Plan Ceibal

Concurso público de precios

Horas de Testing

Pliego específico

Plan Ceibal

Plan Ceibal

1. Objetivo

Centro Ceibal llama a concurso público de precios para contratar horas de testing de software modalidad remota o in situ para asegurar la calidad de proyectos y soluciones brindadas por la institución.

Este llamado tiene como objeto la adquisición de **hasta 1000 horas de Testing Funcional Manual**, de **hasta 1400 horas de Testing Funcional Automatizado**, y de **hasta 500 horas de Testing Especializado**, a ser ejecutadas en un plazo de hasta dos años, según las necesidades de Centro Ceibal, en modalidad bajo demanda previa coordinación.

	Testing Funcional Manual	**Testing Funcional Automatizado**	**Testing Especializado**
Tipos de Testing	Hasta **1000 horas** para diseño y ejecución manual de casos de prueba, reporte de incidentes detectados e informes de calidad del producto.	Hasta **1400 horas** para formación, análisis, definición, desarrollo, implementación y mantenimiento de scripts de testing funcional automatizado sobre sistemas considerados críticos para el negocio.	Hasta **500 horas** para tareas de capacitación específica, consultoría o diagnóstico relacionadas al testing de performance, pruebas de accesibilidad, o experiencia de usuario, sobre sistemas considerados críticos para el negocio.

Cada oferente deberá ofertar cotización por todos tipos de testing, teniendo en cuenta los perfiles necesarios para cada modalidad.

Testing Funcional Manual

Se solicitarán hasta 1000 horas para testing funcional manual de sistemas Web y Mobile. Se deberá asegurar que la aplicación o sistema funcione de forma correcta de acuerdo a los requerimientos brindados por el equipo de desarrollo en las diferentes etapas del mismo. Se podrán solicitar pruebas de compatibilidad del software en diferentes plataformas (hw, sistemas operativos, navegadores), pruebas de integración (asegurando el correcto funcionamiento y comunicación entre los diferentes módulos del sistema e interactuando con otros) y pruebas de regresión.

Centro Ceibal gestionará los proyectos, dividiendo los requerimientos en fases o sprints, utilizando principalmente metodologías ágiles, dependiendo del proyecto.

Para cada fase o sprint, se entregarán los requerimientos a la empresa adjudicada, quien deberá elaborar un plan de pruebas que permita estimar el esfuerzo de testing necesario.

Durante el proceso, será necesario diseñar y documentar los casos de prueba según la estrategia que Ceibal considere más conveniente para la etapa del proyecto (smoke test, testing exploratorio, etc según corresponda),

Al finalizar cada fase o sprint, se deberá entregar informe con el resultado de las pruebas ejecutadas.

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

En todos los casos, 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.

Testing Funcional Automatizado

Hasta 1400 horas para formación, análisis, definición, desarrollo, implementación y mantenimiento de scripts de testing funcional automatizado sobre sistemas considerados críticos para el negocio.

Para algunos proyectos de la organización, en los cuales se aplican mejoras continuas de desarrollo, se requiere cobertura de pruebas que actualmente insumen mucho tiempo dado que su ejecución se realiza en forma manual; por esta razón, se implementó un sistema automatizado de pruebas de regresión de aquellas funcionalidades más críticas que aportan agilidad al proceso de testing, así como también de aquellos sistemas que por su complejidad en la cantidad de casos de uso, requieren mucho tiempo de testing en cada ciclo.

Se requiere seguir incrementando funcionalidades en la cobertura básica, manteniendo al día la automatización al ritmo de los cambios implementados en desarrollo, y explorar nuevas oportunidades de mejora.

Se podrán solicitar análisis automáticos de código , diseño, ejecución e implementación de casos de pruebas automatizados, así como puntualmente el diseño y ejecución de pruebas de rendimiento sobre sistemas con el objetivo de conocer cuellos de botella que afecten la experiencia de usuario.

Al finalizar cada etapa de trabajo planificado, se deberá entregar informe con el resultado de las pruebas ejecutadas y todos los elementos necesarios para operar los scripts en ceibal en futuros proyectos, así como la transferencia de conocimiento requerida para el mantenimiento.

Se acordarán con el proveedor las etapas de transferencias de conocimiento y auditorías de testing durante el transcurso del proyecto; las mismas se realizarán de forma presencial en Ceibal. Se podrán coordinar además reuniones presenciales o por videoconferencia de forma periódica, según lo requiera la naturaleza del proyecto.

En ambos casos, 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.

Testing Especializado

Hasta 500 horas para tareas de capacitación específica, consultoría o diagnóstico relacionadas al testing de performance, pruebas de accesibilidad, o experiencia de usuario, sobre sistemas considerados críticos para el negocio.

Algunos proyectos de la organización, en los cuales se aplican mejoras continuas de desarrollo, requieren ser probados desde nuevos ángulos o puntos de vista diferentes para aportar calidad y mejorar la experiencia de los usuarios finales.

Se podrán solicitar análisis, informes o diagnósticos, así como también el diseño y ejecución de pruebas de carga y rendimiento sobre sistemas con el objetivo de conocer cuellos de botella que afecten la experiencia de usuario.

Al finalizar cada etapa de trabajo planificado, se deberá entregar informe con el resultado de las pruebas ejecutadas y todos los elementos necesarios para disponer en ceibal en futuros proyectos, así como la transferencia de conocimiento requerida para casos específicos

Se listan a modo de ejemplo algunas metodologías o tipos especializados de pruebas que resultan de particular interés para implementar en el área, proyectando su crecimiento: Testing de Performance, Pruebas de Usabilidad, Pruebas de Aceptación del Usuario, Pruebas de Accesibilidad, Test Driven Development (TDD) , entre otras.

Se acordarán con el proveedor las etapas de transferencias de conocimiento y auditorías de testing durante el transcurso del proyecto; las mismas se realizarán de forma presencial en Ceibal. Se podrán coordinar además reuniones presenciales o por videoconferencia de forma periódica, según lo requiera la naturaleza del proyecto.

En todos los casos, 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.

2. Características del servicio

2.1. Especificaciones Funcionales

El oferente deberá contar con sólidos conocimientos en las siguientes herramientas y técnicas de testing,

	Especificaciones Funcionales	
Tipos de Testing	Excluyentes	No excluyentes (se valorará)
Testing Funcional Manual	• Testing de caja negra • Testing exploratorio • Árboles de decisión y máquinas de estado • Herramientas de gestión de incidentes • Testing sobre dispositivos móviles.	• Certificaciones ISTQB o similares
Testing Funcional Automatizado	• Herramientas de gestión de incidentes • Soap UI • Selenium	• Jenkins • Appium • Certificaciones ISTQB o similares
Testing Especializado	• Herramientas de gestión de incidentes • UX/UI • Jmeter • Accesibilidad	• TDD • TDP

2.2. Forma de trabajo

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

Se utilizará redmine/Mantis/JIRA/Trello o similar como herramienta para gestión, tanto de estimaciones como de incidentes. Dicha herramienta será provista por Ceibal.

Una vez acordado con Ceibal las horas que insumirá el desarrollo de cada fase, documentación requerida y la fecha de entrega de la misma, la empresa adjudicataria realizará el desarrollo o ejecutará las pruebas correspondientes.

Mensualmente se realiza un control de las horas efectivamente utilizadas, que serán las horas facturadas de ese mes.

Los servicios serán prestados principalmente en forma remota; no obstante, en proyectos puntuales cuando así se requiera, se podrá solicitar presencia en Ceibal para la ejecución de las pruebas.

La empresa oferente contará con ambientes de testing donde deberá realizar el testeo de todos los requerimientos funcionales y no funcionales. El ambiente de testing será representativo de los ambientes productivos y será brindado por Ceibal.

Se deberá compartir con Ceibal a efectos de auditar los procesos de testing, planes, inventarios de prueba y toda la documentación pertinente para cada etapa del proceso.

Se utilizará la herramienta Mantis Calidad para la gestión de sugerencias, reclamos, y no conformidades que se detecten durante los proyectos asignados.

3. Oferta

3.1. Modalidad de cotización

El oferente deberá cotizar las horas de testing en el siguientes cuadro::

Horas de testing de software - Pesos uruguayos			
	Completar todas las celdas en blanco		
	Testing Funcional Manual [1] (hasta 1000 horas)	**Testing Funcional Automatizado [2]** (hasta 1400 horas)	**Testing Especializado [3]** (hasta 500 horas)
	Costo unitario (imp. incl.)		
Cotizar **por hora**			
Trabajos fuera de Horario de oficina[4] - Cotizar **por hora**			

Todos los costos necesarios para brindar el servicio (conexión a internet, computadoras, teléfono, transporte, accesos a ambientes de desarrollo y pruebas, etc), costo por viático y horas de transferencia de conocimiento deberán ser asumidos por el proveedor (Centro Ceibal estima hasta 120 horas para testing funcional manual y hasta 120 para testing automatizado y performance). La efectiva contratación del servicio comenzará luego de que finalice la transferencia de conocimiento.

[1] Cotizar un único precio por todos los roles involucrados en testing Manual (Tester Senior o Tester Junior) tanto en modalidad remota como in situ.
[2] Cotizar un único precio por todos los roles involucrados en alguna de las especialidades (QA Manager, Líder de Testing, Tester Senior, Docentes o Consultores) tanto en modalidad remota como in situ.
[3] Cotizar un único precio por todos los roles involucrados en alguna de las especialidades (QA Manager, Líder de Testing, Tester Senior, Docentes o Consultores) tanto en modalidad remota como in situ.
[4] Horario de oficina: lunes a viernes de 9:00 a 18:00 días hábiles.

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

3.2. Presentación de la oferta

La empresa oferente deberá presentar propuesta *por cada tipo de testing*, cumpliendo en cada uno de ellos los elementos y condiciones que se mencionan a continuación.

La oferta debe incluir en forma obligatoria los siguientes elementos:

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

a. Sección 2.1 - Especificaciones **funcionales obligatorias excluyentes**: se deberá contar con experiencia en al menos 5 proyectos en los últimos 3 años, sumando un total de al menos 10.000 horas dedicadas.

b. Sección 2.1 - Se valorará tener experiencia acreditada en proyectos en las herramientas descritas o no descritas en las especificaciones **obligatorias no excluyentes**, Se considerarán antecedentes de los últimos 3 años.

c. Se valorará tener experiencia acreditada en proyectos vinculados a enseñanza, hacking ético o pruebas de performance, orientados al aseguramiento de la calidad.

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

3.2.2. Presentación del equipo de trabajo, incluyendo currículos del personal que será responsable de prestar el servicio en cada tipo de testing. Deberán incluir formación y experiencia relevante en testing.

3.2.3. Oferta económica (3.1 - Modalidad de cotización)

4. Evaluación

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

Evaluación	
	% Evaluación máximo
3.2.1 Antecedentes	45
3.3.2 Análisis Cvs	25
Oferta económica	30
Total	**100**

5. Propiedad intelectual

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.

Todos los trabajos realizados a raíz de la contratación de este servicio serán de propiedad intelectual exclusiva de Centro Ceibal a quien tales derechos desde ya se entienden cedidos.

6. 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. Caso contrario, la Empresa se compromete a contar con el consentimiento del titular del dato para la transferencia a un territorio no adecuado, o a que el importador haya suscrito cláusulas contractuales tipo con el exportador o posea un Código de Conducta inscripto, con la consecuente autorización de transferencia 18 internacional de datos tramitada ante la Unidad Reguladora y de Control de Datos Personales, en los dos últimos supuestos.

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.

Anexo

I. Presentación de antecedentes

A. Testing Manual

Los antecedentes deben ser igual o mayor a 5 proyectos.

Técnicas de testing - Herramientas	N° de proyecto/s (1)	Nombre/s del proyecto (2)	Total de horas por proyecto	Total de horas por tecnología	Total de horas acumuladas (últimos 3 años) >= 10.000
Especificaciones obligatorias excluyentes					
Testing en caja negra	1.				
	2...				
Testing Exploratorio					
Árboles de decisión y máquinas de estado					
Herramientas de gestión de incidentes					
Testing sobre dispositivos móviles					

Especificaciones obligatorias no excluyentes					
Certificaciones ISTQB o similares					
Otros					
Otros (Se valorará experiencia en Proyectos de educación)					

B. Testing Automatizado

Técnicas - Herramientas	**N° de proyecto/s (1)**	**Nombre/s del proyecto (2)**	**Total de horas por proyecto**	**Total de horas por tecnología**	**Total de horas acumuladas (últimos 3 años) >= 10.000**
Especificaciones obligatorias excluyentes					
Herramientas de gestión de incidentes					
Soap UI					
Jmeter					
Selenium					
Especificaciones obligatorias no excluyentes					
Jenkins					

Appium					
Certificaciones ISTQB o similares					
Otros					
Otros (Se valorará experiencia en Proyectos de educación)					

C. Testing Especializado

Metodología - Herramientas	**N° de proyecto/s (1)**	**Nombre/s del proyecto (2)**	**Total de horas por proyecto**	**Total de horas por tecnología**	**Total de horas acumuladas (últimos 3 años) >= 10.000**
Especificaciones obligatorias excluyentes					
Herramientas de gestión de incidentes					
UX/UI					
Jmeter					

Accesibilidad					
Especificaciones obligatorias no excluyentes					
TDD/TDP					
Appium					
Certificaciones ISTQB o similares					
Otros					
Otros (Se valorará experiencia en Proyectos de Capacitación)					

Ordenar del más reciente al más antiguo, por tipo de testing. Se valorarán sólo antecedentes de los últimos 3 años (deberán ser al menos 5 proyectos)

Ingresar la sumatoria de las horas dedicadas de todos los proyectos, que deberá sumar al menos 10.000 horas.

Considerar separar información y cuadros por cada tipo de testing.

N° proyecto (1)	Nombre del proyecto (2)	Institución contratante	Contacto responsable de dicha institución, cargo, télefono, mail	Descripción y alcance del proyecto	Período en el que fue realizado Duración en meses	Cantidad de integrantes del equipo de trabajo Nombres y roles de los responsables	Horas dedicadas en total	Técnicas de Testing utilizadas - Herramientas de testing utilizadas.	Hipervínculo a la carta de recomendación (si hubiere)

II. Acuerdos de Calidad del Servicio

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.

2. Acuerdos de nivel de Servicio

En cada proyecto asignado, 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.

3. 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
- b. Seguimiento de pendientes
- c. Notificación oportuna de posibles retrasos

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

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

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

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

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

Se entiende como Reclamo aquellos incumplientos sobre cualquiera de los parámetros descritos anteriormente (punto 2.2 anterior) que impacten de forma negativa sobre la continuidad del proyecto.

Se considera una No conformidad cuando se incumplen los plazos acordados con el Centro Ceibal de cualquiera de los hitos que conforman Análisis y Diseño y Ejecución, 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 puntos 1, 2 Y 3.

Fuera de estos casos, ante incumplimiento grave de parte de la Empresa, Centro Ceibal podrá rescindir el contrato inmediatamente sin responsabilidad, ejecutar la garantía de cumplimiento de contrato y aplicación de las penalidades correspondientes, según puntos 1, 2 Y 3.

- Análisis y Diseño

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

- Ejecución

Hito comprometido	**Retraso Aceptable**
Entrega de evidencia de pruebas ejecutadas / Reporte de errores detectados/ mantenimiento solicitado de Scripts de pruebas.	Una semana desde la fecha acordada

4. PENALIZACIÓN

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

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

III. Presentación de CVs

Presentar información por tipo de Testing.

Cuadro Resumen

Roles (según configuración del equipo): QA Manager, Líder de Testing, Tester Senior, otros

Rol	Nombre y Apellido	Dedicación (parcial o completa)

Cuadro por integrante

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

Cargo propuesto			
Perfil			
Educación			
Certificaciones/ Cursos relevantes			
Experiencia relevante para el llamado	Herramientas de Testing - Técnicas de Testing Especificar cantidad de años en el cargo propuesto	Tiempo de experiencia: Proyectos URL (si corresponde)	
Historia Laboral	Desde	Hasta	Empresa/Rol/Principales actividades
Certificados (si corresponde			

IV. Requisitos de seguridad de la información para la compra de sistemas informáticos y horas de desarrollo

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

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

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

Descripción de requisitos:

- **Diseño y arquitectura**

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

Deberá cumplir los siguientes requisitos:

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

- **Autenticación**

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

Deberá incorporar los siguientes requisitos:

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

- **Gestión de sesiones**

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

Para esto deberá:

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

- **Control de acceso**

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

Para esto deberá cumplir que::

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

- **Codificación y validación**

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

La solución deberá cumplir con:

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

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

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

Para lograr esto la solución deberá:

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

- **Confidencialidad y Protección de datos**

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

- Cumplir con la normativa vigente uruguaya en materia de datos personales (Ley Nº 18.331, de 11 de agosto de 2008 y Decreto Nº 414/2009, de 31 de agosto de

2009). Se considera dato personal la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, a modo enunciativo, cualquier información numérica, alfabética, gráfica, fotográfica, registro de voz e imagen, acústica o de cualquier otro tipo que refiera a ellas directa o indirectamente, conforme con lo dispuesto en el artículo 4 de la Ley 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. .
- 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 subcontratadas, 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 Centro Ceibal establezca.

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

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

- **Uso de archivos y recursos**

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

Para esto debe cumplir con:

- Los archivos inseguros deben ser gestionados adecuadamente de manera de garantizar la confidencialidad, integridad y disponibilidad de la información.
- Se deberán implementar controles para la subida, ejecución, bajada y alojamiento de los archivos que blinden la solución de ataques maliciosos y configuraciones inadecuadas como por ej.: bombas zip, tipos de archivos incorrectos, ataque pass traversal, alojamiento con permisos o en directorios incorrectos, ataque SSRF.

- **API y Web services**

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

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

- **Respaldos y contingencia**

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

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

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

- **Criptografía**

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

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

- **Código malicioso**

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

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

- **Lógica de negocio**

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

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

- **Configuración**

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

Los mismos deberán incluir:

- Un entorno lo más seguro, repetitivo y automatizable posible a través de la incorporación de buenas prácticas (ej. modelo DevSecOps) con herramientas, procesos y tecnologías que la * implementen adecuadamente (ej. contenedores, despliegues automatizados, etc.).
- Herramientas y entornos de desarrollo actualizados y correctamente mantenidos.
- Herramientas y entornos de desarrollo correctamente configurados y verificados en su seguridad (hardening) como por ej. deshabilitar el modo debug en entornos de producción.
- Seguridad por defecto en las configuraciones de los usuarios y los permisos.

- **Certificaciones**

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

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

- **Metodología**

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

- **Análisis de vulnerabilidades**

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

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

Matriz de cumplimiento de requerimientos de Seguridad de la Información

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

15	Configuración	Deseado		
16	Certificaciones	Deseado		
17	Metodologías	Deseado		
18	Análisis de vulnerabilidades	Deseado		

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

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

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

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

Fin del documento