Concurso Público de Precios.

Pliego de Condiciones Técnicas.

Adquisición de servicios.
Agencia de desarrollo y diseño web.

Gerencia de Comunicación y Marca.

Enero, 2023.

ÍNDICE

1. Introducción

Ceibal tiene como misión ser el centro de innovación educativa con tecnologías digitales del Uruguay, promoviendo la integración de la tecnología a la educación con el fin de mejorar los aprendizajes e impulsar procesos de innovación, inclusión y crecimiento personal.

Su visión institucional es impulsar junto al sistema educativo una educación innovadora e inclusiva mirando al futuro, aprovechando las oportunidades que ofrece la tecnología, para que cada estudiante del Uruguay desarrolle su potencial de aprendizaje y creatividad, construyendo capacidades para la ciudadanía global.

En el marco de la implementación de su plan estratégico 2021 - 2025 Ceibal busca consolidar los procesos de comunicación y difusión de su propuesta de valor, que permitan mejorar el vínculo con usuarios. Asimismo, se propone que los beneficiarios y la sociedad en su conjunto conozcan en profundidad la propuesta de Ceibal.

Desde la Gerencia de Comunicación y Marca es un objetivo y compromiso de gestión contribuir a la percepción de valor de Ceibal, vía, entre otros, la mejora del nivel de calidad de sus sitios web.

2. Objetivo

Este llamado a concurso público de precios tiene como objeto la adquisición de servicios de horas de diseño gráfico, diseño UI/UX y desarrollo web, así como horas de mantenimiento.

Las mismas serán destinadas a la realización de proyectos y resolución de incidencias de sitios de comunicación de las diversas áreas de Ceibal, bajo la supervisión y coordinación de la Gerencia de Comunicación y Marca.

Dichas horas serán ejecutadas a demanda, en un plazo de hasta dos años, según las necesidades de Ceibal. El mismo podrá ser renovado mediante acuerdo de ambas partes bajo iguales condiciones por el mismo período.

3. Servicios

Los servicios que el proveedor debe ofrecer se agrupan en los siguientes ítems:

1. Diseño gráfico
2. Diseño UX/UI
3. Criterios de diseño y desarrollo accesible
4. Criterios de desarrollo seguro
5. Desarrollo web
6. Mantenimiento y gestión de incidencias

El nivel de cumplimiento requerido en cada uno de los ítems solicitados es el siguiente:

1. Diseño gráfico

Desarrollo de propuestas gráficas específicamente diseñadas para web y alineadas al manual de identidad gráfica de Ceibal.
Se pretende que el proveedor aporte opciones de recursos de diseño web novedosas, vistosas e innovadoras.
En la oferta se deberán presentar ejemplos de diseño gráfico web que serán tenidos en cuenta en la evaluación del proveedor para validar la capacidad de brindar este servicio.

2. Diseño UX/UI

Muchos de los sitios desarrollados por Ceibal son utilizados por estudiantes de primaria y secundaria, quienes deben navegarlos de forma simple e intuitiva. Es imprescindible que el proveedor tenga pleno dominio de los criterios requeridos para que los diseños se basen en la experiencia de usuario.
En la oferta se deberán presentar ejemplos de diseño UX/UI que serán tenidos en cuenta en la evaluación del proveedor para validar la capacidad de brindar este servicio.

3. Criterios de diseño y desarrollo accesible

Es parte de la política de comunicación de Ceibal y recientemente decretado por ley, que todos los materiales comunicaciones sean accesibles, lo cual incluye la totalidad de sus sitios web. Se solicita al proveedor que tenga plena capacidad de desarrollar diseños web accesibles bajo las recomendaciones de accesibilidad web de AGESIC, así como los estándares de W3C Web accesibility y los criterios de la WCAG.
En la oferta se deberán presentar ejemplos de diseño y desarrollo accesible, que serán tenidos en cuenta en la evaluación del proveedor para validar la capacidad de brindar este servicio.

4. Desarrollo web

Los desarrollos deberán realizarse en WordPress, para lo cual se requiere dominio de sus funcionalidades, plugins, etc.
En la oferta se deberán presentar ejemplos de desarrollo en WordPress, que serán tenidos en cuenta en la evaluación del proveedor para validar la capacidad

de brindar este servicio. Los desarrollos deberán contemplar el estándar de desarrollo definido por Ceibal.

5. Mantenimiento y gestión de incidencias.

El proveedor deberá brindar servicio de mantenimiento base que será utilizado fundamentalmente para diseño y mantenimiento correctivo (resolución de incidencias), y en caso de sobrantes serán utilizadas en proyectos y tareas de mantenimiento evolutivo y preventivo (mejoras y/o ajustes sobre los instancias previamente aprobadas), dentro del mes corriente o mes siguiente.
Este servicio debe abarcar tanto los sitios activos ya desarrollados por Ceibal como los nuevos proyectos a desarrollar en el marco de este contrato.
Se utilizará una herramienta de gestión provista por Ceibal para el seguimiento de incidentes, donde se realizará el control de horas de cada mes. El oferente deberá brindar un resumen mensual clasificado por importancia y también deberá proyectar las horas que se van a consumir con una estimación previa en base a los trabajos solicitados.
La oferta deberá incluir una descripción del nivel del servicio propuesto, según los diferentes niveles de criticidad. A modo de ejemplo, tiempo de respuesta a incidentes, resolución y recuperación ante fallos, considerando un horario de atención de Lunes a Viernes de 9:00 a 18:00 horas (días hábiles).

4. Especificaciones técnicas

El oferente deberá contar y acreditar sólidos conocimientos de las siguientes especificaciones técnicas.

Especificaciones técnicas excluyentes:

- WordPress
- Php
- Bootstrap
- Google Analytics
- Javascript
- Css, html, responsive design
- Git
- October cms
- Seo
- Google Tag Manager

Especificaciones técnicas deseables, no excluyentes:

- Linux
- Percona mysql
- Mysql
- API REST
- Docker
- Redmine, Mantis, Trello o similar.

El proveedor deberá listar las especificaciones técnicas que ofrece y acreditar de forma comprobable que posee sólido dominio de las mismas, para lo cual podrá proveer ejemplos y antecedentes que entienda de valor.

5. Modalidad de trabajo

La empresa adjudicada deberá seguir las pautas de desarrollo y seguridad definidas por Ceibal, que especifica, entre otros puntos, nomenclatura, manejo de repositorio de código fuente, versiones de software base a utilizar y buenas prácticas de desarrollo.

Para todo componente de desarrollo se utilizará Git como repositorio de código fuente utilizando la metodología git-flow. El repositorio Git será provisto por Ceibal.

Los sitios deberán estar construidos siguiendo los estándares Html5 y CSS3 del W3C según las pautas de Accesibilidad para el Contenido Web (WCAG), lo cual incluye WCAG 2.0 y WCAG 2.1. con un nivel de conformidad no menor al AA.

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 ambientes de testing, preproducción y producción.

En el caso de la modalidad in situ, Centro Ceibal proporcionará el espacio físico. Para toda tarea se utilizarán los ambientes de pruebas ya existentes en Centro Ceibal pudiendo ser parte del proyecto realizar tareas de pasaje a producción si así fuese requerido.

En relación al control de horas de desarrollo a consumir, el oferente deberá estimar semanalmente las horas a trabajar, las cuales serán aprobadas previamente por Ceibal y documentadas por el proveedor al terminar la semana. Llegado el cierre del mes, se deberá brindar un detalle del total de horas trabajadas, validando así las horas de servicio a facturar previa aprobación de Ceibal.

Respecto al Hosting, todo sitio ya existente se encuentra hosteado por parte de Ceibal. Para aquellos proyectos a desarrollar durante el plazo del contrato, los cuales impliquen nuevos sitios y por ende nuevo hosting, Ceibal se encargará de proveer la arquitectura necesaria y realizar la operación del mismo. Para determinados portales web, previamente acordados, el proveedor podrá realizar cambios en ambientes productivos siguiendo las pautas de Ceibal.

Como aspecto que condiciona la modalidad de trabajo se detalla que a mediados del 2022 Ceibal realizó la reingeniería de su portal con la que cambió de CMS a Wordpress, modificó la arquitectura y el criterio de desarrollo de sitios.

Se generó un sistema de bloques a medida (y otros de gutenberg con clases CSS) mediante plugins y el diseño del tema que incluye cabezal y footer del portal y subsitios. Estos bloques se alinean a la identidad gráfica de Ceibal y continúan en desarrollo. Por lo que será requerido la creación, customización y mantenimiento de bloques. Adicionalmente, el desarrollo de sitios deberá basarse en el armado de páginas mediante estos bloques predefinidos.

A raíz de esta reingeniería, el desarrollo de sitios deberá basarse en el armado de páginas mediante estos bloques predefinidos, crear nuevos bloques de ser requerido y customizarlos según los requerimientos de cada desarrollo.

6. Cotización

Se solicita a las empresas oferentes cotizar obligatoriamente horas de servicio para dos ítems.

Ítem 1- Desarrollo.
Se trata de horas de desarrollo web, diseño web, diseño UX/UI y testing para la implementación de proyectos.
Modalidad: Bajo demanda, según las necesidades de Ceibal, en modalidad
Cantidad: Máximo de hasta 6.000 horas a consumir a demanda en un plazo máximo de 24 meses de contrato.
Consumo: Si el máximo de 6.000 horas no es consumido en el período de 24 meses del contrato el plazo del mismo se podrá prorrogar hasta completar su consumo.

Ítem 2- Mantenimiento.
Se trata de horas de mantenimiento a ser distribuidas entre mantenimiento correctivo y evolutivo.
Modalidad: Será computado en horas mensuales.
Cantidad: hasta 50 horas mensuales a consumir en los 24 meses de contrato.
Consumo: Si un mes las 50 horas mensuales de mantenimiento no fueran consumidas, podrán ser acumuladas para su consumo el mes siguiente.

La cotización de los dos ítems debe contemplar todos los roles requeridos por el proveedor para brindar el servicio: Project Manager, Arquitecto de Software, Desarrollador, Diseñador UX/UI y Tester. Todos los roles deben poder operar tanto en modalidad remota como in situ en caso de ser requerido.

Asimismo se deberá contemplar las horas de gestión correspondientes a reuniones de trabajo que un proyecto requiera, entendiendo las mismas como un costo por parte del proveedor considerando un máximo de 3 horas semanales, en día y horario de oficina (lunes a viernes de 9 a 18hs).

Todos los costos necesarios para brindar el servicio (conexión a internet, computadoras, teléfono, equipamiento necesario para desarrollar), así como los viáticos y las horas de transferencia de conocimiento serán de cargo del adjudicatario.

En caso de que el adjudicatario manifieste que no cuenta con la capacidad operativa ante un requerimiento específico, Ceibal se reserva el derecho de contratar horas al segundo mejor proveedor de la lista de pre-calificados.

Por otra parte, el proveedor debe cotizar obligatoriamente dos ítems adicionales, que Ceibal podrá utilizar o no en función de que así lo requiera.

Ítems de cotización obligatoria y adjudicación opcional:

Adicional 1: Desarrollo fuera de hora.

Se trata de horas de desarrollo web, diseño web, diseño UX/UI y testing para la implementación de proyectos que por su naturaleza o debido a alguna excepción deban ser gestionadas fuera de horario habitual de oficina, luego de las 18:00 h, en días no laborables o durante los fines de semana.

Modalidad: Bajo demanda, según las necesidades de Ceibal.

Cantidad: Máximo de hasta 240 horas a consumir a demanda en un plazo máximo de 24 meses de contrato.

Consumo: Solo en caso de ser requerido, bajo demanda de Ceibal y previo acuerdo de disponibilidad con el proveedor.

Adicional 2: Hora extra de gestión.

Se trata de horas de gestión correspondientes a reuniones de trabajo que un proyecto requiera y siempre que implique superar las 3 horas semanales incluidas en el costo de gestión del proveedor.

Modalidad: Bajo demanda, según las necesidades de Ceibal.

Cantidad: Máximo de 50 horas a consumir a demanda en un plazo máximo de 24 meses de contrato, en día y horario de oficina (lunes a viernes de 9 a 18hs)

Consumo: Solo en caso de ser requerido, bajo demanda de Ceibal y previo acuerdo de disponibilidad con el proveedor.

7. Presentación de la oferta

Las propuestas deberán enviarse cumpliendo con el siguiente nivel de detalle.

1: Oferta Técnica: Empresa.

- Presentación de antecedentes de la empresa.
- Presentación de especificaciones técnicas que se ofrecen.
- Presentación de equipo de trabajo directamente afectado a Ceibal.
- Acuerdo de calidad de servicio.

2: Oferta técnica: Servicios.

- Ejemplo de Diseño gráfico web
- Ejemplo de Diseño UX/UI
- Ejemplo de Diseño y desarrollo accesible
- Ejemplo de Desarrollo en WordPress
- Gestión de mantenimiento. Niveles de respuesta según criticidad.

3: Oferta Económica: Cotización.

La empresa oferente deberá cotizar su propuesta económica de los dos ítems obligatorios completando el siguiente cuadro.
Estos servicios se prestarán de lunes a viernes de 09:00 a 18:00 h.

Ítem Obligatorio	Descripción	Cantidad de horas	Costo sin IVA	IVA	Costo con IVA
Mantenimiento	Mantenimiento correctivo y evolutivo.	Máximo de 50 horas mensuales	$ UY por hora	$ UY	$ UY por hora
Desarrollo	Desarrollo web, diseño web, testing y diseño UX/UI	Máximo de 6.000 horas	$ UY por hora	$ UY	$ UY por hora

La empresa oferente deberá cotizar su propuesta económica de los dos ítems adicionales de cotización obligatoria y adjudicación opcional completando el siguiente cuadro.
Los mismos podrán o no ser adjudicados por Ceibal a utilizar a demanda sólo en caso de ser requerido.

Completar cuadro con oferta:

Ítem Adicional	Descripción	Cantidad de horas	Costo sin IVA	IVA	Costo con IVA
Extra horario	Hora de desarrollo fuera de horario de oficina	Máximo 240 horas	$ UY por hora	$ UY	$ UY por hora
Gestión	Hora de instancias de coordinación adicionales	Máximo 50 horas	$ UY por hora	$ UY	$ UY por hora

8. Evaluación de la oferta

Las ofertas recibidas serán evaluadas bajo el siguiente criterio:

Oferta	Items	Ponderación
Técnica: Empresa	- Antecedentes - Especificaciones técnicas - Perfiles del equipo - Acuerdo de calidad de servicio	30%
Técnica: Servicios	- Ejemplo de Diseño gráfico web - Ejemplo de Diseño UX/UI - Ejemplo de Diseño y desarrollo accesible - Ejemplo de Desarrollo en WordPress - Gestión de mantenimiento	40%
Económica	- Costo por hora de mantenimiento - Costo por hora de desarrollo	30%
TOTAL		100%

Las empresas que logren sumar un 70% de los puntos requeridos en las ofertas técnicas pasan a ser consideradas en el análisis de la oferta económica.

Los criterios de evaluación considerarán los aspectos que se detallan a continuación.

Oferta técnica: Empresa.

1- Criterios para evaluación de antecedentes:

Antecedente	Fecha	Pertinencia	Nivel del desarrollo
Clientes destacados	- Reciente (menos de 2 años) - Lejano (más de 2 años)	- Cumple o no cumple. Vinculado con educación, tecnología, público infantil u otras áreas relevantes para Ceibal.	- Cumple o no cumple. Se aprecia alto nivel de calidad y cuidado en diseño gráfico, diseño UX/UI u otros aspectos relevantes para la naturaleza del cliente.
Proyectos destacados	- Reciente (menos de 2 años) - Lejano (más de 2 años)	- Cumple o no cumple. Vinculado con educación, tecnología, público infantil u otras áreas relevantes para Ceibal.	- Cumple o no cumple. Se aprecia alto nivel de calidad y cuidado en diseño gráfico, diseño UX/UI u otros aspectos relevantes para la naturaleza del proyecto.

2- Criterios para evaluación de especificaciones técnicas:

Especificaciones técnicas excluyentes		
ESPECIFICACIÓN	**EVIDENCIA SOLICITADA**	**EVALUACIÓN**
WordPress	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
Php	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
Bootstrap	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
Javascript	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
Css, html, responsive design	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
Git	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
October cms	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
Google Analytics	Ejemplo o similar que acredite solvencia en la temática.	Cumple / No cumple
Seo	Ejemplo o similar que acredite solvencia en la temática.	Cumple / No cumple
Google Tag Manager	Ejemplo o similar que acredite solvencia en la temática.	Cumple / No cumple
Especificaciones técnicas no excluyentes		
ESPECIFICACIÓN	**EVIDENCIA SOLICITADA**	**EVALUACIÓN**
Linux	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
Percona mysql	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
Mysql	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
API REST	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
Docker	Ejemplo o similar que acredite solvencia en la temática.	Nivel general del desarrollo
Redmine, Mantis, Trello o similar.	Ejemplo o similar que acredite solvencia en la temática.	Cumple / No cumple

3- Criterios para evaluación de perfiles del equipo:

Perfil	Formación	Experiencia	Nivel de dedicación
Descripción del rol y las las funciones que cumple en el equipo	Básico: Técnico Medio: Universitario Avanzado: Posgrado	Básica: Menos de 2 años o proyectos de baja complejidad. Media: Menos de 5 años o proyectos de moderada complejidad Alta: Más de 5 años o proyectos de alta complejidad.	% de dedicación a la atención de Ceibal.

Este criterio de evaluación aplicará para todos los perfiles presentados en la propuesta, debiendo explicitar qué nivel de dedicación se le adjudicaría a la atención de Ceibal.

4- Criterios para la evaluación del acuerdo de calidad de servicio.

Tiempo de respuesta.

Incidentes en Producción: En la columna de la siguiente tabla "Cumple con 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.

Urgencia del incidente	SLA (en horas)	Observaciones	¿Cumple? [SI/NO]
Alta	0,5 hs	Son aquellos incidentes[1] presentados en producción sobre las soluciones que detienen o afectan la operación, colocando en riesgo la operativa de CEIBAL o el servicio brindado por CEIBAL a sus usuarios/beneficiarios	
Media	2 hs	Son aquellos incidentes presentados en producción sobre las soluciones que no detienen la operación, pero sí impiden que	

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

		algunos recursos cumplan con su función básica.	
Baja	4 hs	Son aquellos incidentes presentados en producción sobre las soluciones que no impiden que cumpla con su función básica, pero sí les dificulta la operación.	

Criterios para atención a pedido de servicio:

Prioridad De la Solicitud	SLA (días hábiles)	Observaciones	¿Cumple? [SI/NO]
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

Oferta técnica: Servicios.

- Criterios para evaluación de servicios ofrecidos.

SERVICIO	EVIDENCIA SOLICITADA	EVALUACIÓN			
Diseño gráfico	Ejemplos de diseño gráfico web	Nivel estético general	Diseño específicamente desarrollado para digital	Nivel de creatividad y originalidad.	
Diseño UX/UI	Ejemplos de diseño UX/UI	Nivel de cumplimiento criterios UX	Nivel de cumplimiento criterios UI		
Diseño y desarrollo accesible	Ejemplos de diseño y desarrollo accesible	Cumple criterios de accesibilidad web de AGESIC,	Cumple estándares de W3C Web accesibility	Cumple criterios de la WCAG.	
Desarrollo en WordPress	Ejemplos de desarrollo en WordPress.	Uso apropiado de temas y plug ins	Facilidad de mantenimiento y actualización.	Nivel de economía de recursos	Contempla el estándar de desarrollo definido por Ceibal.
Mantenimiento y gestión de incidencias.	Descripción del nivel del servicio propuesto, según los diferentes niveles de criticidad.	Tiempos de respuesta ante fallos urgentes (L a V 9 a 18)	Tiempos de respuesta ante fallos moderados (L a V 9 a 18)	Tiempos de respuesta ante fallos leves (L a V 9 a 18)	Tiempos de respuesta fuera de horario laboral.

9. Plazos

Reunión explicativa mediante videollamada: la fecha de la misma así como el

link de acceso será informado en el pliego de condiciones generales y portal de Compras de Ceibal.

10. 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 no infringir 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.

11. Confidencialidad y protección de datos.

La empresa debe informar en la propuesta el territorio donde aloja los datos, y los subcontratos a los que adhiera para el tratamiento de los mismos. En caso que los datos personales se alojen, aun temporalmente, fuera del territorio nacional, la Empresa se obliga a que el importador 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. El oferente que resulte adjudicado se obliga en forma expresa a conservar en la más estricta confidencialidad toda la información que procese o utilice durante su relación con Centro Ceibal.

La Empresa se obliga a tratar los datos a los que tuviere acceso en virtud de este contrato, de conformidad con la Ley Nº 18.331, de 11 de agosto de 2008 y Decreto Nº 414/2009, de 31 de agosto de 2009, únicamente para la prestación y en el marco del servicio contratado, no pudiendo utilizarlos para otra finalidad, ni en beneficio propio ya sea gratuito u oneroso, ni cederlos, comunicarlos o transferirlos a terceros, salvo previa autorización de Centro Ceibal.

Centro Ceibal es responsable de la base de datos y del tratamiento, siendo el oferente adjudicado encargado de tratamiento, de acuerdo con lo dispuesto en los literales H) y K) del artículo 4 de la Ley Nº 18.331. Por tanto, en ningún caso el acceso a datos podrá entenderse como cesión o permiso para su libre utilización por parte de quien resulte adjudicado. El oferente adjudicado se obliga a 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. Al término del contrato el oferente deberá suprimir de todos sus sistemas y archivos físicos y lógicos, sean propios o contratados a terceros, los datos personales accedidos, obtenidos o tratados en virtud de la contratación con Ceibal, 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 Nº 18.331 y artículos 1 y 4 del Decreto Nº 414/009.

12. Acuerdos de Calidad del Servicio

1.1.1 Calidad del Servicio

En cada **proyecto o mantenimiento asignado**, el proveedor será responsable de realizar todas las actividades 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 que hubieran podido ser detectados durante el proceso de testing del proveedor, deberá ejecutarse nuevamente el ciclo de pruebas diseñado sin costo extra..

1.1.2 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.

1.1.2.1 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 en el presente documento, así como las fechas acordadas en instancias de estimación e intercambio entre Ceibal y el proveedor.
- Seguimiento de pendientes: Se espera un intercambio fluído/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 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 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:

- 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.

1.1.2.2 **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.

13. Seguridad de la información

Para un desarrollo seguro de las aplicaciones se deberán seguir las pautas y buenas prácticas de la industria. En particular Ceibal adopta el MCA (Marco de Ciberseguridad de Agesic) 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:

- Cumplir con lo establecido en el Manual de Políticas de Seguridad de la Información de Centro Ceibal, disponibles en el portal de Ceibal: https://www.ceibal.edu.uy/storage/app/media/manual-de-politicas-de-seguridad-de-la-informacion-wiki-ceibal.pdf
- Tomar la última versión del Nivel 1 del estándar ASVS de OWASP como línea base de aceptación de seguridad. Un detalle de los requisitos se puede encontrar en el Anexo de Seguridad de la Información al final del documento.
- Cumplir con los requisitos, configuraciones, marcos de desarrollo y estándares (hardening) establecidos por Ceibal para las tecnologías que se

decidan usar. A modo de ejemplo se debe cumplir con los requisitos de seguridad establecidos para Wordpress.
- Cumplir con los requisitos de seguridad en cuanto a gestión de ambientes, control de cambios y despliegues en producción establecidos por Ceibal.
- Cumplir con lo estipulado en los acuerdos de nivel de servicios (SLA) correspondientes.
- Cumplir con lo establecido en el acuerdo de confidencialidad (NDA).
- Los desarrollos no deberán contar con vulnerabilidades de seguridad críticas a partir de test OWASP ZAP.

En el caso que la información sea almacenada en servidores del proveedor ya sea en modalidad on premise o en nubes, se deberán extremar los cuidados. el proveedor deberá proteger la información en reposo, en tránsito o en uso tomando las medidas necesarias y desplegando los controles que aseguren la confidencialidad, integridad y disponibilidad de la información.

A modo de ejemplo se recomiendan:
- La encriptación a nivel de discos, dispositivos y/o base de datos.
- El uso de herramientas de DLP (data loss prevention) y CASB (cloud access security brokers).
- NO crear ni usar copias de la información, solamente en los casos que sean necesarios.
- La encriptación para los datos en tránsito.
- 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 adecuado de sistemas de gestión de identidades que permitan una correcta autenticación de usuarios en los sistemas del proveedor que incluya 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.
- Manejar esquemas y arquitecturas que tomen en cuenta la continuidad del servicio de manera de garantizar el SLA acordado, como por ejemplo implementar planes de recuperación ante desastres, contingencias, alta disponibilidad y respaldos adecuados.

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.

Se deberá:

- Realizar una gestión adecuada de los usuarios generados al proveedor. Esto incluye información por parte del proveedor de las altas, bajas y modificaciones de los funcionarios 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.

En el caso de un incidente de ciberseguridad se deberá reportar inmediatamente al mail de csirt csirt@ceibal.edu.uy detallando la mayor información posible, para una adecuada gestión del mismo.

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.

El personal del proveedor deberá estar informado y concientizado con el objetivo de gestionar de manera segura la información que manejan 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.

Requisitos seguridad de la Información

A continuación se detallan los requisitos exigidos a una solución de software para Ceibal. Estos requisitos están basados en el estándar OWASP ASVS de desarrollo seguro.

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. (Ver documento)
- Compatibilidad con los sistemas de autenticación centralizados (SSO) usados por Centro Ceibal según corresponda:
- Sistema de Login único para beneficiarios. (protocolo CAS - ver Anexo)
- Compatibilidad para autenticación con alguno de los siguientes proveedores de identidades (Google, Active Directory) detallando protocolos y configuraciones usados. (ver Documento)
- Posibilidad de autenticación con múltiples factores (MFA) para cuentas privilegiadas.

Gestión de sesiones

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

Para esto deberá:

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

Control de acceso

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

Para esto deberá cumplir que::

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

Codificación y validación

Las debilidades más comunes en aplicaciones web modernas, son los fallos en validar correctamente las entradas de datos que provienen de los usuarios y el entorno, previo al uso de esta información. Estas debilidades generan la mayoría de las vulnerabilidades y ataques conocidos como por ejemplo Cross-Site Scripting (XSS), Inyección SQL, ataques al sistema de archivos, ataques Unicode y desbordamiento de buffers.

La solución deberá cumplir con:

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

Manejo de errores y verificación de logs

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

Para lograr esto la solución deberá:

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

Confidencialidad y Protección de datos

La solución deberá asegurar la confidencialidad, integridad y disponibilidad de la información y datos personales. Para implementar una adecuada protección de datos, la solución deberá asegurar la: legalidad, veracidad, finalidad, previo

consentimiento informado, seguridad de los datos, reserva, y responsabilidad. Para esto la solución deberá:

- Cumplir con la normativa vigente uruguaya en materia de datos personales (Ley Nº 18.331, de 11 de agosto de 2008 y Decreto Nº 414/2009, de 31 de agosto de 2009). Se considera dato personal la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, a modo enunciativo, cualquier información numérica, alfabética, gráfica, fotográfica, registro de voz e imagen, acústica o de cualquier otro tipo que refiera a ellas directa o indirectamente, conforme con lo dispuesto en el artículo 4 de la Ley Nº 18.331 y artículos 1 y 4 del Decreto Nº 414/009.
- Adoptar las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de los datos y evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información.
- Proteger la información y datos creada, editada, borrada o accedida sin las autorizaciones correspondientes, en particular en cantidades masivas de datos.
- Tomar las precauciones y controles necesarios para que la información y los datos personales no queden disponibles en navegadores, balanceadores de carga, copias temporales, cookies y otras estructuras donde no sea necesario.
- Asegurar la confidencialidad de toda la información que se procese o utilice. La Información Confidencial comprende, entre otros y a vía de ejemplo, la siguiente información: toda estrategia, plan y procedimiento comercial, información propietaria, software, herramienta, proceso, imágenes, datos personales, metodología, información y secreto comercial, y demás información y material de Ceibal, así como de los alumnos, beneficiarios, docentes, centros de estudios, que pudiera ser obtenida de cualquier fuente o pudiera ser desarrollada. .
- Alojar los datos en territorio uruguayo, o en caso de transferencia internacional asegurar que el servidor se encuentre en países considerados con niveles adecuados de acuerdo con la Directiva 95/46/CE. En caso contrario, contar con el consentimiento del titular del dato para la transferencia a un territorio no adecuado, o a que el importador haya suscripto cláusulas contractuales tipo con el exportador o posea un Código de Conducta inscripto, con la consecuente autorización de transferencia internacional de datos tramitada ante la Unidad Reguladora y de Control de Datos Personales, en los dos últimos supuestos.
- No utilizar la información / datos para una finalidad distinta a la contratada, ni en beneficio propio ya sea gratuito u oneroso, ni cederlos, comunicarlos o transferirlos a terceros.
- Centro Ceibal será el responsable de la base de datos y del tratamiento, siendo la Empresa adjudicada y sus empresas sub contratadas, encargados de tratamiento, de acuerdo con lo dispuesto en los literales H) y K) del artículo 4 de la Ley Nº 18.331.
- Permitir la publicación de las políticas de privacidad y términos y condiciones de uso de Centro Ceibal en el desarrollo.
- Permitir el derecho de acceso, rectificación, actualización, inclusión o supresión de los datos personales.

- Devolver o suprimir de todos sus sistemas y archivos físicos y lógicos, sean propios o contratados a terceros, los datos personales accedidos, obtenidos o tratados, así como los metadatos asociados, a requerimiento de Ceibal.

Comunicaciones

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

Para esto deberá:

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

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 informacion 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:

- 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 mediante informe resumen o certificado correspondiente. Se valorará informe detallando cobertura de amenazas sobre el último OWASP Top Ten vigente

ÍNDICE