

Licitación Pública Internacional

Adquisición e Implantación de Nuevo
CRM

ANEXO A: PLIEGO ESPECÍFICO

ÍNDICE

1. Objetivo	4
1.1. Contexto del proyecto	5
2. Requerimientos	5
2.1. Requerimientos Obligatorios generales a todo el sistema	6
2.2. Requerimientos obligatorios de Usabilidad	6
2.3. Requerimientos Obligatorios Funcionales	7
2.3.1. Requerimientos obligatorios prioritarios a ser implementados dentro de este proyecto (fase 1)	7
2.3.2. Requerimientos obligatorios a ser implementados en un mediano plazo (fase 2).	11
2.4. Requerimiento Deseable no excluyente	12
3. Implantación de la solución	13
Documentación requerida para el Proyecto	14
Documentación Requerida del producto al finalizar la implantación:	14
4. Mantenimiento de la Solución	15
4.1. Servicio de Soporte y Mantenimiento de la solución	15
4.2. Mantenimiento Evolutivo Personalizado	15
5. Dimensionamiento	16
2 Características del servicio	19
2.1 Forma de trabajo	19
3 Oferta	20
3.1 Modalidad de cotización	20
3.2 Presentación de la oferta	21
3.3 Evaluación	23
4 Propiedad intelectual	23
5 Anexo 1	24
5.1 Presentación de antecedentes	24
5.2 Tabla de cumplimiento de Requerimientos	25
Requerimientos obligatorios a ser implementados dentro de este proyecto (fase 1)	25
Requerimientos obligatorios a ser implementados dentro de este proyecto (fase 2)	30
Generales al sistema	33
Usabilidad	36
5.3 Acuerdos de Calidad del Servicio	39
5.3.1 Calidad del Servicio	39
5.3.2 Acuerdos de nivel de Servicio	39
5.3.2.1 Parámetros de evaluación	39

5.3.2.2 Penalización	41
5.4 SLA - Nivel de servicio	42
TIEMPO DE RESPUESTA	42
Atención a pedido de servicio	43
TIEMPO DE RESOLUCIÓN	43
5.5 Equipo de proyecto	44
5.6 Requisitos de seguridad de la información para la compra de sistemas informáticos y horas de desarrollo	45
6 Anexo 2	60
6.1 Interoperabilidad del CRM	60
6.2 Anexo de Autenticación con Login único	60

1. OBJETIVO

Este llamado tiene como objeto la adquisición e implantación de una de las siguientes plataformas SaaS para la gestión integral de la información de los beneficiarios (centros educativos, estudiantes y docentes de la educación pública y privada de nuestro país) de Ceibal que se mencionan a continuación:

- Salesforce
- Microsoft Dynamics 365

Ceibal es el centro de innovación educativa con tecnologías digitales del Estado Uruguayo, al servicio de las políticas públicas educativas. Promueve la integración de la tecnología a la educación con el fin de mejorar los aprendizajes e impulsar procesos de innovación, inclusión y crecimiento personal. Centro Ceibal requiere una herramienta que acompañe su crecimiento optimizando los recursos y permitiendo realizar una gestión eficaz y eficiente de sus beneficiarios, y beneficios asociados, siendo este un aspecto crucial para nuestra organización. En este contexto, una herramienta de CRM (Customer Relationship Management) de clase mundial se convierte en un activo indispensable, asegurando que las comunicaciones sean oportunas y relevantes.

Esta herramienta es fundamental para garantizar la sostenibilidad y el crecimiento a largo plazo de los diferentes servicios que Ceibal brinda a sus beneficiarios.

Los ítems que serán de **cotización obligatoria** son:

ITEM 1: **Implantación de la solución - Requerimientos Prioritarios fase 1 (RFP):** En este ítem se deberá cotizar la implementación de los requerimientos obligatorios Generales (punto 2.1), de Usabilidad (punto 2.2) y los Requerimientos Funcionales que los descritos en el punto 2.3.1.

ITEM 2: **Implantación de la solución - Requerimientos Secundarios fase 2 (RFS):** En este ítem se deberá cotizar la implantación de los requerimientos descrito en el punto 2.3.2

ITEM 3: **Licenciamiento:** Se deberá cotizar el licenciamiento considerando contrato a 5 años. En caso que el licenciamiento dependa del módulo se deberá desglosar para cada uno. Ver punto 5 Dimensionamiento.

ITEM 4: **Mantenimiento de la Solución propuesta:** Se deberá cotizar dos subítems que cubran el mantenimiento correctivo y el mantenimiento evolutivo personalizado (punto 4 – Mantenimiento de la solución).

1.1. CONTEXTO DEL PROYECTO

Centro Ceibal cuenta actualmente con el CRM de Montevideo Comm, el cual fue implantado en las etapas iniciales de desarrollo de la organización. Este producto fue adaptado y configurado para cumplir con los objetivos operativos de aquel entonces (año 2011), pero actualmente presenta dificultades en el acompañamiento de los cambios y nuevas necesidades de la organización.

En la actualidad los productos, programas y servicios que brinda Centro Ceibal a todos sus beneficiarios se han incrementado y diversificado, por lo que es necesario realizar un cambio a una solución tecnológica que cubra las necesidades en su totalidad.

Los principales objetivos que buscamos son:

- Contar con una visión 360 para diferentes entidades (Beneficiarios, Centros Educativos, etc.).
- Mayor eficacia y eficiencia en la gestión de las relaciones y comunicaciones con los beneficiarios y los procesos de negocio asociados.
- Simplificación de la operación diaria incorporando nuevas funcionalidades para la gestión de campañas y automatización de procesos.
- Flexibilidad para la incorporación de nuevos procesos.
- Actualización tecnológica: contar con un producto con un roadmap que le permita la sustentabilidad en el tiempo incorporando nuevas tecnologías y funcionalidades, tales como la introducción de la IA en la interacción con el beneficiario.
- Estricto cumplimiento con los requisitos de seguridad de la información y privacidad de datos.
- Disponibilidad y accesibilidad de los datos, con el objetivo de su explotación para actividades de analítica, medición y seguimiento de procesos.

2. REQUERIMIENTOS

La herramienta deberá cumplir con los siguientes requerimientos funcionales y no funcionales.

Centro Ceibal se reserva el derecho de adjudicar total o parcialmente los módulos que deriven de la propuesta.

2.1. REQUERIMIENTOS OBLIGATORIOS GENERALES A TODO EL SISTEMA

- RG-1. Seguridad: deberá cumplirse con lo solicitado en el Anexo 5.6
- RG-2. La herramienta debe contar con la posibilidad de personalizar con los colores y logos corporativos
- RG-3. La herramienta deberá permitir la autenticación con Active Directory para la gestión dentro de la organización.
- RG-4. El sistema debe poder utilizarse en dispositivos móviles. El sistema se debe poder usar en estos dispositivos con una resolución y formato acorde al dispositivo que se está utilizando
- RG-5. Toda información se deberá poder exportar en formatos PDF y Excel como mínimo siendo todos los datos e información del sistema visualizados o convertibles a reportes exportables
- RG-6. En cada módulo del sistema se debe poder visualizar información contando con múltiples filtros de modo de poder segmentar la información que sea requerida.
- RG-7. El producto debe contar con servicios que permitan la interoperabilidad con los sistemas corporativos y de explotación de datos de Centro Ceibal (se entiende por esto, interoperabilidad vía servicios web, API, intercambio de archivos, bases de datos, entre otros).
- RG-8. Reportes y Dashboards: Toda la información se deberá poder visualizar en reportes y dashboards para la gestión eficaz y eficiente de servicios.
- RG-9. El producto propuesto debe contar con un plan de evolución continua que asegure su sustentabilidad en el tiempo (Roadmap).

2.2. REQUERIMIENTOS OBLIGATORIOS DE USABILIDAD

- RU-1. El sistema deberá utilizar escritura simple y breve, ya que los usuarios deben poder leer y saber interpretar rápidamente a dónde ir y qué hacer. Además las modificaciones deben ser fáciles de realizar.
- RU-2. La nomenclatura debe ser adaptable a la terminología de Ceibal, Ej. Centros Educativos, Beneficiarios, etc.
- RU-3. El sistema deberá cumplir con "Nivel A" de accesibilidad web (https://www.w3.org/WAI/WCAG21/quickref/?current_sidebar=%23col_customize&levels=aa%2Caaa).
- RU-4. El sistema deberá ser navegable e informar al usuario en todo momento sobre dónde se encuentra y en caso de errores, orientar al usuario a continuar con el uso del sistema.
- RU-5. El producto deberá contar con una interfaz de usuario de fácil uso e intuitiva que evite errores o dificultades en la experiencia de uso.
- RU-6. El sistema deberá ser de fácil adaptación y apropiación por parte del usuario tanto en la gestión del sistema como en el uso final.
- RU-7. El diseño y estética deberán ser sencillos de modo de facilitar la experiencia del usuario. Una acción concreta de un usuario no deberá exceder en promedio de 4 interacciones del usuario. Ver tabla 5.2.

2.3. REQUERIMIENTOS OBLIGATORIOS FUNCIONALES

2.3.1. Requerimientos obligatorios prioritarios a ser implementados dentro de este proyecto (fase 1)

El producto propuesto debe contar con las siguientes funcionalidades :

RFP-1. Gestión centralizada de la información de los contactos beneficiarios de la organización

La nueva plataforma de gestión debe permitir reflejar la siguiente información:

- ◆ Información de nuestros beneficiarios, la cual es actualizada diariamente por procesos automatizados de cargas masivas con datos provenientes de los

subsistemas educativos (Primaria, Secundaria, UTU y Formación Docente).

Algunos de los datos sincronizados son:

- Datos personales generales (nombre completo, fecha de nacimiento, nacionalidad, edad, género, sexo, documento de identidad, dirección, teléfonos de contacto, etc).
- Datos de pertenencia a uno o más centros educativos con su rol (docente, estudiante, funcionario, etc) por año lectivo, generando datos históricos.
- Datos de grupos y grado a los que pertenece por año lectivo.
- ◆ Información de los Centros Educativos, ubicación geográfica y relación/es con las personas beneficiarias (con uno o más roles bien identificados) e infraestructura (instalaciones de conectividad, dispositivos, laboratorios de informática, etc.).
- ◆ Se requiere contar con la posibilidad de agregar atributos adicionales y personalizados en las entidades principales como ser Centros Educativos y Beneficiarios.
- ◆ Se requiere contar con funcionalidades de gestión de datos maestros, como ser productos, tipos de casos, casos, etc.
- ◆ Programas y Productos educativos: Ceibal cuenta con sistemas de registración con información relevante para la segmentación, por lo que es requerido contar con servicios y estructuras de datos que nos permitan reflejar dicha información en la herramienta tanto en los beneficiarios persona como en los centros educativos. Ej. Participación en eventos, cursos, proyectos, etc.

RFP-2. Matriz de Beneficios: Posibilidad de registro de los beneficios definidos y otorgados por Ceibal para cada persona beneficiaria y/o centros educativos. La matriz de beneficios se basa en una serie de lineamientos definidos por la organización, los cuales determinan de manera clara y estructurada a quiénes corresponden los diferentes beneficios (productos, programas y servicios) ofrecidos.

Esta herramienta permite determinar para cada beneficiario los productos, programas y servicios de acuerdo con criterios preestablecidos. Contar con esta información en el CRM facilita la atención al usuario.

RFP-3. Segmentación de la información: Posibilidad de clasificar a la persona beneficiaria y/o centro educativo en diferentes grupos según criterios específicos (como demografía, geografía, uso de determinados productos, servicios y/o programas, o ciclo educativo), con el objetivo de personalizar las estrategias de comunicación y campañas. En este sentido se debe tener en cuenta que un beneficiario o centro educativo podrá pertenecer a varias categorías o segmentos dependiendo de inscripciones o participación a diferentes propuestas educativas. La segmentación debe permitir múltiples clasificaciones con criterios estáticos y dinámicos, tanto en función de los datos maestros de las personas, como del historial de interacciones con Ceibal, resultado de interacciones y campañas, estados de incidentes y reclamos, y cualquier otro dato disponible en el CRM o importado de datos externos.

RFP-4. Gestión de casos de atención al usuario: Se debe contar con registro de cada interacción con los beneficiarios y centros educativos sin importar el medio por el que se contacta ej. correo electrónico, llamada telefónica, chatbot, redes sociales. Toda interacción generada en torno a un caso debe quedar asociada al mismo (único ticket) independientemente del nivel de atención donde se genere y del canal empleado por el beneficiario.

RFP-5. Historial de Interacciones: La herramienta debe contar con historial de cada interacción (comunicaciones tanto entrantes como salientes) con el beneficiario, ya sea a través de correos electrónicos, llamadas telefónicas u otros medios, lo que proporcionará un contexto valioso para futuras comunicaciones

RFP-6. Gestión de entregas de equipos, licencias de Software, etc: La herramienta debe permitir registrar toda entrega que se le realice a un beneficiario o a un centro educativo. La herramienta debe guardar toda la información histórica de entregas, pendientes de devolución, devoluciones, préstamos, etc., pudiendo contar con la información detallada que nos permita brindar soporte.

En este punto es requerido que mediante servicios (APIs, WebServices), quede el registro de las entregas realizadas a nuestros beneficiarios (personas y centros) que son gestionadas por el sistema de asignación de equipos existente en Ceibal.

La herramienta debe contar además con la posibilidad de registración interactiva de esta misma información.

- RFP-7.** Se requiere contar con la posibilidad de realizar flujos de trabajo con notificaciones automáticas para la gestión de procesos que pueden requerir la actuación de diversas áreas operativas y educativas de la organización. Estas actuaciones deben contar con registro de tiempos de respuesta de cada área actuante de modo que permita analizar Niveles de Servicio (SLA).
- RFP-8.** Gestión del servicio: La herramienta debe proporcionar la información para poder determinar responsabilidades (asignación de casos por grupos de responsables) y tiempos de actuación previamente establecidos (SLA) para todos los casos registrados de cualquiera de los servicios, incluyendo la gestión de alertas internas y notificaciones (tracking) al beneficiario..
- RFP-9.** Gestión de formularios : La herramienta debe contar con funcionalidades que permitan recolectar información mediante formularios quedando la información generada en estructuras de datos dentro de la base de datos de la propia plataforma.
- RFP-10.** Integración con sistemas de registros y gestión que Ceibal utiliza hoy día: La herramienta debe contar con mecanismos que permitan la comunicación entre sistemas. Es un requerimiento obligatorio que se cuente con APIs, y/o Web Services (WS) que permitan conectar la información (tanto como entrada como salida) con otros sistemas.
- RFP-11.** El proyecto de implantación fase 1 deberá considerar integración con canales de comunicación (Chatbot en Whatsapp , Chatbot Web, , SMS, llamadas y correo electrónico). y plataformas de gestión de canales (Inconcert, central telefónica)
- RFP-12.** Así mismo el proyecto de implantación en fase 1 deberá considerar desarrollos o adecuaciones de servicios para la correcta integración con sistemas desarrollados para la gestión de órdenes de trabajo (ej: reparaciones, entregas) así como interacciones con procesos desarrollados en BPMS como por ej: inscripciones a cursos y emisión de constancias, etc.
- RFP-13.** Gestión de Campañas:Selección (usando la segmentación de la información) de destinatarios, elaboración de correos electrónicos personalizados, trazabilidad en el seguimiento de enlaces individualizados, registro individual de los resultados de la campaña e interacciones posteriores relacionadas, indicadores para evaluar la campaña, segmentación para segundo envío en función de los resultados.

RFP-14. Gestión Omnicanal de comunicaciones: Posibilidad de gestión, envío y registro de comunicaciones. Será necesario gestionar de forma centralizada todos los puntos de contacto de comunicación (saliente y entrante) ya sea a través de Mails, SMS, Whatsapp o similares. Allí es importante visualizar la cantidad de mensajes recibidos por los usuarios según los distintos medios, constatar las suscripciones y desuscripciones de los usuarios. Tener la posibilidad de realizar envíos de Mails, SMS y/o Whatsapp a través de la plataforma o que la misma permita una integración con servicios de envíos de este tipo.

RFP-15. La herramienta deberá contar con la posibilidad de desarrollar Chatbots de atención como parte del sistema Omnicanal de comunicación con los usuarios, mediante sistema ITR y con uso de Inteligencia artificial.

2.3.2. Requerimientos obligatorios a ser implementados en un mediano plazo (fase 2).

Los requerimientos listados a continuación son aquellos con los que el producto ofrecido debe contar pero que serán implementados a futuro y no como prioritarios:

RFS-1. Audiencias Publicitarias: La herramienta deberá permitir la generación, gestión y conexión de audiencias con medios externos de publicidad digital. Posibilidad de generar clusters de audiencias dentro del CRM que a través de la integración con medios digitales permita la generación de campañas de marketing digital. Siempre y cuando dicha información se encuentre protegida al amparo de la normativa vigente.

RFS-2. Gestión de instalaciones de conectividad en centros educativos: Nuestra organización realiza tanto instalación como soporte de la conectividad en cada centro educativo del país por lo que se requiere contar con la posibilidad de registro de casos de instalaciones con información técnica de dicha instalación así como también el registro histórico de actuaciones posteriores de soporte y visitas de técnicos. Actualmente para cubrir esta necesidad se realizó un desarrollo a medida con interfases con el CRM y el ERP (gestión de stocks). Es requerido que la nueva plataforma pueda gestionar todo el proceso de instalación y soporte posterior.

RFS-3. Reparaciones: Nuestra organización cuenta con el servicio de reparación tanto de los dispositivos. Es requerido para esta fase del proyecto poder resolver toda la funcionalidad de registración de la actividad de reparación, controles que correspondan, y registración de los repuestos consumidos tanto en CRM como en ERP.

RFS-4. Portal de Autogestión: Se deberá contar con un Portal de acceso por parte de los beneficiarios que les permita hacer seguimiento de un caso reportado y contar con la posibilidad de agregar información. El acceso para cada persona beneficiaria deberá realizarse autenticado con el actual Login Unificado para estudiantes y docentes, basado en el protocolo CAS. Se deberá además contar con gestión de preferencias de comunicación/ suscripciones.:Se requiere que el beneficiario pueda suscribirse o desuscribirse para diferentes categorías de comunicados con Ceibal.

Todos los requerimientos deben ser considerados en la propuesta. No serán evaluadas las propuestas que no cumplan con el 100% de los requerimientos obligatorios.

2.4. Requerimiento Deseable no excluyente

RD-1. Para brindar soporte sería deseable poder contar con herramienta de videollamada con el usuario.

Escala de Calificación de los requerimientos funcionales de la solución:

Los requerimientos deberán ser clasificados según la siguiente escala (esta clasificación deberá incluirse en la Tabla de cumplimiento de requerimientos del anexo 6):

- 4 Funcionalidad que provee el sistema sin necesidad de desarrollos o ajustes adicionales
- 3 Funcionalidad parcialmente suministrada y puede ser complementada a través de personalizaciones del mismo sistema

- 2 Funcionalidad que no posee el sistema pero puede ser suministrada sin costos adicionales
- 1 Funcionalidad que no posee el sistema pero que puede ser suministrada a un costo adicional
- 0 Funcionalidad que no posee el sistema y la cual no será complementada por el proveedor

3. IMPLANTACIÓN DE LA SOLUCIÓN

El oferente deberá considerar todas las actividades relativas a la puesta en marcha de la solución propuesta, entre ellas la migración de la información existente en sistemas actuales y configuraciones requeridas para el cumplimiento de los requerimientos expuestos en el punto anterior.

La propuesta deberá incluir obligatoriamente:

- Estrategia de implantación y metodología de trabajo propuesta que contemple la continuidad del negocio por el periodo que dure el proyecto de implementación. Se valorará la presentación de estrategias que contemplen la ejecución del proyecto de implantación con base en metodologías ágiles de trabajo y tomando en cuenta el impacto de cada cambio en la operación de Ceibal.
- Actividades, responsabilidades y dedicación que correspondan para las partes.
- Cronograma a alto nivel incluyendo los hitos principales.
- Estrategia de capacitaciones a usuarios finales y transferencia de conocimientos a los administradores del sistema. Las mismas deben incluir capacitación a proveedores mediante el diseño de materiales gráficos (videos, guías, entre otros).
- Estrategia de gestión del cambio incluyendo consultor que apoye las actividades.

- Estrategia de migración de datos del sistema anterior al sistema propuesto según alcance definido por Centro Ceibal. Se debe considerar en dicho plan el plan de limpieza de datos y control de la calidad de datos previo a la migración

DOCUMENTACIÓN REQUERIDA PARA EL PROYECTO

Es requerido contar con un Plan de Trabajo que incluya como mínimo:

- Plan de Comunicación de Proyecto
- Riesgos identificados con su plan de mitigación
- Plan de Calidad y Testing
- Cronograma detallado de proyecto que incluya detalle de entregables/hitos
- Plan de actividades orientadas a la gestión del cambio en la organización
- Plan de transferencia de conocimiento a administradores del sistema y de sustentabilidad a funcionales y técnicos
- Plan de Capacitación a usuarios finales
- Plan de Despliegue

DOCUMENTACIÓN REQUERIDA DEL PRODUCTO AL FINALIZAR LA

IMPLANTACIÓN:

Como parte de los entregables del proyecto se deberá considerar la siguiente documentación como mínimo:

- Documentación técnica de la solución
- Documentación de Arquitectura de la solución

- Documentación de desarrollos adicionales que sean identificados en el proyecto
- Manuales de usuarios en español y actualizados.

Debe considerarse en la propuesta que se deberá contar con un ambiente de pruebas y un ambiente productivo de forma permanente.

El ambiente de pruebas quedará disponible luego de la implantación definitiva de modo de contar con este para futuros cambios y pruebas.

4. MANTENIMIENTO DE LA SOLUCIÓN

La oferta debe detallar el alcance del servicio de soporte tanto correctivo como evolutivo de la solución propuesta.

4.1. SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA SOLUCIÓN

El servicio de soporte correctivo se entiende por el soporte referido a la solución de errores o incidentes reportados en ambiente productivo.

El mantenimiento evolutivo del producto se entenderá incluido en el costo del licenciamiento o del soporte y mantenimiento de la solución quedando a disposición de Centro Ceibal la posibilidad de actualizar la versión siempre que así lo considere oportuno.

4.2. MANTENIMIENTO EVOLUTIVO PERSONALIZADO

El oferente deberá cotizar valor unitario hora de desarrollos específicos para cambios o personalizaciones a demanda por Ceibal.

Las horas de desarrollo serán demandadas en caso que Centro Ceibal requieran ajustes no incluidos en el proyecto de implantación, personalizaciones con un tope de contrato de hasta 3.000 horas,

Se utilizará una herramienta de gestión provista por Centro Ceibal para el seguimiento de incidentes, donde se realizará el control de horas. Las horas consumidas no pueden superar la estimación aprobada, salvo razones fundadas con aprobación del Centro Ceibal.

5. DIMENSIONAMIENTO

5.1. Licenciamiento

El esquema de licenciamiento dependerá de la configuración del sistema y los diferentes tipos de usuarios que harán uso del mismo.

Por tanto, Ceibal pretende una propuesta de compra escalonada de usuarios año a año, a medida de que implementen las diferentes fases ya descritas, las cuales requerirán incrementar la cantidad de usuarios que utilizarán el sistema.

Para el año 1, Ceibal estima una participación de hasta 100 usuarios del sistema, considerando que estaremos en período de implantación.

En caso de que para el sistema propuesto, el costo variase según el tipo o rol de usuario, el oferente deberá presentar cotización desglosada por cada tipo o rol en base a un sistema de escalonamiento por cantidad de usuarios (ej. hasta 100 usuarios, hasta 200 usuarios, hasta 500 usuarios, más de 500 usuarios).

Para el proceso de evaluación económica, Ceibal estimará el costo de licenciamiento total por el período completo de años a contratar. Para lograr este cometido el oferente deberá cotizar de forma escalonada para cubrir las cantidades de usuarios según el siguiente cuadro especificando tipos de usuarios requeridos para cubrir las funciones detalladas en el cuadro a continuación. De esta manera Ceibal podrá dimensionar los costos futuros según el período a contratar.

Se espera que el oferente asocie los diferentes roles para cubrir las funciones con los diferentes tipos de usuarios del producto ofrecido. Estos tipos de usuario serán los que se prestarán descritos en el cuadro de oferta económica.

Funciones a Cubrir	Cantidades		
	Año 1	Año 2	Año 3 al 5

Super usuario	5	5	5
Atención al usuario	10	20	40
Administradores	5	10	15
Gestión de casos	10	20	50
Gestión de asignación de productos (entregas e instalaciones)	10	20	20
Usuarios transaccionales (interoperabilidad)	30	60	100
Gestión de formularios	10	20	30
Comunicaciones con beneficiarios (canales)	10	20	30
Marketing / Campañas	10	10	10
Consulta	50	100	150

5.2. Datos de uso

Como referencia de dimensionamiento, se comparten algunos datos del año 2023:

1. Cantidad de usuarios activos: **450**
2. Cantidad de usuarios que acceden de forma mensual (promedio): **260**
3. Cantidad de beneficiarios persona: **750.000**
4. Cantidad de Locales educativos: **4.000**
5. Cantidad de casos en un año: **1.300.000**.

2 CARACTERÍSTICAS DEL SERVICIO

2.1

FORMA DE TRABAJO

Los servicios podrán ser prestados en forma remota, así como in situ en las oficinas de Centro Ceibal. El oferente deberá tener representación en Uruguay y se deberá disponer con personal técnico y de gestión en las oficinas de Ceibal al menos un 30% de horas totales del proyecto.

Centro Ceibal se reserva el derecho de solicitar la presencia física de los implementadores en fases críticas del proyecto si así lo considera necesario para el éxito del mismo.

Se entiende que todo producto/entregable deberá testearse de forma fiable, en base al criterio de aceptación acordado. Los errores encontrados, deberán solucionarse a costo asumido por el proveedor.

El oferente debe establecer un período no menor a 12 meses de garantía post implementación en producción.

3 OFERTA

3.1

MODALIDAD DE COTIZACIÓN

El oferente deberá cotizar según el siguiente cuadro:

Cotización¹	
	Completar todas las celdas en blanco
	Costo (imp. incl.)
ITEM 1- Implantación de la solución - Requerimientos fase 1	
ITEM 2 -Implantación de la solución - Requerimientos fase 2 (
Total Implantación :	
ITEM 3 -Licenciamiento Anual² (cotización por tipo de usuario y cantidad)	<ul style="list-style-type: none">• Tipo 1: hasta 100 usuarios• Tipo 1: hasta 200 usuarios• Tipo 1: hasta 500 usuarios• Tipo 1: más de 500 usuarios• Tipo 2: hasta 100 usuarios• Tipo 2: hasta 200 usuarios• Tipo 2: hasta 500 usuarios• Tipo 2: más de 500 usuarios• Etc.
ITEM 4 - Mantenimiento de la solución	
ITEM 4.1 - Servicio de soporte y mantenimiento (costo anual³) (si correspondiese)	

¹ Se podrá cotizar en moneda local o extranjera, haciendo la aclaración pertinente en cada campo, impuestos incluidos.

² Se debe cotizar obligatoriamente considerando un lapso de 5 años
Detallar en caso que se requiera más de un tipo de licenciamiento para contar con los perfiles requeridos según lo especificado en el llamado.

³ Se debe cotizar obligatoriamente considerando un lapso de 5 años

ITEM 4.2 - Mant. Evolutivo Personalizado: Cotizar valor⁴ hora de desarrollo (hasta 3.000 horas a lo largo del período del contrato)	
Otros costos (si corresponde) - especificar	(si corresponde)

CENTRO CEIBAL se reserva el derecho de adjudicar a la o las ofertas que considere más convenientes para sus intereses y a las necesidades del objeto de la compra, estando facultada para: adjudicar al proponente que reúna las mejores condiciones; no adjudicar algún o ningún ítem; dividir la adjudicación, adjudicar menor cantidad a la solicitada.

3.2

PRESENTACIÓN DE LA OFERTA

La oferta debe incluir en forma obligatoria los siguientes elementos:

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

a. El oferente deberá tener al menos 4 implantaciones exitosas de la solución propuesta en empresas de similar porte que Ceibal en los últimos 4 años.

b. El oferente deberá presentar carta de recomendación, licitaciones similares adjudicadas y datos de contacto específicos de los clientes para corroboración de antecedentes. (Deberá presentarse de acuerdo al Anexo 1 punto 5.1)

En caso que el oferente se presente en forma de consorcio o subcontratista se considerarán los antecedentes en forma conjunta.

✓ Propuesta Técnica-Funcional, deberá presentar de forma obligatoria:

a. Tabla completada de requerimientos, de acuerdo al Anexo 1 punto 5.2.

⁴ El horario sería de oficina: lunes a viernes (excepto feriados no laborables) de 9:00 a 17:00hs, hora local Uruguay. Cotización que contemple todos los roles: tanto en modalidad remota como in situ.

b. Propuesta con plan de trabajo incluyendo, supuestos, equipo del proyecto, metodología de trabajo, responsabilidades, cronograma a alto nivel, estrategia de implantación, plan de capacitación y de migración de datos.

c. Demo y acceso al producto: Como parte de la presentación de la oferta se coordinará una demo específica para Centro Ceibal en la que deberá presentar todas las funcionalidades definidas a continuación. Asimismo el oferente debe habilitar el acceso temporal al producto para realizar pruebas por parte de Centro Ceibal como parte de la evaluación técnica. Centro Ceibal podrá excluir de la evaluación (descalificar), aquellos productos que no cumplan con los requisitos establecidos.

En la demo se solicitará se muestren los siguientes casos de uso:

1. Registrar información de un beneficiario tal como se expresa en los requerimientos obligatorios y agregar dos atributos customizados.
2. Registrar la entrega de un dispositivo a un beneficiario o centro educativo.
3. Realizar una simulación de campaña segmentando la información por docentes de un solo grado.
4. Registración de un caso de consulta, a ser derivado a un grupo responsable para su solución.

✓ Tabla de Equipo de trabajo propuesto, (Deberá presentarse de acuerdo al Anexo 1 punto 5

✓ .5)

✓ Oferta económica (Deberá presentarse de acuerdo a la sección 3.1 - Modalidad de cotización)

✓ Tabla de Cumplimiento de SLA deberá presentarse de acuerdo Anexo 1 punto 5.4

✓ Tablas de Cumplimiento de requisitos de Seguridad y Privacidad deberá presentarse de acuerdo al Anexo 1 punto 5.6

3.3

EVALUACIÓN

El criterio de evaluación técnica de los oferentes será en base al cumplimiento de las especificaciones obligatorias detalladas en el punto 3.2 – Presentación de la Oferta. Se procederá a estudiar la oferta económica de aquellas propuestas que hayan superado el 60% de los puntos totales correspondientes a la evaluación técnica.

Evaluación	
	% Evaluación máximo
Antecedentes	10
Equipo de proyecto	10
DEMO	20
Propuesta técnica-funcional	20
Oferta económica	40
TOTAL	100

4 PROPIEDAD INTELECTUAL

Todos los trabajos a medida y la documentación 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. Se excluye el material y desarrollo preexistente del proveedor.

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 1

5.1

PRESENTACIÓN DE ANTECEDENTES

Ordenar del más reciente al más antiguo. Se valorarán sólo antecedentes de los últimos 4 años.

Tabla

N° proyecto	Nombre del proyecto	Institución contratante	Contacto responsable de dicha institución /proyecto, cargo, teléfono, email	Descripción y alcance del proyecto Cantidad de Usuarios	Horas dedicadas en total	Producto implantado y Fecha de implantado en producción	Hipervínculo a la carta de recomendación (obligatorio)

5.2 REQUERIMIENTOS

TABLA DE CUMPLIMIENTO DE

Se deberá completar la tabla para todos los requerimientos detallados en el punto 2 de este documento.

Con el objetivo de facilitar y clarificar codificamos los requerimientos con la siguiente nomenclatura:

RFP = Requerimientos obligatorios Prioritarios (Fase 1)

RFS = Requerimientos obligaciones Secundarios (Fase 2)

RG = Requerimientos Generales del sistema

RU = Requerimientos de usabilidad del sistema

RD = Requerimientos Deseables

Requerimientos obligatorios a ser implementados dentro de este proyecto (fase 1)			
REQUERIMIENTOS		Clasificación según valores de tabla ⁵	OBSERVACIONES
Nro	Descripción breve		
RFP1	Gestión centralizada de la información de los contactos beneficiarios de la organización		

⁵ 4 - Funcionalidad que provee el sistema sin necesidad de desarrollos o ajustes adicionales

3 - Funcionalidad parcialmente suministrada y puede ser complementada a través de personalizaciones del mismo sistema

2 -Funcionalidad que no posee el sistema pero puede ser suministrada sin costos adicionales

1 -Funcionalidad que no posee el sistema pero que puede ser suministrada a un costo adicional

0 -Funcionalidad que no posee el sistema y la cual no será complementada por el proveedor

RFP2	Matriz de Beneficios: Posibilidad de registro de los beneficios definidos y otorgados por Ceibal para cada persona beneficiaria y/o centros educativos		
RFP3	Segmentación de la información: Posibilidad de clasificar a la persona beneficiaria y/o centro educativo en diferentes grupos según criterios específicos con el objetivo de personalizar las estrategias de comunicación y campañas		
RFP4	Gestión de casos de atención al usuario: Se debe contar con registro de cada interacción con los beneficiarios y centros educativos sin importar el medio por el que se contacta ej. correo electrónico, llamada telefónica, chatbot, redes sociales		
RFP5	Historial de Interacciones: La herramienta debe contar con historial de cada interacción (comunicaciones tanto		

	entrantes como salientes) con el beneficiario		
RFP6	Gestión de entregas de equipos, licencias de Software, etc: La herramienta debe permitir registrar toda entrega que se le realice a un beneficiario o a un centro educativo.		
RFP7	Se requiere contar con la posibilidad de realizar flujos de trabajo con notificaciones automáticas para la gestión de procesos que pueden requerir la actuación de diversas áreas operativas y educativas de la organización		
RFP8	Gestión del servicio: La herramienta debe proporcionar la información para poder determinar responsabilidades (asignación de casos por grupos de responsables) y tiempos de actuación previamente establecidos (SLA) para todos los casos registrados de cualquiera de los		

	servicios, incluyendo la gestión de alertas internas y notificaciones (tracking) al beneficiario.		
RFP9	Gestión de formularios : La herramienta debe contar con funcionalidades que permitan recolectar información mediante formularios quedando la información generada en estructuras de datos dentro de la base de datos de la propia plataforma		
RFP10	Integración con sistemas de registros y gestión que Ceibal utiliza hoy día: La herramienta debe contar con mecanismos que permitan la comunicación entre sistemas. Es un requerimiento obligatorio que se cuente con APIs, y/o Web Services (WS) que permitan conectar la información (tanto como entrada como salida) con otros sistemas		

RPF11	Integración con canales de comunicación (Chatbot en Whatsapp , Chatbot Web, , SMS, llamadas y correo electrónico). y plataformas de gestión de canales (Inconcert, central telefónica)		
RPF12	Desarrollos o adecuaciones de servicios para la correcta integración con sistemas desarrollados para la gestión de órdenes de trabajo (ej: reparaciones, entregas) así como interacciones con procesos desarrollados en BPMS como por ej: inscripciones a cursos y emisión de constancias, etc.		
RPF13	Gestión de Campañas: Selección (usando la segmentación de la información) de destinatarios, elaboración de correos electrónicos personalizados, trazabilidad en el seguimiento de enlaces individualizados,		

	registro individual de los resultados de la campaña e interacciones posteriores relacionadas, indicadores para evaluar la campaña, segmentación para segundo envío en función de los resultados.		
RPF14	Gestión Omnicanal de comunicaciones: Posibilidad de gestión, envío y registro de comunicaciones. Será necesario gestionar de forma centralizada todos los puntos de contacto de comunicación (saliente y entrante) ya sea a través de Mails, SMS, Whatsapp o similares		
RPF15	Posibilidad de desarrollar Chatbots de atención como parte del sistema Omnicanal de comunicación con los usuarios, mediante sistema ITR y con uso de Inteligencia artificial.		

Requerimientos obligatorios a ser implementados dentro de este proyecto (fase 2)

REQUERIMIENTOS		Clasificación según valores de tabla ⁶	OBSERVACIONES
Nro	Descripción Breve		
RFS1	Audiencias Publicitarias: La herramienta deberá permitir la generación, gestión y conexión de audiencias con medios externos de publicidad digital. Posibilidad de generar clusters de audiencias dentro del CRM que a través de la integración con medios digitales permita la generación de campañas de marketing digital. Siempre y cuando dicha información se encuentre protegida al amparo de la normativa vigente		
RFS2	Gestión de Instalaciones de conectividad en centros educativos: Nuestra organización		

⁶ 4 - Funcionalidad que provee el sistema sin necesidad de desarrollos o ajustes adicionales

3 - Funcionalidad parcialmente suministrada y puede ser complementada a través de personalizaciones del mismo sistema

2 -Funcionalidad que no posee el sistema pero puede ser suministrada sin costos adicionales

1 -Funcionalidad que no posee el sistema pero que puede ser suministrada a un costo adicional

0 -Funcionalidad que no posee el sistema y la cual no será complementada por el proveedor

	<p>realiza tanto instalación como soporte de la conectividad en cada centro educativo del país por lo que se requiere contar con la posibilidad de registro de casos de instalaciones con información técnica de dicha instalación así como también el registro histórico de actuaciones posteriores de soporte y visitas de técnicos. Actualmente para cubrir esta necesidad se realizó un desarrollo a medida con interfases con el CRM y el ERP (gestión de stocks). Es requerido que la nueva plataforma pueda gestionar todo el proceso de instalación y soporte posterior.</p>		
RFS3	<p>Reparaciones: Nuestra organización cuenta con el servicio de reparación tanto de los dispositivos. Es requerido para esta fase del proyecto poder resolver toda la funcionalidad de registración de la actividad de reparación, controles que correspondan, y registración de los repuestos consumidos</p>		

	tanto en CRM como en ERP.		
RFS4	Portal de Autogestión: Se deberá contar con un Portal de acceso por parte de los beneficiarios que les permita hacer seguimiento de un caso reportado y contar con la posibilidad de agregar información. El acceso para cada persona beneficiaria deberá realizarse autenticado con el actual Login Unificado para estudiantes y docentes, basado en el protocolo CAS. Se deberá además contar con gestión de preferencias de comunicación/ suscripciones.:Se requiere que el beneficiario pueda suscribirse o desuscribirse para diferentes categorías de comunicados con Ceibal.		
Generales al sistema			
	REQUERIMIENTOS		OBSERVACIONES

Nro	Descripción breve	Clasificación según valores de tabla ⁷	
RG1	Seguridad: deberá cumplirse con lo solicitado en el Anexo 5.6.		
RG2	La herramienta debe contar con la posibilidad de personalizar con los colores y logos corporativos		
RG3	La herramienta deberá permitir la autenticación con Active Directory para la gestión dentro de la organización.		
RG4	El sistema debe poder utilizarse en dispositivos móviles. El sistema se debe poder usar en estos dispositivos con una resolución y formato acorde al dispositivo que se está utilizando		

⁷ 4 - Funcionalidad que provee el sistema sin necesidad de desarrollos o ajustes adicionales
3 - Funcionalidad parcialmente suministrada y puede ser complementada a través de personalizaciones del mismo sistema
2 - Funcionalidad que no posee el sistema pero puede ser suministrada sin costos adicionales
1 - Funcionalidad que no posee el sistema pero que puede ser suministrada a un costo adicional
0 - Funcionalidad que no posee el sistema y la cual no será complementada por el proveedor

RG5	Toda información se deberá poder exportar en formatos PDF y Excel como mínimo siendo todos los datos e información del sistema visualizados o convertibles a reportes exportables		
RG6	En cada módulo del sistema se debe poder visualizar información contando con múltiples filtros de modo de poder segmentar la información que sea requerida		
RG7	El producto debe contar con servicios que permitan la interoperabilidad con los sistemas corporativos y de explotación de datos de Centro Ceibal (se entiende por esto, interoperabilidad vía servicios web, API, intercambio de archivos, bases de datos, entre otros).		
RG8	Reportes y Dashboards: Toda la información se deberá poder visualizar en reportes y dashboards para la gestión eficaz y eficiente de servicios		

RG9	El producto propuesto debe contar con un plan de evolución continua que asegure su sustentabilidad en el tiempo (Roadmap).		
Usabilidad			
REQUERIMIENTOS		Clasificación según valores de tabla ⁸	OBSERVACIONES
Nro	Descripción Breve		
RU1	El sistema deberá utilizar escritura simple y breve, ya que los usuarios deben poder leer y saber interpretar rápidamente a dónde ir y qué hacer. Además las modificaciones deben ser fáciles de realizar.		
RU2	La nomenclatura debe ser adaptable a la terminología de Ceibal,		

⁸ 4 - Funcionalidad que provee el sistema sin necesidad de desarrollos o ajustes adicionales
3 - Funcionalidad parcialmente suministrada y puede ser complementada a través de personalizaciones del mismo sistema
2 -Funcionalidad que no posee el sistema pero puede ser suministrada sin costos adicionales
1 -Funcionalidad que no posee el sistema pero que puede ser suministrada a un costo adicional
0 -Funcionalidad que no posee el sistema y la cual no será complementada por el proveedor

	Ej. Centros Educativos, Beneficiarios, etc.		
RU3	El sistema deberá cumplir con "Nivel A" de accesibilidad web (https://www.w3.org/WAI/WCAG21/quickref/?currentsidebar=%23col_customize&levels=aa%2Caaa).		
RU4	El sistema deberá ser navegable e informar al usuario en todo momento sobre dónde se encuentra y en caso de errores, orientar al usuario a continuar con el uso del sistema.		
RU5	El producto deberá contar con una interfaz de usuario de fácil uso e intuitiva que evite errores o dificultades en la experiencia de uso.		
RU6	El sistema deberá ser de fácil adaptación y apropiación por parte del usuario tanto en la gestión del sistema como en el uso final.		

RU7	El diseño y estética deberán ser sencillos de modo de facilitar la experiencia del usuario. Una acción concreta de un usuario no deberá exceder en promedio de 4 interacciones del usuario.		
Deseables			
.RD1	Para brindar soporte sería deseable poder contar con herramienta de videollamada con el usuario.		

5.3

ACUERDOS DE CALIDAD DEL SERVICIO

5.3.1

Calidad del Servicio

El oferente será responsable de realizar todas las actividades que considere pertinentes para garantizar el funcionamiento correcto de la solución aplicativa propuesta, tanto en requerimientos funcionales como no funcionales definidos.

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 que hubieran podido ser detectados durante el proceso de testing del proveedor, deberá ejecutarse nuevamente el ciclo de pruebas diseñado sin costo extra.

5.3.2

Acuerdos de nivel de Servicio

Se establecerán 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 a continuación.

5.3.2.1

Parámetros de evaluación

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

- Cumplimiento de plazos acordados: Refiere a la ejecución de las distintas fases dentro de los plazos establecidos, así como las fechas acordadas en instancias de estimación e intercambio entre Ceibal y el proveedor.
- Seguimiento de pendientes: Se espera un intercambio fluido/acorde en base a los incidentes reportados y/o solicitudes de otra índole, así como la apropiación en la gestión de los mismos alineándose en base a las prioridades con Ceibal.
- Notificación oportuna de posibles retrasos: En consideración con las necesidades del negocio, los eventuales retrasos que se vayan previendo deberán ser notificados de forma inmediata, que permita a Ceibal gestionar el riesgo e impacto.

2. Calidad del servicio recibido: se busca medir si el 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:

- Calidad de la solución: Se espera que las soluciones brindadas no presenten errores que afecten los objetivos y transacciones de los distintos procesos de negocio. En el caso de existir errores bloqueantes en cualquier ambiente (priorizando aquellos que se presenten en ambiente productivo), se espera una gestión eficiente de los mismos.
- Trabaja según los procedimientos acordados con Ceibal: Alineado a las pautas de desarrollo y seguridad provistas por Ceibal.
- Calidad de la documentación provista: Ceibal proporcionará templates de documentación técnica, funcional, análisis y diseño, etc. Se espera que la documentación sea autocontenida y exhaustiva.
- Idoneidad del personal clave: Se espera que los miembros del equipo de trabajo cuenten con el expertise esperado, así como buena predisposición a la hora de emprender su labor.
- Seguridad, mantenibilidad, performance y usabilidad de la solución: se recomienda utilizar normas y estándares de seguridad OWASP. La solución deberá , de acuerdo a las reglas del negocio, ser performante y mantenible. Se espera además que se cumplan los estándares de usabilidad acordados en cada caso

3. Otros aspectos: se busca medir el grado de respuesta del proveedor en pro de satisfacer necesidades vinculadas con el servicio adquirido post producción. 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:

- Capacidad de trabajo: Se espera la comunicación temprana de aceptación / rechazo de trabajos de nuevas soluciones incluyendo en caso que corresponda, la justificación de dicho rechazo.
- Cumplimiento de garantías: Se evaluará el cumplimiento de garantías por parte de proveedor, en base a las líneas establecidas en el presente documento
- Coherencia de facturación: En base a las horas aprobadas y registradas en la herramienta provista por Ceibal.

El incumplimiento de los acuerdos del nivel de servicio o plazos comprometidos sobre cualquiera de los parámetros para cada fase o hito acordado con el Centro Ceibal, 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 que impacten de forma negativa sobre la continuidad del proyecto. En el caso de los errores bloqueantes en cualquier etapa, hito, sprint, ambiente: la tolerancia es cero.

Se considera una No conformidad cuando se incumplen los parámetros con mayor gravedad e impacto, cuando se acumulen 5 Reclamos, o ante otros incumplimientos a los términos acordados y obligaciones asumidas.

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.

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.

5.3.2.2 Penalización

El ingreso de una No conformidad podrá determinar la aplicación de una penalidad equivalente al 10% del precio acordado para esa fase, sprint o hito, 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.

5.4

SLA - NIVEL DE SERVICIO

Se debe cumplir con el siguiente SLA.

TIEMPO DE RESPUESTA

Incidentes en Producción

Urgencia del incidente	SLA (en horas)	Observaciones
Urgente	0,5 hs	Son aquellos incidentes ⁹ presentados en producción sobre la solución aplicativa que detienen o afectan la operación, colocando en riesgo la operativa de CEIBAL o el servicio brindado por CEIBAL a sus usuarios/beneficiarios
Alta	2 hs	Son aquellos incidentes presentados en producción sobre la solución aplicativa que no detienen la operación, pero sí impiden que algunos recursos cumplan con su función básica.
Media /Baja	4 hs	Son aquellos incidentes presentados en producción sobre la solución aplicativa que no impiden que cumpla con su función básica, pero sí les dificulta la operación.

⁹ Incidencias: corresponden a cualquier evento que cause una interrupción del servicio o una reducción de la calidad del mismo

Atención a pedido de servicio

Prioridad De la Solicitud	SLA (días hábiles)	Observaciones
Alta	2 días	Son aquellas solicitudes que por su naturaleza requieren una atención priorizada.
Media	5 días	Son aquellas solicitudes que por su naturaleza pueden ser atendidas a mediano plazo
Baja	8 días	Son aquellas solicitudes que por su naturaleza no forman parte del camino crítico por lo que pueden ser atendidas a largo plazo

TIEMPO DE RESOLUCIÓN

Las partes acordarán para cada incidente/solicitud el tiempo de solución del mismo.

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, de acuerdo al formato que otorgue Ceibal.

5.5

EQUIPO DE PROYECTO

El oferente deberá proponer el equipo de proyecto que entienda adecuado para dar cumplimiento a los servicios del que es objeto este llamado. Se deberá completar la tabla a continuación con la información para cada miembro del equipo propuesto.

Se evaluará el equipo de trabajo de acuerdo a su conformación, formación académica, experiencia en la implantación del producto propuesto y certificaciones presentadas. Los integrantes del equipo deben contar con experiencia en la implementación del producto propuesto y haber participado en al menos uno de los proyectos presentados como antecedentes de la empresa oferente.

Cualquier modificación en el equipo de trabajo deberá ser notificada previamente por escrito y su integración al equipo quedará sujeta a la aprobación de Centro Ceibal.

Asimismo se deberá notificar cuando dichos miembros se ausenten por licencias u otros motivos, en esos casos deberán presentar un backup que asumirá las funciones y responsabilidades

Rol	Descripción del Rol	Nombre y Apellido	Formación Académica	Experiencia relevante para el rol en el proyecto	Certificaciones
				Ej: Proyecto/ Cliente XX Rol: XX (fecha inicio - fecha fin)	

5.6 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. Podrá 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)
- 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 N° 18.331, de 11 de agosto de 2008 y Decreto N° 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 N° 18.331 y artículos 1 y 4 del Decreto N° 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. .
- Alojamiento de 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 el Reglamento General de Protección de Datos 2016/679, del Parlamento Europeo y del Consejo, modificatorias, concordantes y complementarias. 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 N° 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 Ceibal establezca.
- 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.

Matriz de cumplimiento de requerimientos de Seguridad de la Información

A completar por Ceibal		A completar por oferente		
Nº Req.	Requerimiento	Tipo	¿Acepto lo requerido? [SI/NO]	Observaciones (si corresponde)
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	Obligatorio		
13	Código malicioso	Obligatorio		
14	Lógica de negocio	Deseado		
15	Configuración	Obligatorio		
16	Certificaciones	Deseado		
17	Metodologías	Deseado		
18	Análisis de vulnerabilidades	Obligatorio		

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.

Requisitos de seguridad de la información y privacidad a ser tenidos en cuenta al momento de firmar el contrato con el proveedor adjudicado y la contratación de horas de consultoría y desarrollo.

Requisitos obligatorios

Estos requisitos son obligatorios para todos los llamados de compras de horas de servicio, a ser adquiridas por Centro Ceibal. Podrán haber excepciones que deberán estar justificadas y aprobadas por quien corresponda.

Cumplimiento de Políticas

Todo proveedor debe conocer el Manual de Políticas de Seguridad de la Información. (https://www.ceibal.edu.uy/wp-content/uploads/2023/02/38-30_Manual-de-politicas-de-Seguridad-de-la-informacion.pdf)

Acuerdo de confidencialidad

Se deberá incluir una cláusula de confidencialidad con el proveedor adjudicado que garantice la protección de la información de Ceibal.

Ejemplo de cláusula de confidencialidad:

El Proveedor se obliga a tratar la información a la que acceda de manera confidencial y únicamente en el marco del cumplimiento del presente contrato.

El término "Información Confidencial" incluye, sin que ello implique limitación toda información tangible o intangible de tipo cultural, técnico, económico, financiero, comercial,

estratégico o de cualquier otro tipo (sea de las Instituciones, servicios, alumnos, beneficiarios, centros educativos o terceros), incluyendo, pero no limitado a datos personales, que sea revelada, por cualquier medio, de forma oral, escrita, o en cualquier soporte.

La "Información Confidencial" no podrá ser revelada por el Proveedor a ningún tercero, sin el consentimiento previo y por escrito del Centro Ceibal.

En este contexto, el Proveedor se obliga a:

- (a) no revelar ninguna Información Confidencial a terceros, y no utilizarla en beneficio propio o de terceros ni aún luego de finalizado el contrato que las vincula;
- (b) adoptar precauciones razonables de seguridad para conservar en secreto la Información Confidencial de acuerdo con los lineamientos que establezca Ceibal;
- (c) no divulgar, reproducir, resumir ni distribuir Información Confidencial.

No quedará sujeta a la obligación de confidencialidad la información que:

- (a) sea o deviniera de dominio público sin responsabilidad ni intervención de las partes del presente convenio; y (b) fuera requerida por una autoridad competente y siempre que la parte se encontrara legalmente obligado a divulgarla. De todas formas, ante un eventual requerimiento de Información Confidencial, emanado del Poder Judicial o de cualquier autoridad reguladora, el Proveedor se obliga a notificar de inmediato al Centro Ceibal parte del requerimiento y remitirle sus antecedentes a fin de brindarle a la parte una oportunidad razonable para cuestionar, limitar y/o asistir en la forma de dicha divulgación.

Uso de la infraestructura del Centro Ceibal

En el caso que el servicio a contratar incluya el uso, instalación, configuración y/o mantenimiento de infraestructura de Ceibal tanto lógica como física, se deberán estipular claramente las condiciones, responsabilidades y usos adecuados de la información afectada de manera de asegurar la confidencialidad, integridad y disponibilidad de la misma. A tales efectos, se recomienda:

- Estipular claramente las responsabilidades y tareas que puedan quedar a cargo de los proveedores.
- Realizar una gestión adecuada de los usuarios generados a los proveedores. Esto debe incluir:
 - Información de las altas, bajas y modificaciones de los funcionarios de los proveedores por parte de estos en tiempo y forma, incluyendo los perfiles y roles a ser generados, de manera de garantizar un acceso seguro a los recursos de Ceibal.

- Generar los usuarios de VPNs y demás componentes necesarios para un acceso seguro, usando los criterios de mínimos privilegios.
- Coordinar con los proveedores, las medidas de seguridad a ser configuradas en la infraestructura de Ceibal, como ser listas blancas de IPs permitidas, conexiones de administración remota permitidos y aplicaciones habilitadas.
- Informar y acordar en conjunto con los proveedores las configuraciones de seguridad en servidores, estaciones, dispositivos de red y demás componentes tecnológicos a ser usados y/o administrados por los proveedores. Esto incluye entre otros el hardening de componentes y las configuraciones de logs y auditoría.
- Detallar claramente los esquemas de comunicación y gestión de incidentes que permitan asegurar la continuidad del negocio del Centro Ceibal, tomando en cuenta la criticidad de los activos gestionados.

Protección de la información manejada

La información sobre el Centro Ceibal manejada por el proveedor deberá cumplir con los requisitos establecidos en el Manual de Políticas de Seguridad de la Información. Para ello deberá cumplir con las medidas de seguridad que garanticen una confidencialidad, integridad y disponibilidad de la información tanto en reposo como en tránsito y en uso. En el caso que la información sea almacenada en servidores del proveedor ya sea en modalidad onpremise o en nubes, se deberán extremar los cuidados.

Protección de la información en reposo

La información en reposo deberá estar protegida de manera de garantizar la seguridad de la misma. De acuerdo al nivel de criticidad y sensibilidad de la información se podrán implementar distintos controles de seguridad. Se promueve:

- La encriptación a nivel de discos, dispositivos y/o base de datos.
- El uso de herramientas de DPL (data loss prevention) y CASB (cloud access security brokers).
- NO crear ni usar copias de la información, solamente en los casos que son necesarios.

- Cumplir con las distintas regulaciones en materia de protección de datos.

Protección de la información en tránsito

La información en tránsito deberá estar protegida, garantizando que no esté disponible para usuarios en general y no sea pasible de ataques de ciberseguridad como por ejemplo: "Man in the Middle";. Para ello se promueve:

- La encriptación para los datos en tránsito, por ejemplo al enviarlo como adjunto en un correo electrónico o un medio físico como un pendrive.
- El uso de SFTP en el caso de compartir información a través de servidores o transferencia gestionada de archivos a través de links encriptados seguros (con cifrado cifrado SSL y TLS).
- El uso de herramientas de DPL (data loss prevention) y CASB (cloud access security brokers).

Protección de la información en uso

La información en uso deberá estar protegido garantizando la confidencialidad, integridad y disponibilidad de la misma. Para ello se promueve:

- El uso adecuado de sistemas de gestión de identidades que permitan una correcta autenticación de usuarios en los sistemas del proveedor que incluyan por ejemplo: uso de políticas de contraseñas adecuadas, doble factor de autenticación para cuentas privilegiadas y otras medidas habituales para asegurar la identidad de los usuarios con acceso a la información.
- El uso de sistemas de autorización de usuarios adecuados que garanticen que los usuarios con los perfiles y roles correctos puedan acceder a la información para la cual tienen los privilegios necesarios.
- La aplicación de políticas, procesos y controles tecnológicos que garanticen la seguridad de la información en uso.

Concientización y capacitación del personal

El personal del proveedor deberá estar informado y concientizado con el objetivo de gestionar de manera segura la información que manejen del Centro Ceibal y dar un adecuado tratamiento a posibles incidentes de seguridad. Para ello se recomienda:

- Capacitar y concientizar al personal en temas relacionados a la seguridad de la información y la privacidad.
- Informar al personal de los canales y procesos adecuados para poder reportar eventos de seguridad en Ceibal.
- Concientizar al personal en la correcta aplicación de los procesos asociados a la seguridad de la información, como por ejemplo: uso adecuado de contraseñas, uso seguro en entornos de teletrabajo, manejo responsable de dispositivos móviles y compartir información de manera segura.

Trazabilidad y auditoría

Centro Ceibal se reserva el derecho de auditar los procesos relacionados a la seguridad de la información y la privacidad con el objetivo de verificar que se cumpla lo estipulado entre las partes. Para ello podrá solicitar al proveedor la documentación respaldante que corresponda en cada caso. A estos efectos deberá preverse tal facultad en el contrato.

Ejemplo de cláusula:

Centro Ceibal se reserva el derecho de auditar los procesos relacionados a la seguridad de la información y la privacidad del Proveedor con el objetivo de verificar que se cumpla lo estipulado entre las partes. En este contexto podrá solicitar al proveedor la documentación respaldante que corresponda en cada caso.

Protección de datos personales

Incluir en el acuerdo con el proveedor una cláusula que regule la protección de datos personales, y en los casos que sea necesario firmar un acuerdo de encargado de tratamiento.

Ejemplo cláusula Protección de datos personales:

En caso de acceder a datos personales el Proveedor se obliga a su tratamiento de conformidad con la Ley N° 18.331, de 11 de agosto de 2008 y Decreto N° 414/2009, de 31 de agosto de 2009, y a utilizarlos exclusivamente para los fines del acuerdo que vincula a las partes, no pudiendo utilizarlos para otra finalidad, ni cederlos, comunicar o transferirlos a terceros, salvo previa autorización por escrito del Centro Ceibal, y sus titulares o representantes.

Centro Ceibal es responsable de sus bases de datos, siendo el Proveedor, en caso de acceder a la base de datos, encargado de tratamiento, de acuerdo con lo dispuesto en los

literales H) y K) del artículo 4 de la Ley N° 18.331. No se autoriza la subcontratación de encargados de tratamiento de datos.

El Proveedor se obliga a adoptar las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de los datos personales y evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información.

En caso de que se alojen los datos personales, el Proveedor se obliga a que los servidores se sitúen en Uruguay. Sin perjuicio de lo anterior, en caso que los datos se alojen, aun temporalmente, fuera del territorio nacional, se obliga a que el servidor se encuentre en países considerados con niveles adecuados a los estándares europeos de protección de datos, de acuerdo con el Reglamento General de Protección de Datos 2016/679, del Parlamento Europeo y del Consejo, modificatorias, concordantes y complementarias.

Frente a requerimiento del Centro Ceibal, el Proveedor se obliga a 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, en caso de corresponder.

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, acústica o de cualquier otro tipo que refiera a ellas directa o indirectamente, conforme con lo dispuesto en el artículo 4 de la Ley N° 18.331 y artículos 1 y 4 del Decreto N° 414/009.

En la columna de la siguiente tabla "Acepto lo requerido"; es donde el oferente deberá expresamente indicar "Si" o "No" con lo solicitado. En caso de que no se indique explícitamente el cumplimiento por parte del oferente, la oferta será rechazada.

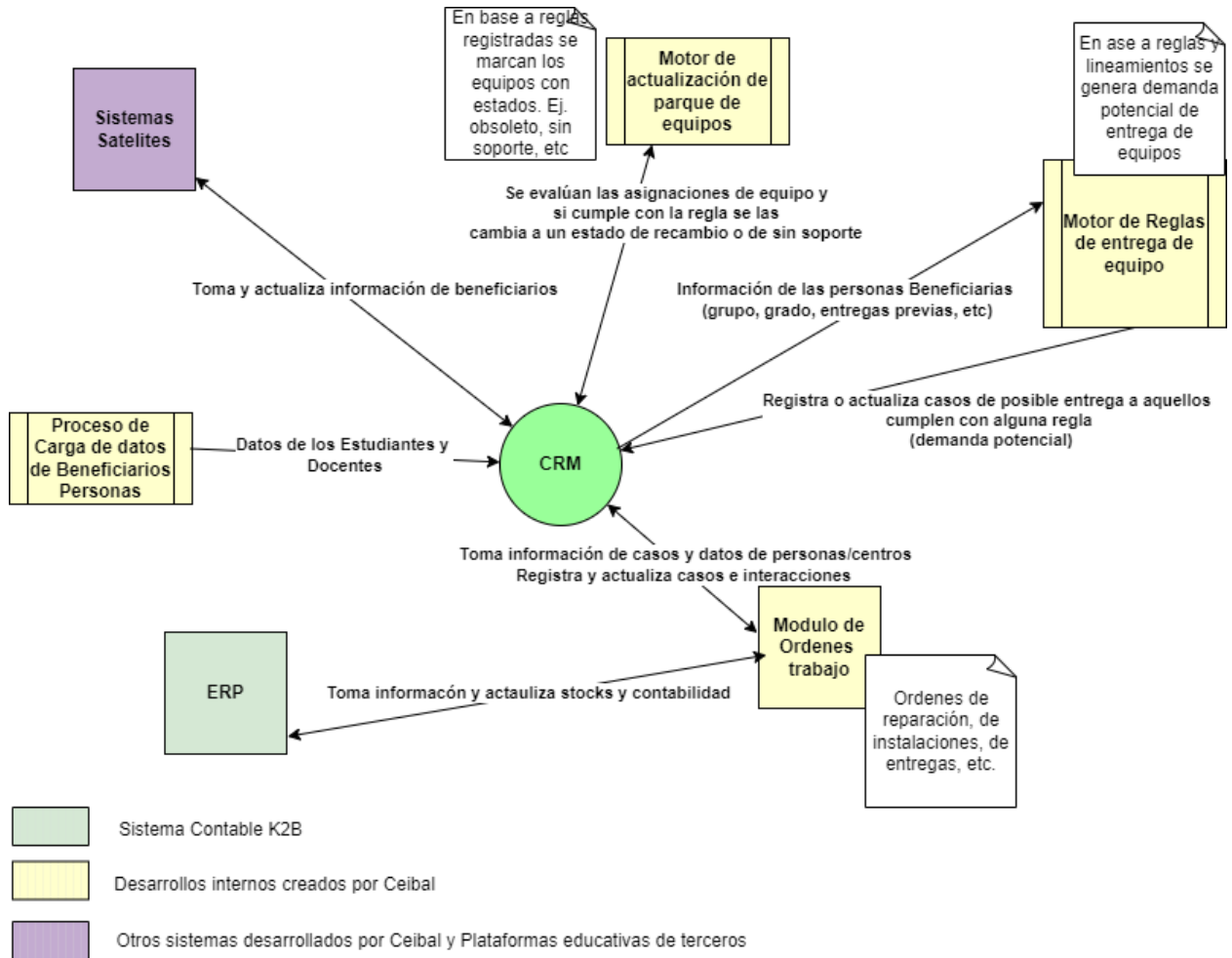
Matriz de cumplimiento de requerimientos de Seguridad de la Información Compra de horas de servicios (consultoría, desarrollo, soporte, etc.)		
A completar en conjunto por parte de Ceibal y el proveedor		
Requerimiento	¿Acepto lo requerido? [SI/NO]	Observaciones (si corresponde)
Cumplimiento de políticas		
Acuerdo de confidencialidad		
Uso de la infraestructura de Ceibal		
Protección de la información manejada		

Concientización y capacitación		
Trazabilidad y auditoría		
Protección de datos personales		

6 ANEXO 2

6.1

INTEROPERABILIDAD DEL CRM



6.2

ANEXO DE AUTENTICACIÓN CON LOGIN ÚNICO

La solución deberá integrarse con el sistema de login centralizado de Ceibal mediante el protocolo CAS en su versión 6.2.2 (<https://apereo.atlassian.net/wiki/spaces/CAS>)

- **Ambientes**

Ambientes	URL
Pruebas	https://ingreso.preprod-ceibal.edu.uy/
Producción	https://ingreso.ceibal.edu.uy

Fin del documento

