

# Licitación pública

## Horas de desarrollo y mantenimiento

### PLIEGO ESPECÍFICO

# ÍNDICE

<b>Índice</b>	2
<b>Objetivo</b>	3
ITEM 1	3
ITEM 2	4
ITEM 3	5
<b>Características del servicio</b>	6
Especificaciones Obligatorias	6
Forma de trabajo	8
<b>Oferta</b>	<b>9</b>
Modalidad de cotización	9
Presentación de la oferta	10
Evaluación	11
<b>Propiedad intelectual</b>	<b>12</b>
<b>Confidencialidad y protección de datos</b>	12
<b>Anexo</b>	13
Presentación de antecedentes	15
Acuerdos de Calidad del Servicio	19
Presentación de CVs	23
Requisitos de seguridad de la información y privacidad para la compra de horas de servicio con proveedores	24

## 1 OBJETIVO

Centro Ceibal llama a Licitación Pública para contratar a uno o más proveedores horas de desarrollo de software en modalidad remota o in situ para el desarrollo de proyectos y mantenimiento de soluciones informáticas de la institución.

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

Cada oferente deberá ofertar todos los ítems.

Ítem 1	Ítem 2	Ítem 3
<p><b>320 horas mensuales de soporte, desarrollo y mantenimiento</b> a ser distribuidas entre mantenimiento correctivo y evolutivo (computado en horas mensuales). Las horas no ejecutadas podrán ser acumuladas, dentro de los dos meses siguientes.</p>	<p>La adquisición de <b>hasta 20.000 horas de desarrollo y mantenimiento</b> a ser ejecutadas en un plazo de hasta dos años, según las necesidades de Centro Ceibal, en modalidad bajo demanda.</p>	<p>La adquisición de <b>hasta 200 horas fuera de horario de oficina destinadas a mantenimiento programado</b> y a soporte de incidencias, a ser ejecutadas en un plazo de hasta dos años, según las necesidades de Centro Ceibal, en modalidad bajo demanda.</p>

### ITEM 1

Las 320 horas mensuales de soporte, desarrollo y mantenimiento, serán utilizadas principalmente para la gestión de incidencias y mantenimiento correctivo, no obstante podrán ser utilizadas para actividades de mantenimiento evolutivo, así como para proyectos de investigación y de despliegue de nuevas herramientas/productos. Las horas no ejecutadas podrán ser acumuladas, dentro de los dos meses siguientes. Las mismas podrán ejecutarse dentro de las oficinas de Ceibal (in situ) o de forma remota.

La oferta debe contemplar la aceptación de los requerimientos de nivel de servicio propuestos por Centro Ceibal en la sección 6.2.3.

El horario sería de oficina: lunes a viernes (excepto feriados comunes y no laborables) de 9:00 a 17:00hs, hora local Uruguay.

## ITEM 2

Hasta **20.000** horas a demanda podrán ejecutarse dentro de las oficinas de Ceibal (in situ) o de forma remota. Al igual que el ítem 1, podrán ser horas de desarrollo, mantenimiento correctivo, mantenimiento evolutivo, o investigación y despliegue de nuevas herramientas/productos.

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

Para los proyectos solicitados, los roles para la conformación del equipo podrán ser: Account Manager (ej. gestión de recursos y seguimiento de proyectos, cartera, indicadores generales de servicio y forma de trabajo, propuestas de mejora de servicio y metodología de trabajo), 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.

Centro Ceibal podrá solicitar específicamente alguno de los perfiles mencionados en el pliego, el que trabajará en los días y horario habitual del Centro Ceibal (lunes a viernes de 9 a 17 hs - hora local Uruguay, excepto feriados comunes y no laborales). Esto podrá ser tanto en modalidad remota como in situ, dependiendo de las necesidades por parte de Ceibal.

## ITEM 3

Las 200 horas de mantenimiento programado y de gestión de incidencias fuera del horario de oficina, estarán orientadas a trabajos dentro de dicho horario, los cuáles serán requeridos en base a las necesidades operativas de Centro Ceibal.

Se considera horario *fuera* de oficina: lunes a viernes de 8 a 9 hs y de 17 a 22 hs y sábados de 8 a 17 hs, hora local Uruguay, excepto feriados comunes y no laborables.

Este ítem tiene como objetivo garantizar la continuidad de servicio de aquellas soluciones tecnológicas catalogadas como críticas para el Centro Ceibal (las cuáles se acordarán al inicio del servicio e irán variando según la necesidad operativa de Centro Ceibal).

La oferta debe contemplar la aceptación de los requerimientos de nivel de servicio propuestos por Centro Ceibal en la sección 6.2.3.

## 2 CARACTERÍSTICAS DEL SERVICIO

### 2.1 ESPECIFICACIONES OBLIGATORIAS

El oferente deberá contar con sólidos conocimientos de Laravel PHP, React/Node JS/Next JS/Nest JS, Java/Java EE y Pentaho, los cuales serán excluyentes.

Dentro de las tecnologías no excluyentes pero que Ceibal valorará especialmente se encuentran Power Apps y Power Platform y aquellas relacionadas con el diseño e implementación de soluciones con inteligencia artificial.

A continuación se presenta lista no taxativa de otras tecnologías no excluyentes que se evaluarán:

DevOps (jenkins, docker, y selenium)	Linux	Base de datos MySQL
Protocolo CAS	Flutter	October CMS
Rancher	Wordpress	Superset
Camunda / BPMS	Kotlin	

Las tecnologías mencionadas anteriormente serán sobre las cuales se evaluará la oferta de cada proveedor. Esto no implica que en el transcurso de la ejecución del contrato, se puedan utilizar otras tecnologías que a juicio de Ceibal, en conjunto con el proveedor, entiendan se ajustan mejor a las necesidades de Ceibal.

## 2.2 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.

La empresa oferente deberá contar con ambientes de desarrollo, mientras que Ceibal proporcionará los ambientes de testing, preproducción y producción. Si bien estos serán hospedados y administrados por parte de Ceibal, se podrá requerir realizar tareas de deploy por parte del proveedor, dependiendo de la necesidad del Centro Ceibal.

Se entiende que el 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.

Se establecerá con el proveedor un período de garantía post implementación en producción, considerando 30 días como pauta general.

Una vez implementado en ambiente productivo, se añadirá a los sistemas productivos a mantenerse. El oferente deberá brindar soporte y mantenimiento de los productos asignados, asegurando la calidad del servicio.

Se utilizará una herramienta de gestión provista por Ceibal, tanto para el seguimiento de incidentes, como el control de horas de cada mes.

El oferente deberá brindar un resumen mensual en base al SLA propuesto (aplicable a los ítems 1 y 3).

### 3 OFERTA

#### 3.1 MODALIDAD DE COTIZACIÓN

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

<b>Horas de desarrollo y mantenimiento - Pesos uruguayos</b>		
Items (*)		Costo (imp. incl.)
Ítem 1	Cotizar <b>por el total de 320 horas mensuales</b>	
Ítem 2	Cotizar <b>por hora (hasta 20.000 horas)</b>	
Ítem 3 (**)	Cotizar <b>por hora de mantenimiento fuera de horario de oficina (hasta 200 hs)</b>	

Todos los costos necesarios para brindar el servicio (conexión a internet, computadoras, teléfono, equipamiento necesario para desarrollar), viáticos y horas de transferencia deberán ser asumidos por el proveedor (para esto último Centro Ceibal estima 20 horas).

(\*) En los 3 Ítems la cotización debe contemplar todos los roles: Account Manager, Project Manager, Arquitecto de Software, Desarrollador y Tester, tanto en modalidad remota como in situ.

(\*\*) Se considera horario fuera de oficina: lunes a viernes de 8 a 9 hs y de 17 a 22 hs y sábados de 8 a 17 hs, hora local Uruguay, excepto feriados comunes y no laborables.

### 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. Especificaciones **obligatorias excluyentes**: como requisito excluyente, el oferente deberá tener al menos 37.000 horas (acumuladas) de dedicación para dichas tecnologías con antigüedad no mayor a 4 años (Laravel PHP, React/Node Js/Next JS/Nest JS, Pentaho, Java/Java EE).

Deberá cumplirse los mínimos de horas acumulados de:

- Laravel PHP - 10.000 horas
- React/Node JS/Next JS/Nest JS - 10.000 horas
- Pentaho - 7.000 horas
  
- Java/Java EE - 10.000 horas

b. - Se valorará experiencia demostrable en el diseño e implementación de **soluciones con inteligencia artificial**, especialmente en el uso de modelos de machine learning, modelos de lenguaje (LLMs), agentes basados en el protocolo MCP, visión por computadora, así como en su integración en entornos productivos.

c. Se valorará tener experiencia demostrable en proyectos con tecnologías Power Apps y Power Platform

d. - Se valorará tener experiencia acreditada en proyectos en las tecnologías descritas en las herramientas **no excluyentes**:

DevOps (jenkins, docker, y selenium), Linux, Rancher, Camunda/BPMS, Flutter, Kotlin, Protocolo CAS, Wordpress, Base de datos MySQL, October CMS, Superset

e. - Se valorará tener experiencia acreditada en proyectos de desarrollo de sistemas **orientados a la educación** de alcance nacional.

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

(Deberá presentarse de acuerdo al Anexo 5.1)

El oferente se podrá asociar o subcontratar con otras firmas conforme punto 2.5 C del Pliego General con el fin de mejorar sus calificaciones de antecedentes.

No se admitirán horas de desarrollo interno para el propio oferente.

✓ **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 al objeto del llamado (parcial o total). (Deberá presentarse de acuerdo al Anexo 5.3)

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

✓ **Tabla de SLA para mantenimiento correctivo** deberá presentarse de acuerdo Anexo 5.2.3

✓ **Tabla de Cumplimiento de Seguridad** deberá presentarse de acuerdo al Anexo 5.4

### 3.3 EVALUACIÓN

El criterio de evaluación técnica de los oferentes será en base al cumplimiento de las especificaciones para la prestación del servicio (sección 3.2), sumado a un análisis de los curriculums de los técnicos presentados por las empresas oferentes y antecedentes; contemplando aceptación de las tablas de consideraciones de seguridad y SLA.

En relación a los antecedentes requeridos se le asignará el mayor puntaje, por cada tecnología, a aquellas ofertas que presenten el doble del mínimo requerido.

Durante el proceso de evaluación técnica, Centro Ceibal aplicará una prueba/entrevista técnica de carácter eliminatorio a los desarrolladores presentados para las tecnologías definidas como excluyentes. La aprobación mínima de la prueba será 60%.

Se procederá a estudiar la oferta económica de aquellas propuestas que hayan superado el 60% de los puntos totales correspondientes a la evaluación técnica.

<b>Evaluación</b>	
	<b>% Evaluación máximo</b>
<b>Antecedentes</b>	20
<b>Cvs</b>	5
<b>Prueba Técnica</b>	25
<b>Oferta Económica</b>	50
<b>TOTAL</b>	<b>100</b>

## **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

(1 y 2) Por cada tecnología, discriminar los proyectos asociados. Tal cómo se indica en la primera tecnología, deberá replicarse para el resto.

(3) Cantidad de horas a cada proyecto. Deberá coincidir con la descripción por cada proyecto (cuadro). Se admitirán como válidas cifras exactas en cantidad de horas (no se admitirá por ejemplo +500 horas).

(4) Sumatoria total de cantidad de horas por tecnología. Es decir, la sumatoria de la columna 3.

(5) Sumatoria de la totalidad de horas de las tecnologías obligatorias excluyentes.

Tecnología utilizada	Mínimo solicitado (hs)	N° de proyecto/s (1)	Nombre/s del proyecto (2)	Total de horas por proyecto (3)	Total horas por tecnología (4)	Total de horas acumuladas (últimos 4 años) >= 20.000 (5)
<b>Especificaciones excluyentes</b>						
<b><u>Laravel</u></b> <b><u>PHP</u></b>	<b>10.000</b>	N° 1	Proyecto 1	Hs proyecto 1	<b>Suma hs proyecto 1+2+3</b>	<b>Suma de columna (4) en las tecnologías obligatorias excluyentes.</b>
		N° 2	Proyecto 2	Hs proyecto 2		
		N° 3	Proyecto 3	Hs proyecto 3		
<b>React/Node JS/Next JS/Nest JS</b>	<b>10.000</b>					
<b>Java/Java EE</b>	<b>10.000</b>					
<b>Pentaho</b>	<b>7.000</b>					

Proyectos	N° de proyecto/s (1)	Nombre/s del proyecto (2)	Total de horas por proyecto (3)	Total horas por tecnología (4)
<b>Especificaciones especialmente valoradas no excluyentes</b>				
Power Apps y Power Platform	N° 1	Proyecto 1	Hs proyecto 1	<b>Suma hs proyecto 1+2+3</b>
	N° 2	Proyecto 2	Hs proyecto 2	
	N° 3	Proyecto 3	Hs proyecto 3	
Proyectos vinculados a soluciones con inteligencia artificial				

Tecnología utilizada	N° de proyecto/s (1)	Nombre/s del proyecto (2)	Total de horas por proyecto (3)	Total horas por tecnología (4)
<b>Especificaciones no excluyentes</b>				
DevOps (jenkins, docker, y selenium)	1	Proyecto 1	Hs proyecto 1	<b>Suma hs proyecto 1+2+3</b>
	2	Proyecto 2	Hs proyecto 2	
	3	Proyecto 3	Hs proyecto 3	

Linux				
Rancher				
Camunda / BPMS				
Flutter				
Wordpress				
Kotlin				
Base de datos MySQL				
October CMS				
Superset				
Protocolo CAS				

Otros proyectos de interés	N° de proyecto/s (1)	Nombre/s del proyecto (2)	Total de horas por proyecto (3)	Total horas por tecnología (4)
<b>Otros</b>				
<b>Proyectos vinculados a la Educación</b>	N° 1	Proyecto 1	Hs proyecto 1	<b>Suma hs proyecto 1+2+3</b>
	N° 2	Proyecto 2	Hs proyecto 2	
	N° 3	Proyecto 3	Hs proyecto 3	
<b>Otros proyectos que se consideren relevantes en proyectos de mantenimiento</b>				

Cuadro excluyente a completar por cada proyecto. Ordenar del más reciente al más antiguo, por tecnología (de acuerdo a la tabla anterior). Sólo antecedentes de los últimos 4 años.

N° proyecto (1)	Nombre del proyecto (2)	Institución contratante	Contacto responsable de dicha institución, cargo, teléfono, mail	Descripción y alcance del proyecto	Período en el que fue realizado Duración en meses	Horas dedicadas en total	Lenguajes y Base de datos (incluir versiones usadas)	Hipervínculo a la carta de recomendación (si hubiere)

## 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 a 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 6.2.3.
- 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
- f. f. Gestión de errores bloqueantes en producción (Incumplimiento de requerimiento, imposibilidad de probar una funcionalidad)

**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, sprint 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 (punto 6.2.2.1 anterior) 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 plazos acordados con el Centro Ceibal de cualquiera de los parámetros descritos en el punto 6.2.2.1, 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 punto 6.2.2.2

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 punto 6.2.2.2.

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.

#### **5.2.2.2 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.

## 5.2.3 SLA - NIVEL DE SERVICIO

### TIEMPO DE RESPUESTA

Completar la columna "Cumple/No cumple", en base al SLA establecido por Centro Ceibal

Urgencia del incidente	SLA Ítem 1 <sup>1</sup>	SLA ítem 4 <sup>2</sup>	Observaciones	Cumple/ No Cumple
Urgente	1 hs	2 hs	Son aquellos incidentes <sup>3</sup> 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	2 hs	4 hs	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	4 hs	N/A	Son aquellos incidentes presentados en producción sobre el aplicativo que no impiden que cumpla con su función básica, pero sí les dificulta la operación.	

<sup>1</sup> El horario sería de oficina: lunes a viernes (excepto feriados comunes y no laborables) de 9:00 a 17:00hs, hora local Uruguay.

<sup>2</sup> Se considera horario *fuera* de oficina: lunes a viernes de 8 a 9 hs y de 17 a 22 hs y sábados de 8 a 17 hs, hora local Uruguay, excepto feriados comunes y no laborables,.

<sup>3</sup> 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.

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, con el siguiente contenido:

- Indicadores de cantidad de incidentes mensuales (y acumulados) según nivel de urgencia
- Indicadores de tiempo de respuesta de incidentes, medidos contra los tiempos descritos en el cuadro anterior, especificando los números de mantis. En el caso, de contar con desvío justificar.
- Indicadores de tiempos de resolución de incidentes mensuales según nivel de urgencia.
- Porcentaje de incidentes resueltos en el plazo comprometido, en el mes y según nivel de criticidad.
- Saldo de horas contratadas

### 5.3 PRESENTACIÓN DE CVs

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

#### Cuadro Resumen

- (1) **Roles:** Account Manager, Project Manager, Arquitecto de Software, Desarrollador y Tester
- (2) **Educación:** Especificar en:
  - Terciaria completa, incompleta o en curso
  - Técnica Superior
  - Posgrado/Máster completa, incompleta o en curso
- (3) **Descripción:** Especificar carrera y avance de la misma, orientación y añadir todo dato que el oferente considere.
- (4) **Otros:** añadir cursos/certificaciones relevantes para el rol.
- (5) **Cantidad de años de experiencia en el rol propuesto:** especificar dentro de la empresa actual
- (6) **Experiencia relevante para el llamado:** Especificar por tecnología los proyectos en lo que haya participado y su rol en el mismo.
- (7) **Historia laboral:** Especificar lo que se considere relevante respecto a Empresa, Rol, Principales actividades y periodo.

Rol (1)	Nombre y Apellido	Educación (2)	Descripción (3)	Otros (4)	Cantidad de años en el rol propuesto (5)	Experiencia (6)	Historia Laboral (7)
PM	Integrante 1	Terciaria completa	Ing en Sistemas	Scrum Master PMP	x	Tecnología 1: proyecto x, y Tecnología 2:	Empresa x PM 4 años Act 1, 2, 3

## 5.4 REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD PARA LA COMPRA DE HORAS DE SERVICIO CON PROVEEDORES

---

### Requisitos obligatorios

Estos requisitos son obligatorios para todos los llamados de compras de horas de servicio, a ser adquiridas por Centro Ceibal.

### Requisitos deseados

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

### Cumplimiento de Políticas

Todo proveedor debe conocer el [Manual de Políticas de Seguridad de la Información](#)

### Desarrollo seguro

Para tareas de desarrollo se deberán exigir los requisitos correspondientes que permitan brindar soluciones seguras.

Para tener un proceso de desarrollo seguro Ceibal sigue las buenas prácticas a nivel y sigue los lineamientos de OWASP para el desarrollo seguro.

Se debe incorporar el desarrollo seguro a lo largo del ciclo de vida de desarrollo del software (SDLC) incorporando la seguridad y la privacidad por diseño desde la planificación de los proyectos.

Se deben respetar los siguientes lineamientos:

- Tomar la última versión del Nivel 1 del estándar [ASVS \(Application Security Verification Standard\)](#) de OWASP como línea base de aceptación de seguridad. Detalle sobre los requisitos se pueden encontrar en [Requisitos de Seguridad de la información y Privacidad para pliegos de compra de soluciones TI](#)
- Cumplir con los requisitos, configuraciones, marcos de desarrollo y estándares (hardening) establecidos por Ceibal para las tecnologías que se

decidan usar. Por ejemplo, a nivel de aplicaciones web, se fomenta el desarrollo en base al CMS Wordpress y sus [lineamientos de seguridad](#).

- Cumplir con los requisitos de seguridad en cuanto a gestión de ambientes, control de cambios y despliegues en producción establecidos por Ceibal.

## **Acuerdo de confidencialidad**

Para asegurar la confidencialidad, integridad y disponibilidad de la información se deberán seguir las pautas y buenas prácticas de la industria. En particular Ceibal adopta el [MCA \(Marco de Ciberseguridad de Agesic\)](#).

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 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.

## **Cadena de suministro**

- La empresa se obliga a trasladar estas mismas exigencias a todos sus subcontratistas, proveedores y terceros que participen directa o indirectamente en la prestación de los servicios objeto del presente contrato, garantizando que:
  - Los subcontratistas implementen controles de seguridad equivalentes o superiores a los exigidos por este contrato.
  - Se pueden realizar auditorías o evaluaciones a los subcontratistas sobre el cumplimiento de dichos controles.
  - Se notifique de forma inmediata cualquier incidente de seguridad que afecte o pueda afectar la información o los sistemas de Centro Ceibal.
  - Se mantiene un plan de respuesta a incidentes y continuidad del negocio que incluya a los subcontratistas.

## **Inteligencia Artificial generativa:**

- Para el caso en que el proveedor utilice modelos de inteligencia artificial

generativa (IAG) propios o de terceros se deberán implementar los controles necesarios para proteger los datos garantizando la seguridad de la información. Para ello se deberán implementar controles y acuerdos que aseguren:

- • Que la información enviada por parte de Centro Ceibal a los modelos no es usada para el entrenamiento de los mismos.
- • Que los datos personales utilizados en el entrenamiento, validación o inferencia de los modelos han sido obtenidos legalmente y cuentan con las autorizaciones necesarias.
- • Que se implementen medidas técnicas y organizativas adecuadas para proteger la confidencialidad, integridad y disponibilidad de la información procesada.
- • Proporcionar documentación técnica que describa el funcionamiento del sistema, sus limitaciones y riesgos.
- • Implementar controles de ciberseguridad que aseguren la protección frente a accesos no autorizados, manipulación de modelos, y vulnerabilidades en el ciclo de vida de la IAG.
- • Mantener un registro de auditoría de eventos relevantes del sistema de IAG.
- • Abstenerse de utilizar modelos de IAG para generar contenido falso, discriminatorio, ofensivo o que infrinja derechos de propiedad intelectual.
- • Garantizar que los modelos utilizados han sido entrenados con datos que respetan los derechos de autor y no vulneran derechos de terceros
- El Proveedor se obliga a trasladar estas exigencias a cualquier subcontratista o tercero que participe en el desarrollo, implementación o mantenimiento de los sistemas de IAG utilizados en el marco del presente contrato.

## **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.

Compra de horas de servicios (consultoría, desarrollo, soporte, etc.)			
A completar por el proveedor			
Requerimiento	Tipo	Acepto/No Acepto	Observaciones
Cumplimiento de políticas	Obligatorio		
Acuerdo de confidencialidad	Obligatorio		
Uso de la infraestructura de Ceibal	Obligatorio		
Protección de la información manejada	Obligatorio		
Concientización y capacitación	Obligatorio		
Cadena de Suministro	Obligatorio		
Inteligencia artificial generativa	Obligatorio		
Trazabilidad y auditoría	Obligatorio		
Protección de datos personales	Obligatorio		

Deberá indicar la aceptación de las condiciones de entrega de servicio especificada.

En caso que Ceibal lo requiera, se deberá tener a disposición y presentar, material que acredite lo declarado en la presente matriz. 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.

**Nivel de Madurez en Seguridad:** Los proveedores deberán completar la siguiente autoevaluación:

**Autoevaluación Seguridad**