datos personales, metodología, información y secreto comercial, y demás información y material de Ceibal, así como de los alumnos, beneficiarios, docentes, centros de estudios, que pudiera ser obtenida de cualquier fuente o pudiera ser desarrollada. .
- Alojar los datos en territorio uruguayo, o en caso de transferencia internacional asegurar que el servidor se encuentre en países considerados con niveles adecuados de acuerdo con la Directiva 95/46/CE. En caso contrario, contar con el consentimiento del titular del dato para la transferencia a un territorio no adecuado, o a que el importador haya suscripto cláusulas contractuales tipo con el exportador o posea un Código de Conducta inscripto, con la consecuente autorización de transferencia internacional de datos tramitada ante la Unidad Reguladora y de Control de Datos Personales, en los dos últimos supuestos.
- No utilizar la información / datos para una finalidad distinta a la contratada, ni en beneficio propio ya sea gratuito u oneroso, ni cederlos, comunicarlos o transferirlos a terceros.
- Centro Ceibal será el responsable de la base de datos y del tratamiento, siendo la Empresa adjudicada y sus empresas sub contratadas, encargados de tratamiento, de acuerdo con lo dispuesto en los literales H) y K) del artículo 4 de la Ley Nº 18.331.
- Permitir la publicación de las políticas de privacidad y términos y condiciones de uso de Centro Ceibal en el desarrollo.
- Permitir el derecho de acceso, rectificación, actualización, inclusión o supresión de los datos personales.
- Devolver o suprimir de todos sus sistemas y archivos físicos y lógicos, sean propios o contratados a terceros, los datos personales accedidos, obtenidos o tratados, así como los metadatos asociados, a requerimiento de Ceibal.

- **Comunicaciones**

La solución deberá proveer una comunicación segura de la información gestionada de manera de asegurar la confidencialidad de la misma.

Para esto deberá:

- Publicar servicios a través de protocolos seguros (TLS o encriptación robusta) para todos los usuarios y sin importar la sensibilidad de la información transmitida.
- Se utilizarán protocolos y algoritmos considerados seguros por la industria y las buenas prácticas, dejando como último recurso o por temas de compatibilidad que sean expresamente autorizados por Centro Ceibal el uso de otros protocolos menos seguros.
- La solución deberá ser enteramente compatible con los certificados usados por Centro Ceibal y en caso de usar certificados generados internamente deberán ser validados por las autoridades de certificación que Centro Ceibal establezca.

Nombre	Proveedor	Versión / Observaciones
Certificado SSL Comodin Amazon	**Amazon**	**Version 3 - 256 bits**
Certificado SSL Comodin Godaddy	**Godaddy**	**256 bits**
Certificado SSL Estandar Godaddy	**Godaddy**	**256 bits**
Certificado SSL Estandar UCC Godaddy – Hasta 5 subdominios	**Godaddy**	**256 bits**

- Todas las comunicaciones por fuera del protocolo HTTP, como por ej. accesos remotos, comunicación entre capas de la solución, middleware, bases de datos, fuentes externas de datos, monitoreo, herramientas de comunicación, etc. deberán ser comunicaciones seguras y en lo posible encriptadas.

- **Uso de archivos y recursos**

La solución deberá proveer controles sobre la gestión de archivos de manera de garantizar la seguridad de la información.

Para esto debe cumplir con:

- Los archivos inseguros deben ser gestionados adecuadamente de manera de garantizar la confidencialidad, integridad y disponibilidad de la información.

- Se deberán implementar controles para la subida, ejecución, bajada y alojamiento de los archivos que blinden la solución de ataques maliciosos y configuraciones inadecuadas como por ej.: bombas zip, tipos de archivos incorrectos, ataque pass traversal, alojamiento con permisos o en directorios incorrectos, ataque SSRF.

- **API y Web services**

La solución que haga uso de APIs (comúnmente a través del uso de JSON, XML, GraphQL u otros formatos) deberá cumplir con:

- Mantener una adecuada autenticación, gestión de sesiones y autorizaciones para todos los web services.
- Validación de entrada para todos los parámetros que son ingresados.
- Controles efectivos de seguridad sobre todo tipo de APIs, incluidas las nubes y las APIs sin servidores.

- **Respaldos y contingencia**

La solución deberá ser compatible con una adecuada política de respaldos y recuperación de datos de manera de asegurar la integridad y disponibilidad de la información frente a incidentes.

En caso de brindar la solución en modalidad de software como servicio (SaaS) la solución deberá:

- Cumplir con un plan de continuidad del negocio, que ofrezca la contingencia necesaria para asegurar la disponibilidad, integridad y confidencialidad de la información frente a distintos tipos de incidentes.
- Brindar las soluciones tecnológicas necesarias (por ej. respaldos y plan de recuperación ante desastres) de manera de asegurar los niveles de disponibilidad e integridad estipulados en el acuerdo de nivel de servicio correspondiente (SLA).

- **Criptografía**

La solución deberá cumplir con los siguientes requisitos a nivel de controles criptográficos:

- Permitir el uso de módulos criptográficos para proteger la información sensible de la solución como ser información financiera, datos personales y datos de roles y permisos, ya sea en reposo, en uso y en tránsito.
- Usar algoritmos de cifrado robustos (como por ej AES y RSA) con claves de longitud adecuadas para protegerse contra ataques.
- Generar números aleatorios adecuados.

- El acceso a las claves de cifrado es gestionado de manera segura.

- **Código malicioso**

La solución no deberá contener código malicioso de ningún tipo. Para cumplir con esto la solución deberá entre otras características:

- Utilizar herramientas de detección del código malicioso en el proceso de desarrollo.
- No incluir bombas de tiempo u otros tipos de ataque similares.
- No realizar transmisiones de información o contacto a destinos maliciosos o no autorizados.
- No contener puertas traseras, rootkits, ataques "salami", huevos de pascua y otros tipos de códigos maliciosos o que no siguen las buenas prácticas.
- Tomar las medidas necesarias para que la solución no incorpore código malicioso a través de controles como ser firma de código, uso de bibliotecas y frameworks seguros, control de caducidad sobre DNS, etc.

- **Lógica de negocio**

La solución deberá proveer una capa de negocio desarrollada de manera segura y que permita evitar los ciberataques más frecuentes. Para esto debe cumplir que:

- El flujo de la lógica de negocio debe ser secuencial, coherente y no puede ser alterado.
- La lógica de negocio incluye controles y límites que permiten detectar y prevenir ataques automatizados.
- La lógica de negocio debe tomar en cuenta casos de uso que incluyen actores maliciosos, casos de abuso y además debe contener protecciones contra ataques de spoofing, manipulación, repudio, divulgación de información y elevación de privilegios entre otros.

- **Configuración**

La solución deberá cumplir con los requerimientos y controles de configuración que garanticen una aplicación segura.

Los mismos deberán incluir:

- Un entorno lo más seguro, repetitivo y automatizable posible a través de la incorporación de buenas prácticas (ej. modelo DevSecOps) con herramientas, procesos y tecnologías que la * implementen adecuadamente (ej. contenedores, despliegues automatizados, etc.).

- Herramientas y entornos de desarrollo actualizados y correctamente mantenidos.
- Herramientas y entornos de desarrollo correctamente configurados y verificados en su seguridad (hardening) como por ej. deshabilitar el modo debug en entornos de producción.
- Seguridad por defecto en las configuraciones de los usuarios y los permisos.

- **Certificaciones**

Se valorarán las certificaciones y el cumplimiento con estándares relacionados al desarrollo seguro, la seguridad de la información y la privacidad como ser:

- Common criteria certification (ISO IEC 15408)
- CPA Build Standard
- OWASP ASVS
- ISO 27001
- FIPS 140
- SCAMP
- CIS Benchmarks
- AICPA SOC2-3
- NIST CSF / 800
- ISACA Cobit
- PCI DSS
- GDPR

- **Metodología**

Se valorarán las propuestas que incorporen metodologías de diseño y desarrollo del software con una visión integral de la seguridad en el proceso de desarrollo.

- **Análisis de vulnerabilidades**

Se valorarán las soluciones que hayan sido sometidas a chequeos estandarizados de vulnerabilidades y/o tests de penetración. Se deberá proveer constancia de las mismas mediante un informe resumen o certificado correspondiente.

Se valorará informe detallando cobertura de amenazas sobre el último OWASP Top Ten vigente.

Plan Ceibal

Matriz de cumplimiento de requerimientos de Seguridad de la Información

A completar por Ceibal			A completar por oferente	
Nº Req.	Requerimiento	Tipo	Cumplimiento	Observaciones
1	Diseño y Arquitectura	Obligatorio		
2	Autenticación	Obligatorio		
3	Gestión de sesiones	Obligatorio		
4	Control de acceso	Obligatorio		
5	Codificación y validación	Obligatorio		
6	Manejo de errores y logs	Obligatorio		
7	Confidencialidad y protección de datos	Obligatorio		
8	Comunicaciones	Obligatorio		
9	Uso de archivos y recursos	Obligatorio		
10	API y Web Services	Obligatorio		
11	Respaldos y contingencia	Obligatorio		
12	Criptografía	Deseado		
13	Código malicioso	Deseado		
14	Lógica de negocio	Deseado		
15	Configuración	Deseado		
16	Certificaciones	Deseado		
17	Metodologías	Deseado		
18	Análisis de vulnerabilidades	Deseado		

El campo Cumplimiento deberá completarse con "Cumple totalmente", "Cumple parcialmente" o "No cumple"

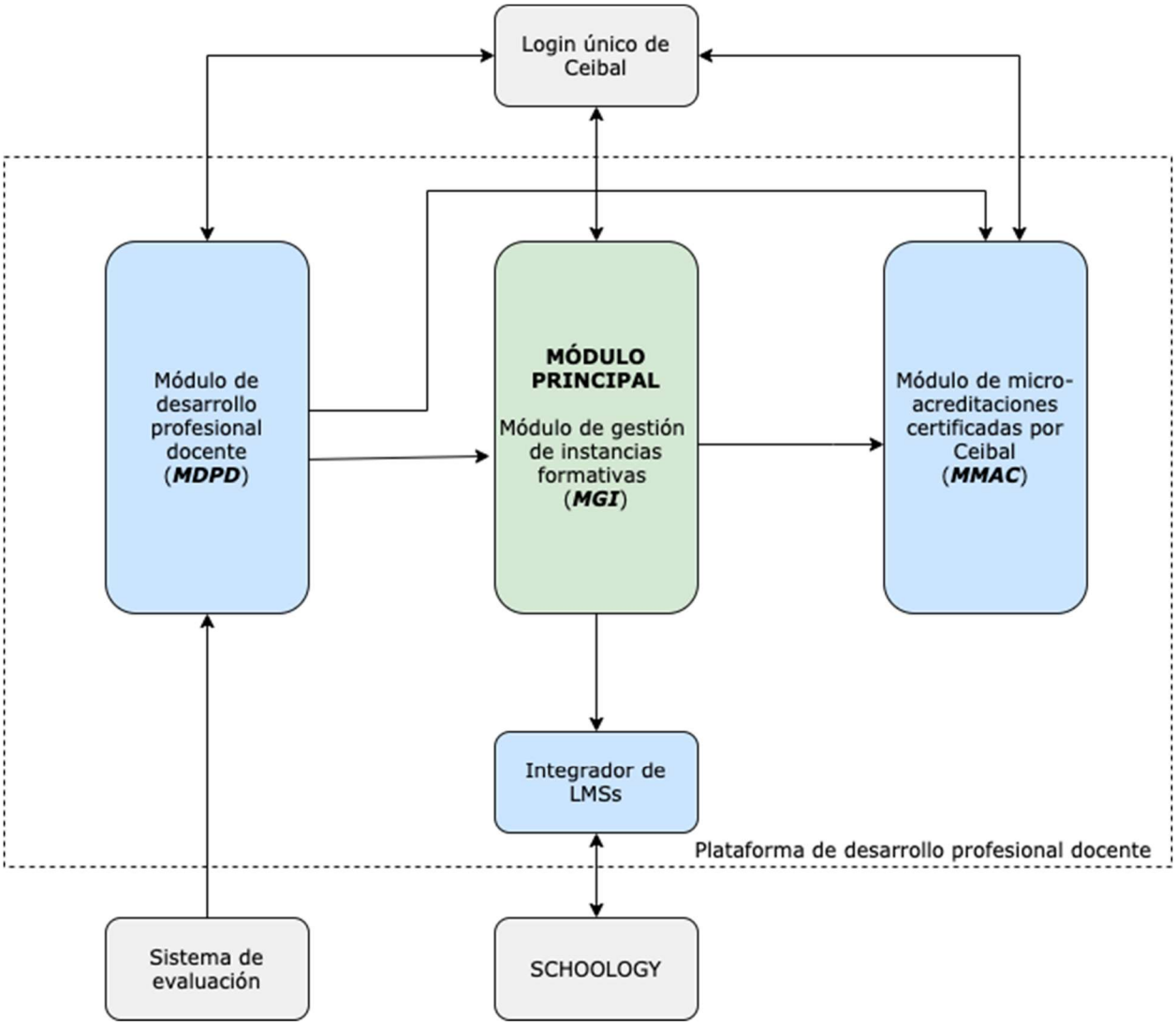
El campo Tipo contiene las sugerencias de obligatorios y deseables que brinda Seguridad de la Información. Los mismos podrán variar de acuerdo a las necesidades particulares de la solución a adquirir.

En caso que Ceibal lo requiera, se deberá tener a disposición y presentar, material que acredite lo declarado en la presente matriz de cumplimiento. A modo de ejemplo, se detallan algunos documentos que podrían ser solicitados:

- Set de pruebas de respaldos y plan de recuperación ante desastres para los casos en que la solución se brinda en modalidad SaaS.
- Certificación que acredite la ubicación física de los datos de acuerdo a los requisitos regulatorios de territorialidad.
- Arquitecturas y protocolos utilizados.

5.5 REQUISITOS DE ARQUITECTURA DE LA SOLUCIÓN

El siguiente diagrama muestra los distintos componentes que al día de hoy, se considera, serán parte de la plataforma:



El componente principal de la plataforma es el **módulo de gestión de instancias formativas (MGI),** el cual tiene como objetivo presentar la oferta de cursos. El mismo habilita la inscripción, para luego realizar el seguimiento de las distintas instancias formativas ofrecidas por Plan Ceibal.

Se integra con diferentes LMSs para la sincronización de datos a través de un componente integrador; es altamente probable que la primera integración se realice con Schoology. Para esto, el módulo debe enviar los datos de usuarios, instancias formativas y enrolamientos a través de una API que Schoology disponibiliza para hacerlo. A su vez, deberá obtener, a través de API, la información de instancias formativas finalizadas para actualizar el estado y solicitar la acreditación correspondiente.

El componente **MGI**, se integra además con el **módulo de micro-acreditaciones certificadas por Ceibal (MMAC)** cuya funcionalidad es emitir certificados, tanto digitales (cumpliendo con el estándar Open Badges), como tradicionales en formato pdf u otro formato a definir.

Ceibal dispone de una instalación de Open Badges, la cual podría utilizarse como punto de partida para la plataforma. Es altamente deseable que el futuro proveedor de servicios domine esta tecnología. Para esta integración, el **MGI** deberá enviar la confirmación de finalización de la instancia formativa, para que el **MMAC** puede emitir la micro-acreditación asociada a esa instancia.

Finalmente, se prevé un tercer componente denominado **módulo de desarrollo profesional docente (MDPD)**, cuya principal funcionalidad se basa en la oferta y seguimiento de cursos y trayectorias formativas basadas en el desarrollo de competencias.

Este módulo, podrá a su vez, recibir información de un sistema de evaluación de competencias digital que busca ofrecer a los usuarios instancias formativas que permitan desarrollar dichas competencias. Este módulo está fuertemente integrado con el **MGI**, de dónde obtendrá información de las instancias formativas, inscripciones, instancias finalizadas para la oferta, gestión y seguimiento de las trayectorias formativas.

Cada uno de estos módulos deberá implementar autenticación de usuario a través del sistema de login único que dispone Ceibal.

Es importante que la o las propuestas arquitectónicas presentadas contemplen estructuras de datos orientadas a la explotación de datos en sus diferentes niveles: reportes dentro de la plataforma, herramientas de repostería básica (ej.: Redash), herramientas de reportería avanzada (BI).