LLAMADO SITIO WEB Y CRM

FUNDACIÓN CEIBAL

Índice

SOLICITUD DE PROPUESTAS

1. Introducción

La Fundación Ceibal es una institución autónoma y sin fines de lucro cuyo objetivo es generar y promover el desarrollo de investigación en educación y tecnología, así como favorecer la transferencia de conocimiento y la creación de capacidades.

2. Contexto

La Fundación Ceibal busca resolver desafíos relacionados con el aprendizaje y la mediación de las tecnologías, a través de metodologías innovadoras y un abordaje práctico, social y participativo. Está orientada a problematizar y aportar ideas y soluciones a la implementación actual y futura del Plan Ceibal y de otros actores educativos nacionales e internacionales.

Desde el inicio de sus actividades, en 2015, la Fundación logró posicionarse como una reconocida institución a nivel nacional, regional e internacional, insertándose y conformando redes de excelencia en investigación e innovación. Realizó más de 70 proyectos, 60 conferencias y 150 publicaciones.

3. Objeto

La divulgación y el fomento a la investigación, así como la innovación en el ámbito educativo son parte esencial de la misión institucional. En este marco la Fundación se ha propuesto como parte de su estrategia 2020-2024 la conformación y fomento de una comunidad de actores relevantes asociados a estas temáticas con el fin de instaurar un ámbito de discusión apropiada para encontrar soluciones en un entorno tan desafiante para los sistemas educativos.

Con esto presente la Fundación Ceibal necesita de herramientas que le permitan desarrollar y gestionar dicha comunidad a través de nuevos y potentes canales de comunicación.

El presente llamado solicita entonces la cotización para realizar rediseño del sitio web institucional, y la implementación asociada de un proceso de gestión de contactos y actividades (basada en CRM - Customer Resource Management).

4. Productos

La propuesta deberá considerar la entrega de la totalidad de los siguientes puntos:

A. Rediseño del sitio web de la Fundación Ceibal que tenga un fuerte impacto visual y presente los elementos principales de la marca Fundación Ceibal de un modo novedoso planteando interacciones en la lectura.

   El nuevo sitio deberá contemplar:
   - Albergar información institucional
   - Contener un espacio de novedades con contenidos multimedia.
   - Integrar visualmente desde la experiencia de usuario el repositorio actual de investigaciones y publicaciones.

- Desarrollar e integrar un espacio para presentar webinars, instancias de formación y otros productos audiovisuales.
- Tener capacidad para integrar otro portal de menor tamaño ya existente.
- Auto-registro de interesados con datos básicos y flujo definido en función de la categoría de cada tipo de interesado, ej: institución financiadora, investigador, representante de sistemas educativos del exterior, interesados de instituciones asociadas, público general, etc.

  Dichos flujos deberán considerar:

  i. Registro datos del nuevo contacto / usuario (con integración y alta automática en un CRM que también será parte de la propuesta).
  ii. Formulario de solicitud a la Fundación según el perfil, ej: reunión, información, bibliografía, etc. Desencadenando en integración con el CRM diferentes acciones pendientes.
  iii. Inscripción para la participación de diferentes eventos (webinars, talleres, capacitaciones, etc.).
  iv. Integración con una herramienta CRM que deberá formar parte de la propuesta.

  NOTA: En este punto lo que se requiere es la implementación (o parametrización) de formularios para auto-registro, inscripción a evento, solicitud de información o consulta los cuales deben estar disponibles en la WEB institucional. Dichos formularios deberán generar una acción que se refleje en el CRM, se espera que la lógica de estas casuísticas sea resuelta por la herramienta del CRM.

Este ítem incluye cualquier tipo de licenciamiento necesario para el funcionamiento, así como el hosting anual de todo el sitio WEB.

B. CRM de contactos integrado al sitio web para el alta de registro, inscripciones, solicitudes o consultas. El servicio del CRM podrá ser prestado en modalidad SaaS (se valorará este tipo de soluciones siempre que sean estándares del mercado) y en este caso el precio de suscripción deberá ser incluido en el costo de la propuesta (por un año) y será registrado a nombre de la Fundación. Este ítem incluye cualquier tipo de licenciamiento necesario para el funcionamiento, así como el hosting anual (en caso de corresponder) de la solución de CRM.

   NOTA: En caso de que la oferta considere un software on premise la propuesta deberá considerar el hosting por un periodo anual.

C. Capacitación para personal de la Fundación Ceibal para la gestión del sitio web y del CRM y entrega de los manuales (o instrucciones) de uso correspondientes.

D. Mantenimiento correctivo (corrección de errores detectados en producción), garantía de funcionamiento (detallando política de respaldos), hosting de la solución y soporte técnico de todos los productos anteriores por 12 meses a partir de la puesta en producción, incluyendo todas las rutinas de mantenimiento necesarias en toda la solución para asegurar el óptimo desempeño del sitio, accesibilidad, navegabilidad, etc.

Existe el requisito obligatorio de cotizar los siguientes productos de adquisición opcional:

E. Paquete de horas de desarrollo de hasta 100 horas de mantenimiento evolutivo.

F. Extensión del (producto D) mantenimiento correctivo (corrección de errores detectados en producción), garantía de funcionamiento (detallando política de respaldos), hosting de la solución y soporte técnico por 12 meses adicionales.

5. Etapas mínimas previstas para el desarrollo de los productos

A. Plan de trabajo: Presentación del plan de trabajo, conteniendo cronograma, fecha de entregables (presentación de diseño, presentación de funcionalidades, versiones prototipo, versión de testing, versión de producción, capacitación, etc.), responsables de ejecución y de validación.
B. Definición del alcance:
    a. Análisis de requerimientos y ajustes de cronograma
    b. Presentación del borrador de la web con los principales aspectos de diseño
    c. Documento con requerimientos funcionales y no funcionales
    d. Diseño de la arquitectura con las alternativas de integración del CRM
    e. Diseño de los procesos de negocio
C. Desarrollo de productos:
    a. Migración de contenidos y desarrollo de contenidos nuevos
    b. Entregable de prototipos para aprobación inicial (al menos uno)
    c. Entregable con versión de testing
    d. Parametrización y configuración inicial del CRM
    e. Entregable para validación y puesta en producción
D. Documentación:
    a. Manuales de uso del sistema
    b. Instructivos técnicos (instalación, configuración, parametrización, monitoreo, respaldo y acciones de contingencia)
    c. Parametrizaciones iniciales y método de actualización y resguardo
    d. Esquemas de permisos y roles e instrucciones para adaptarlos
    e. Procesos de negocio sistematizados
E. Capacitación de personal y entrega de manuales adaptados

6. Consideraciones generales

A. El sitio web será diseñado en español y debe tener su versión en inglés (los contenidos tanto en español como en inglés serán brindados por la Fundación Ceibal).
B. La empresa debe contemplar la migración de todos los contenidos que tiene hoy el sitio web de la Fundación tanto en su versión en español como en inglés.
C. Los derechos de autor y el código desarrollado en el marco de esta contratación, así como cualquier otro derecho intelectual protegido, pertenecen exclusivamente a la institución contratante. Sin perjuicio que podrán utilizarse en cualquier etapa de la construcción materiales con licencias abiertas.
D. Fecha prevista de puesta en producción: máximo 90 días luego de adjudicado.
E. Sitio web de referencia estética: https://cambridge.nuvustudio.com/

F. ANEXO 1 - Especificaciones técnicas sitio web
G. ANEXO 2 - Gestión de contactos a través de la integración pagina web - CRM
H. ANEXO 3 - Formato para la presentación de antecedentes
I. ANEXO 4 - Requisitos de Seguridad

7. Presentación y evaluación de propuestas

A. Antecedentes: Se solicita presentar antigüedad de permanencia en el mercado de la empresa con un máximo de 5 antecedentes de trabajos anteriores similares a los solicitados en el presente llamado respetando el formato correspondiente al ***Anexo 3*** del presente TDR.
B. Plan de Proyecto:
    - Asunciones: En esta sección se podrá aclarar cualquier supuesto necesario para lograr el éxito del proyecto, como puede ser el tiempo de respuesta para con la Fundación Ceibal así como los recursos necesarios que la Fundación deba brindar, entre otros.
    - Cronograma tentativo: Especificar fecha posible de inicio del trabajo, actividades, hitos principales y duración total del proyecto. Se valorarán cronogramas razonables en su asignación de recursos y duración de actividades que sean menores a 90 dias.
C. Descripción de la solución propuesta: indicar características funcionales y técnicas de la solución propuesta explicitando la justificación de la pertinencia de cada componente para resolver el problema planteado.
D. Método de Trabajo: Describir específicamente cómo se va a trabajar y cuál es su implementación práctica, debe ser real, simple y llevada a este proyecto en particular.
    - Validación y testing: Indicar cómo se realizará el testing de los diferentes entregables, qué tipo de testing, a quién involucra.
    - Documentación, capacitación, transferencia, sugerencias.
    - Garantía: Indicar qué garantía se brindará al producto final. No podrá ser menor a 12 meses.
    - Soporte: características del nivel de servicio brindado por la propuesta (tiempos de respuesta, horario de atención, canales de comunicación, registro de incidentes, etc.)
E. Propuesta económica: Cotizar el costo del proyecto, desglosando el costo según se indica en el punto 10 del presente documento.

8. Criterios de Evaluación

1. Antecedentes (20%)
2. Solución propuesta (50%)
    - Arquitectura de la solución (10%)
    - Solución y diseño de página Web (20%)
    - Propuesta de CRM con integración al sitio Web (20%)
3. Precio (30%)

9. Plazos de entrega

Todos los productos deben ser entregados según el cronograma acordado al inicio del contrato.

10. Cotización de la propuesta:

Item de la propuesta	Precio (*)	Observaciones
● Rediseño, desarrollo e implementación del Portal institucional ○ Requerimientos y plan de trabajo ○ Boceto del sitio, con diseño y características generales y distintivas ○ Diseño, desarrollo e implementación ○ Desarrollo de la integración entre el portal y el CRM, así como de los casos de uso necesarios. ○ Migración de contenidos desde el portal actual de la institución. ○ Hosting anual		
● Solución CRM integrada con el portal institucional ○ Requerimientos y plan de trabajo ○ Diseño, desarrollo, parametrización, e implementación ○ Desarrollo de la integración entre el portal y el CRM, así como de los casos de uso necesarios. ○ Carga de las bases de contactos actuales ○ Hosting anual		
● Costo de licenciamiento anual de la solución (si corresponde) discriminada por producto. Ej: licencias del CRM, complementos del CMS, etc.		
● Capacitación ○ Para el mantenimiento y actualización de la WEB ○ Para el uso y gestión del CRM ○ Técnica la comprensión general de la solución. ○ Manuales, instructivos y documentos		
● Mantenimiento correctivo y soporte técnico		

Corrección de errores detectados, administración del hosting, soporte técnico por 12 meses a partir de la puesta en producción incluyendo todas las rutinas de mantenimiento necesarias en toda la solución para asegurar el óptimo desempeño del sitio, accesibilidad, navegabilidad, etc.		
Item de la propuesta (cotización obligatoria y adjudicación opcional)	**Precio**	**Observaciones**
● Paquete de hasta 100 horas de mantenimiento evolutivo .		
● Extensión del hosting, mantenimiento correctivo y soporte técnico por 12 meses Administración del hosting y soporte técnico por 12 meses a partir del segundo año incluyendo todas las rutinas de mantenimiento necesarias en toda la solución para asegurar el óptimo desempeño del sitio, accesibilidad, navegabilidad, etc.		

(*) Cotizar en pesos uruguayos o dólares estadounidenses con los impuestos desglosados. En caso de no desglosar los mismos se entenderán incluidos en el precio total ofertado. A efectos comparativos se considerará el valor del dólar billete del BCU al día anterior de la fecha de apertura.

11. Forma de pago

Se abonará contra la aprobación de cada producto y entrega de materiales asociados. La forma de pago es hasta 30 días corridos desde la fecha de facturación mediante transferencia bancaria.

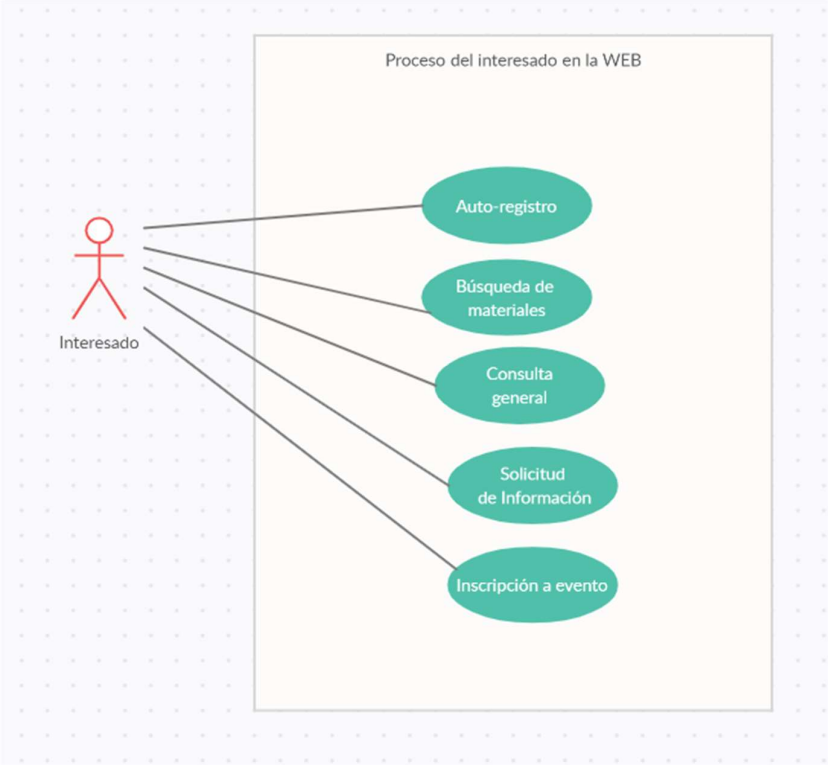
Plan de trabajo y diseño	Testing Validación	Puesta en Producción	Cierre (al mes de la puesta en producción)
10%	**20%**	**40%**	**30%**

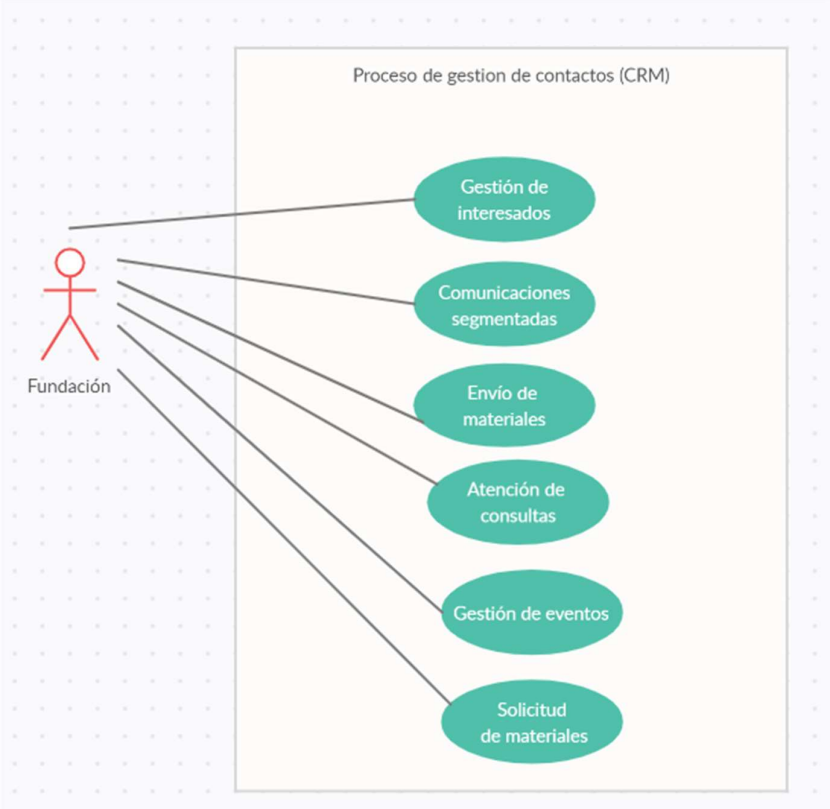
Nota: los valores anteriores se basan en el total de los ítems no opcionales. En caso de los opcionales se abonarán de la siguiente manera: En el caso de las horas contra el consumo efectivo y en el caso de los servicios según acuerdo de las partes en modalidades mensual, bimestral o trimestral

ANEXO 1 - Especificaciones técnicas sitio web

1. Desarrollado en October CMS o Wordpress (en las últimas versiones estables)
2. Responsive y optimizado para los navegadores más usados (Chrome, Explorer, Firefox y Safari). Considerando compatibilidad hacia atrás con las versiones más populares de estos navegadores.
3. Las interoperabilidades definidas en la arquitectura presentada por el proveedor deberán estar claramente documentadas, y desarrolladas utilizando estándares abiertos (en base a servicios web (REST).
4. El código fuente de los desarrollos específicos será propiedad intelectual de la Fundación y deberá ser entregado como producto. La modificación de dicho código deberá ser posible a través de herramientas abiertas.
5. El proveedor debe seguir las pautas de desarrollo proporcionadas por Fundación - Ceibal, que especifica, entre otros puntos, nomenclatura, manejo de repositorio de código fuente, versiones de software base a utilizar y buenas prácticas de desarrollo.

ANEXO 2 - Gestión de contactos a través de la integración pagina web -CRM





ANEXO 3 - Formato para la presentación de antecedentes

#	Antecedente	Cliente/Contacto	Tipo Contrato	Descripción de los Entregables	Equipo	Duración del contrato
1	*Manual de marca*	*Plan Ceibal, Ana López, tel: 29003333*	*Subcontratado*	*Manual de marca, diseño pagina web, plantillas ppt.*	*Diseñador gráfico, diseñador web, ilustrador*	*4 meses*
2			*Proveedor Principal*			
3			*Consorcio*			

Ejemplos:

#1: (Opcional - Incluir aquí ejemplo de los entregables relevantes)

ANEXO 4 - Requisitos de Seguridad

			A completar Proveedor	
Nº Req.	**Requerimiento**	**Tipo**	**Cumplimiento**	**Observaciones**
1	*Diseño y Arquitectura*	*Deseado*	*SI/NO*	
2	*Autenticación*	*Obligatorio*		
3	*Gestión de sesiones*	*Obligatorio*		
4	*Control de acceso*	*Obligatorio*		
5	*Codificación y validación*	*Deseado*		
6	*Manejo de errores y logs*	*Deseado*		
7	*Confidencialidad y protección de datos*	*Obligatorio*		
8	*Comunicaciones*	*Deseado*		
9	*Uso de archivos y recursos*	*Deseado*		
10	*API y Web Services*	*Deseado*		
11	*Respaldos y contingencia*	*Deseado*		
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*		

1. *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.

2. *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.

3. *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).

4. *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.

5. *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.

6. *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)

7. *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, comunicarnos 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 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.

8. *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.

9. *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.Requisitos
- 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.

10. *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.

11. *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).

12. ***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.

13. ***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.

14. ***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.

15. ***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.

16. ***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

17. ***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.

18. ***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.