Concurso Público de Precios
Pliego de condiciones Particulares
PRÓRROGA

1. Objeto

Plan Ceibal llama a concurso público de precios a empresas interesadas en el **rediseño, desarrollo y mantenimiento del Portal Estudiantil de Plan Ceibal** https://estudiantes.ceibal.edu.uy/.

Las empresas interesadas deberán proponer un rediseño del portal estudiantil a través de una propuesta creativa con elementos de gamificación, que refuerce el concepto de entorno Ceibal seguro y personalizado, donde el usuario tenga fácil acceso a las noticias y recursos educativos acordes a sus intereses y necesidades.

Asimismo, la propuesta debe contemplar elementos de gamificación como la integración con Logros, la creación de un avatar, la personalización del sitio para generar más interacción entre el portal, los recursos educativos, las plataformas y las distintas áreas de Ceibal, contando con una comunicación clara y una experiencia atractiva que incentive la creatividad e invite a profundizar en los contenidos ofrecidos.

Antecedentes

El Portal de estudiantes, es la principal puerta de entrada a las propuestas y contenidos educativos de Ceibal.. En lo que va del 2020 se han realizado más de 30 millones de sesiones, con un promedio de 100.000 usuarios por día, y 15 sesiones por usuario. Estos usuarios pasan por el portal y usan los accesos directos a las plataformas como Biblioteca, CREA, PAM, Matific, REA, además de otros recursos como videos, videojuegos y Logros, el sitio de desafíos gamificados.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

De esta manera todas las propuestas educativas y contenidos previamente evaluados por Ceibal, se encuentran nucleadas en un solo lugar seguro, accesible e intuitivo, al que se puede acceder desde todos los dispositivos con conexión a Internet.

Información general

El Portal Estudiantil es por defecto la página inicial para los navegadores de los dispositivos de Plan Ceibal y en gran medida sirve para acceder a los diferentes recursos y plataformas ya que concentra todos los accesos directos y links de interés. Es el lugar ideal para que el estudiante pueda buscar y encontrar los recursos a su disposición, y enterarse de las propuestas de actividades y noticias que se le ofrecen.
El objetivo de este llamado, es rediseñar el Portal Estudiantil utilizando como base el portal actual, para mejorar e incentivar el uso de los recursos, a través de mejoras y personalizaciones de la experiencia de usuario y elementos de gamificación que contribuyan a generar una sinergia entre el portal y los estudiantes.

Es posible ingresar al portal estudiantil accediendo desde el portal de Plan Ceibal (https://www.ceibal.edu.uy/es) o directamente con el link estudiantes.ceibal.edu.uy . El portal es de libre acceso, sin embargo tiene algunos contenidos y recursos restringidos disponibles solo para beneficiarios de Plan Ceibal una vez autenticados a través de nuestra plataforma central de login ingreso.ceibal.edu.uy.
Con el propósito de facilitar la visualización del portal estudiantil actual, sus características y funcionamiento, se ha creado el siguiente usuario de prueba:

usuario: userdemo1
contraseña: C3ib4L.2020

Público

Una vez iniciada la sesión, el público que accede al contenido personalizado del portal está conformado por todos los beneficiarios de Plan Ceibal que sean estudiantes del sistema de

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

educación pública del Uruguay, es decir usuarios desde los 5 años a los 15+.

2. Plazos y fechas

El portal deberá estar funcionando en producción para Mayo de 2021.

Se realizará una reunión informativa virtual el Jueves 21 de Enero 2021, 14:30 horas. Los interesados deberán contactarse a través del mail compras@ceibal.edu.uy donde se les proveerá el link correspondiente. Deberán inscribirse a través del email compras@ceibal.edu.uy, debiendo realizar dicha inscripción con una anticipación no menor 24 hs de la fecha y hora prevista para la reunión, a los efectos de coordinar los aspectos técnicos para la conexión., indicando dirección de mail con la cual ingresaran al Meet y nombre.

3. Requerimientos obligatorios

A continuación se enumeran las funcionalidades requeridas en el nuevo diseño,

3.1. Funcionalidades ya existentes en el diseño actual

El sitio web actual ya cuenta actualmente con las siguientes funcionalidades, que la nueva propuesta también deberá incluir en el nuevo diseño:

3.1.1. Login único Ceibal

El portal estudiantil se integra con el sistema de login centralizado de Ceibal mediante protocolo CAS (versión 3.5.3 en adelante), con APIs REST brindadas por Ceibal para consultar la información del usuario.

Por más información consultar: https://wiki.jasig.org/display/CAS/Home

Si el usuario es estudiante, el sistema deberá desplegar el Portal Estudiantil, personalizando el contenido para los diferentes perfiles de acuerdo a las franjas de edad.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

3.1.2. Administración de usuario

El portal estudiantil cuenta con Login/logout al portal, cambio de contraseña, restablecimiento de contraseña.

3.1.3. Buscador

El portal cuenta con un buscador que le permitirá realizar una búsqueda dentro de los recursos del portal..

3.1.4. Accesos rápidos

El usuario cuenta con accesos rápidos a las plataformas y recursos más usados acordes a su perfil (CREA, Matific, PAM, Biblioteca País, etc). Dependiendo del dispositivo, debe alertar al usuario si accederá a través de la web o bajará una aplicación.

3.1.5. Recursos online

El portal cuenta con links a las distintas secciones con contenidos propios del sitio:

- Libros de texto
- Aplicaciones
- Videojuegos
- Videos
- Carrusel de libros
- Otros recursos y links de interés

3.1.6. Noticias

El usuario podrá ver un slideshow de noticias correspondientes a su perfil.

- Noticias
- Artículos de interés
- Cursos
- Embeber streamings de Ceibal

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

3.2. Nuevas funcionalidades requeridas

La propuesta de rediseño del portal estudiantil deberá contener y/o contemplar las siguientes nuevas funcionalidades:

3.2.1. Información del usuario

A la información del usuario se desea agregar información como la clase, el dispositivo que tiene asignado, etc. e información sobre ese dispositivo y notificaciones del servicio al usuario. Esto se hará a través de API 's que dispone Ceibal.

3.2.2. Contenido dinámico

Los contenidos ofrecidos en el Portal Estudiantil deberán adaptarse a los diferentes perfiles de usuarios, definidos acordes a los subsistemas, grados y edades. El estudiante sólo tendrá acceso al contenido que está disponible para el perfil adecuado, por lo tanto verá contenidos (noticias, videos, logros, información, etc) acordes a su edad, grado y subsistema.

3.2.3. Integración con Logros

El portal se integrará con el sistema de medallas de Ceibal llamado Logros https://logros.ceibal.edu.uy/ y buscará mejorar la experiencia del usuario, visualizando y reforzando los logros con recompensas generando incentivos para interactuar con el portal y con las plataformas y recursos de Plan Ceibal.

La plataforma deberá poder integrarse con APIs REST brindadas por Ceibal para consultar los logros asignados al usuario y obtener todos los logros disponibles.

3.2.4. Economía

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

El oferente deberá proponer un diseño de sistema gamificado de recompensas utilizando los Logros alcanzados por el usuario.
Con cada logro alcanzado con el uso de los recursos y plataformas, el usuario podrá obtener como recompensa, elementos que usará para personalizar su experiencia, por ejemplo un sombrero para modificar su avatar, un fondo de pantalla, etc. Generando la necesidad de conseguir el siguiente.

3.2.5. Creación del Avatar

Una de las grandes atracciones del portal será el avatar y la posibilidad de que el usuario pueda crear y modificar su avatar combinando elementos decorativos que irá adquiriendo a medida que consigue alcanzar los desafíos de Logros.
A medida que el usuario va alcanzando logros, podrá “reclamar” los premios correspondientes que luego le serán habilitados para customizar su avatar.

3.2.6. Notificaciones

El usuario recibirá notificaciones en el sitio, cada vez que haya alcanzado un Logro, que le indicarán el link para poder ir al logro alcanzado y reclamar su recompensa.

3.2.7. Backend

Se deberá soportar la configuración de distintos perfiles de usuarios y permisos. A modo de ejemplo:

- Contenidista: Gestión de contenidos o recursos de la web.
- Editor: Gestión de front end o maquetado del sitio.
- Administrador: Gestión de usuarios y configuración del sistema.

3.2.8. Entornos

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

Al igual que está implementado actualmente en October, el portal estudiantil deberá contar con un entorno de testing, pre-producción y producción.

3.2.9. Subir recursos en las diferentes secciones

Al igual que está implementado actualmente en October, el portal estudiantil deberá contar con una interfaz para poder subir y configurar (agregar tags, edad, keywords para la búsqueda) los contenidos y recursos nuevos a las distintas secciones, como ser noticias, videos, links a videojuegos, accesos directos a plataformas, etc.

3.2.10. Base de datos

El sitio guardará los datos necesarios de cada usuario para el funcionamiento del sitio, como por ejemplo notificaciones ya leídas por el usuario, datos del avatar creado, etc.

3.2.11. Compatibilidad con los dispositivos

Se evaluará el comportamiento responsivo de la herramienta en los dispositivos de Ceibal entregados al público objetivo del portal, teniendo en cuenta, entre otros aspectos, la adecuación al tamaño de la pantalla y la performance de los mismos. La lista de equipos es la siguiente (por más información consultar http://www.ceibal.edu.uy/es/dispositivos).

3.2.12. Estadísticas

El sitio deberá contar con herramientas para el monitoreo y análisis de uso, además de la posibilidad de trackear potenciales campañas de marketing.

4. Aspectos deseados

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

A continuación se mencionan algunos aspectos a valorar para la propuesta:

- Es deseable que la plataforma esté implementada en October CMS (https://octobercms.com/). Sin embargo Ceibal está abierto a propuestas en otras tecnologías a evaluar por el equipo de TI.
- Se valorará que la aplicación de creación del avatar contemple aspectos inclusivos.
- Se valorará que la propuesta incluya un paquete de funcionalidades de accesibilidad.
- En función de los perfiles de usuario, se valorará el manejo de tipo de letra adecuado (mayúscula 7 para primeros niveles de Educación inicial y primaria) y la utilización de recursos gráficos icónicos que potencien la comprensión del público objetivo.
- Se valorará el abordaje lúdico tanto en el diseño y estética del portal como en la integración de los elementos de gamificación.
- Se valorará la participación de un game designer en el equipo de trabajo.
- Se valorará la existencia de un departamento de QA (testing), que trabaje en conjunto con el departamento de testing de Centro Ceibal en la investigación y seguimiento de incidentes hallados en etapas de pruebas.

La empresa oferente podrá sugerir la inclusión de otros ítems no detallados en el presente documento, siendo considerados como opcionales sin obligación de compra por parte de Plan Ceibal.

5. Hosting

El hosting del Portal será provisto por Plan Ceibal.

El proveedor deberá especificar los requerimientos para los ambientes de trabajo de testing, preproducción y producción.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

6. Testing

Para cada hito que se establezca en el cronograma, el proveedor deberá presentar evidencia de testing y Plan Ceibal tendrá la opción de realizar testing adicional.

Se utilizará una herramienta de gestión a acordar con Ceibal para el seguimiento de tareas e incidentes,

7. Documentación técnica

El oferente deberá entregar el código fuente y toda la documentación relativa al desarrollo del portal, incluyendo como mínimo:

- Modelo de datos
- Interfaces con otros sistemas
- Configuración de las herramientas de desarrollo utilizadas.
- Instructivo de armado de versiones e instalación
- Evidencia de pruebas unitarias.

8. Propuesta

La propuesta debe incluir las horas de transferencia de conocimiento.

Dentro de la propuesta se evaluará el cumplimiento de los requisitos del pliego, así como la creatividad y estética del diseño, la calidad de la UI/UX, el grado de innovación, la gamificación, la adecuación al público objetivo y a la estructura de Plan Ceibal.

Cada oferente deberá presentar:

a. Memoria descriptiva propuesta del nuevo Portal Estudiantil
b. POC: Prueba de concepto, esquema ilustrativo (no necesariamente funcional) de la propuesta.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

c. Oferta económica por rediseño y desarrollo del Portal Estudiantil.
d. Costo por hora de mantenimiento evolutivo, de cotización obligatoria y adjudicación opcional.

El consultor deberá cotizar horas de desarrollo (con un máximo de 1.500 horas), las cuales serán demandadas en caso que Centro Ceibal requiera ajustes identificados en etapas posteriores a la fase de implantación

Franja
Hasta 100 horas
Entre 101 y 250 horas
Entre 251 y 500
Entre 501 y 1000
Entre 1000 y 1500 horas

* Cotizar precio unitario Hora para cada una de las franjas

e. Tabla de Cumplimiento de Seguridad de la Información: disponible en el ANEXO I
f. Antecedentes empresariales del oferente y porfolio de soluciones similares a la problemática planteada. Se valorará experiencia en gamificación y juegos educativos.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

g. Cronograma tentativo de desarrollo y facturación: incluyendo propuesta de reuniones de trabajo en Plan Ceibal y coordinación con el equipo de comunicación de Plan Ceibal.
h. Composición del equipo de trabajo (incluyendo CVs de los participantes del equipo)
i. Demo/Presentación de la propuesta a Ceibal.

.

8.1. Evaluación

Para la evaluación técnica de las propuestas, se considerarán los aspectos de la siguiente forma:

- Antecedentes: 20% (portfolio de proyectos similares a los solicitados 10%, antigüedad en mercado 5%, referencias de clientes 5%)
- Oferta técnica: 50% (propuesta 30%, creatividad e innovación 10%, conformación del equipo 5% aspectos deseados 5%)
- Oferta económica: 30%

9. Propiedad intelectual

Centro Ceibal será el único titular de los derechos de autor y propiedad intelectual de todo lo creado en el marco del presente llamado y contratación. El oferente deberá asegurar que las creaciones y obras realizadas serán originales y no infringirán derecho alguno de Propiedad Intelectual o Industrial de terceros, así como tampoco derechos de imagen y/o protección de datos personales de participantes. En este contexto la empresa contratada será la única responsable por acciones legales y/o reclamaciones de cualquier naturaleza que puedan originarse en relación con la originalidad y autoría de las obras, materiales, imágenes, etc, realizadas en el marco del presente llamado, y responderá de los daños y perjuicios, multas, penas, costas, costos, gastos causídicos, honorarios de abogado, gastos, y cualesquiera otras pérdidas que pudieren irrogarse al Centro Ceibal por tal motivo.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

10. Seguridad y privacidad

El oferente deberá informar junto con su oferta dónde estarán alojados los datos que procese en caso de resultar adjudicado, debiendo el servidor encontrarse en países considerados con niveles adecuados de acuerdo con la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, modificativas, 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.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

11. ANEXO I - Requisitos de seguridad de la información para la compra de sistemas informáticos

Este documento establece los requisitos a incluir al momento de realizar llamados para la compra de soluciones informáticas.

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.

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.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

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:

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

- 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.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

- 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

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

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

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

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

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

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

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

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

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

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:

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

- 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

Se deberá completar por parte de los oferentes la siguiente matriz de cumplimiento:

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

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	Deseado		
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		

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

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.

+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy