

Concurso público de precios
Horas de desarrollo y diseño para
portales de Comunicación

PLIEGO ESPECÍFICO

ÍNDICE

Índice	2
Objetivo	4
ITEM 1 - Mantenimiento Base	5
ITEM 2 - Horas de desarrollo y diseño web	5
Características del servicio	7
Especificaciones requeridas	7
Sitios involucrados	8
Hosting	8
Forma de trabajo	9
Oferta	10
Modalidad de cotización	10
Presentación de la oferta	12
Evaluación	14
Propiedad intelectual	15
Anexo	16
Presentación de antecedentes	16
Acuerdos de Calidad del Servicio	19
Calidad del Servicio	19
Acuerdos de nivel de Servicio	19
Parámetros de evaluación	19
hitos	21
Penalización	22
SLA - Nivel de servicio	23
Presentación de CVs	25
	2



Plan Ceibal

Requisitos de seguridad de la información para la compra de sistemas informáticos	26
Requerimientos proyecto portal Centro Ceibal	36

1 OBJETIVO

Centro Ceibal llama a Concurso público de precios para contratar horas de diseño (que incluya también diseño UI/UX centrado en el usuario) y desarrollo web, en modalidad remota o in situ, para realizar proyectos y mantenimiento de portales de comunicación de la institución.

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

Ítem 1 (Obligatorio)	Ítem 2 (Obligatorio)
40 horas mensuales "Mantenimiento base" a ser distribuidas entre mantenimiento correctivo y evolutivo (computado en horas mensuales, donde las horas no ejecutadas podrán ser acumuladas hasta el siguiente mes).	Hasta 2300 Horas de desarrollo y diseño web a ser ejecutadas en un plazo de hasta dos años, según las necesidades de Centro Ceibal, en modalidad bajo demanda.

Cada oferente deberá ofertar los ítems 1 y 2.

ITEM 1 - MANTENIMIENTO BASE

Las 40 horas mensuales de mantenimiento base. serán utilizadas fundamentalmente para diseño y mantenimiento correctivo (resolución de incidencias), y en caso de sobrantes serán utilizadas en proyectos y tareas de mantenimiento evolutivo y preventivo (mejoras y/o ajustes sobre los instancias previamente aprobadas), dentro del mes corriente y mes siguiente.

Se utilizará una herramienta de gestión provista por Ceibal para el seguimiento de incidentes, donde se realizará el control de horas de cada mes. El oferente deberá brindar un resumen mensual en base al SLA propuesto.

La oferta deberá incluir una descripción del nivel del servicio propuesto, según los diferentes niveles de criticidad. A modo de ejemplo, tiempo de respuesta a incidentes, resolución y recuperación ante fallos, considerando un horario de atención de Lunes a Viernes de 9:00 a 18:00 horas (días hábiles).

ITEM 2 - HORAS DE DESARROLLO Y DISEÑO WEB

Centro Ceibal proporcionará lineamientos de necesidades de comunicación, y lineamientos gráficos (key visual.), así como los contenidos (textos e imágenes). El proveedor deberá diseñar en base a lo propuesto por el Centro Ceibal (sujeto a posibles modificaciones durante el proceso). En otros casos puede suceder que Centro Ceibal proporcione el diseño de las páginas (en formato vectorial) para que el proveedor maquete el proyecto.

El diseño web propuesto, deberá cumplir con UI/UX contemplando al usuario como centro y con la revisión de un proceso de user research dentro de Ceibal.

Las horas de mantenimiento, tanto evolutivo como correctivo, serán administradas por el equipo del Centro Ceibal según un esquema de trabajo previamente acordado con el proveedor.

Para el mantenimiento evolutivo, el Centro Ceibal gestionará el proyecto, dividiendo los requerimientos en fases o sprints, con una metodología ágil a acordar con el proveedor. Para cada fase, se entregarán los requerimientos a la empresa adjudicada, quien deberá estimar el esfuerzo de desarrollo necesario. Para cada sprint, se requerirá la elaboración de entregables, como documentación relativa al proyecto. Una vez acordado con Centro 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.



Una vez informada la necesidad y los requerimientos de las tareas a realizar, el proyecto deberá comenzar como máximo en un plazo de 7 días calendario. Las horas consumidas no pueden superar la estimación aprobada para la fase, salvo razones fundadas con aprobación del Centro Ceibal. Los roles para la conformación del equipo será: Project Manager, Arquitecto de Software, Desarrollador, Tester y Diseñador Gráfico UX/UI.

Cualquier modificación en el equipo de trabajo deberá ser notificada previamente (mínimo una semana) por escrito al Centro Ceibal, y la integración de una nueva persona al equipo quedará sujeta a la aprobación del Centro Ceibal.

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

2 CARACTERÍSTICAS DEL SERVICIO

2.1 ESPECIFICACIONES REQUERIDAS

El oferente deberá contar y acreditar sólidos conocimientos de:

Especificaciones	
Excluyentes	No excluyentes
<ul style="list-style-type: none"> ● October cms ● Wordpress ● Php ● Bootstrap ● Google Analytics ● Javascript, ● Css, html, responsive design. ● Git 	<ul style="list-style-type: none"> ● Linux ● Percona mysql ● Sketch, Figma ● Mysql ● API REST ● Seo ● Google Tag Manager

2.2 SITIOS INVOLUCRADOS

La siguiente lista contempla las características generales de los sitios involucrados tanto en mantenimiento correctivo como evolutivo. La misma no es taxativa, pudiendo modificarse durante la vigencia del contrato.

Sitios que serán parte de la cartera de proyectos a ejecutar:

- Portal institucional de Ceibal (ceibal.edu.uy).
- Sitio Mi Espacio (miespacio.ceibal.edu.uy).
- Sitio Ceibal en Inglés (ingles.ceibal.edu.uy)
- Red Global de Aprendizajes (redglobal.edu.uy)
- Enlace 360 (enlace360.uy)
- Sitio "premio a la innovación pedagógica" (nombre a definir)
- Desafíos Profundos (desafioprofundo.org)
- Pensamiento Computacional (www.ceibal.edu.uy/pensamientocomputacional)
- Microbit (microbit.ceibal.edu.uy)
- Escuela de Verano
- Blog de formación (<http://formacion.ceibal.edu.uy/>)

Sitios externos de Plan Ceibal:

- Sitio Jóvenes a Programar
- Sitio Data Science
- Sitio ALTER
- Sitio Uruguay Estudia (<https://uruguayestudia.uy/>)

2.3 HOSTING

Todo sitio ya existente se encuentra hospedado por parte de Ceibal. Para aquellos proyectos a desarrollar durante el plazo del contrato, los cuales impliquen nuevos sitios y por ende nuevo hosting, Ceibal se encargará de proveer la arquitectura necesaria y realizar la operación del mismo.

2.4 FORMA DE TRABAJO

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

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

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

Los servicios podrán ser prestados en forma remota así como in situ en las oficinas de Centro Ceibal por su característica o urgencia, según Centro Ceibal considere conveniente.

La empresa oferente deberá contar con ambientes de desarrollo, mientras que Ceibal proporcionará ambientes de testing, preproducción y producción.

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

3 OFERTA

3.1 MODALIDAD DE COTIZACIÓN

El oferente deberá cotizar las horas de desarrollo de acuerdo al siguiente cuadro:

Cotizar en Pesos uruguayos imp. incl	
Item	Completar todas las celdas en blanco Costo (imp. incl)
Cotizar por el total de 40 horas mensuales¹ - Mantenimiento base	
Cotizar por hora² - Desarrollo y diseño web	
Cotizar por hora³ - Trabajos fuera de Horario de oficina	

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

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

¹ Cotización que contemple todos los roles: Project Manager, Arquitecto de Software, Desarrollador, Diseñador/UX/UI y Tester, tanto en modalidad remota como in situ. Horario de oficina: lunes a viernes (excepto feriados comunes y no laborables) de 9:00 a 18:00hs.

² Cotización que contemple todos los roles: Project Manager, Arquitecto de Software, Desarrollador, Diseñador/UX/UI y Tester, tanto en modalidad remota como in situ. Horario de oficina: lunes a viernes (excepto feriados comunes y no laborables) de 9:00 a 18:00hs.

³ Cotización que contemple todos los roles: Project Manager, Arquitecto de Software, Desarrollador, Diseñador/UX/UI y Tester, tanto en modalidad remota como in situ.



En caso de incluirse cláusula de ajuste, la misma tendrá vigencia a partir de la fecha de adjudicación y período de ajuste mayor o igual al semestra.

3.2 PRESENTACIÓN DE LA OFERTA

La oferta debe incluir en forma obligatoria los siguientes elementos:

- ✓ **Antecedentes** relativos a experiencias en proyectos en sistemas y tecnologías similares a las que son objeto del presente llamado:
 - a. Sección 2.1 - Especificaciones **obligatorias excluyentes**: se deberá contar con al menos un proyecto en cada tecnología en los últimos 3 años, pudiendo un mismo proyecto calificar a más de una tecnología . Además, como especificación excluyente, el oferente deberá tener al menos 20.000 horas (acumuladas) de dedicación en estas tecnologías (para el cálculo se consideran todas las tecnologías de desarrollo Web mencionadas menos las que involucran el manejo de Git como repositorio de código fuente). Además, se deberá contar con 3 proyectos gestionados bajo repositorio de código Git, en los últimos 3 años.
 - b. Sección 2.1 - Se valorará tener experiencia acreditada en proyectos en las tecnologías descrita 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.
 - d. Se valorará tener experiencia acreditada en proyectos que resuelvan necesidades de accesibilidad y usabilidad (UX).

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

El oferente se podrán asociar con otras firmas en forma de asociación en participación (Joint Venture) o subcontratistas conforme se menciona en el Pliego General con el fin de mejorar sus calificaciones de antecedentes.

- ✓ **Oferta técnica**: Los requerimientos están incluidos en el ANEXO. 6.5. Dentro de los entregables a incluir se encuentran:

- a. Propuesta del proyecto en una maqueta de navegación / demo que represente gráficamente la propuesta y una breve memoria descriptiva de lo que se propone
- b. Plan de trabajo (desglose de actividades), supuestos, equipo del proyecto, metodología a utilizar y cotización de horas.
- c. Diseño técnico, arquitectura o especificación de componentes de terceros a utilizar en el proyecto.

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 y la adecuación al público objetivo. El objetivo de este punto es evaluar la idoneidad técnica del proveedor y tener una primer propuesta base que permita resolver uno de los proyectos que podrá ser ejecutado bajo el "ITEM 2 - Horas de desarrollo y diseño web", una vez adjudicado.

- ✓ **Presentación del equipo de trabajo**, incluyendo currículos del personal que será responsable de prestar el servicio. Deberán incluir formación y experiencia relevante en desarrollo, con su respectiva dedicación horaria al objeto del llamado.
- ✓ **Oferta económica** (3.1 - Modalidad de cotización)
- ✓ **Propuesta de SLA para mantenimiento correctivo** (Ver Sección 6.2.3)
- ✓ **Tabla de Cumplimiento de Seguridad** de la Información: disponible en el ANEXO 6.4

3.3 EVALUACIÓN

El criterio de evaluación técnica de los oferentes será en base al cumplimiento de las especificaciones obligatorias para la prestación del servicio (sección 3.2), sumado a [la oferta técnica del proyecto previsto en el punto 5.5 del presente](#), un análisis de los curriculums de los técnicos presentados por las empresas oferentes, antecedentes, calidad e innovación de la propuesta y SLA presentado.

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

Evaluación		
	% Evaluación máximo	Detalle
Antecedentes	25	Portfolio de proyectos similares a los solicitados 25%
Oferta técnica	25	Propuesta, creatividad e innovación 25%
Cvs	15	Conformación del equipo 15%
SLA	5	Propuesta SLA 5%
Oferta económica	30	Propuesta económica 30%
TOTAL	100	

4 PROPIEDAD INTELECTUAL

Todos los trabajos realizados a raíz de la contratación de este servicio serán de propiedad exclusiva de Centro Ceibal, debiendo la empresa adjudicada transferir los códigos y la información que Ceibal requiera .

El oferente garantizará que no infringirá derechos de autor, de propiedad industrial e intelectual de terceros y que mantendrá indemne al Centro Ceibal ante cualquier reclamo derivado de violaciones de derechos de propiedad intelectual y/o derechos de autor.

5 ANEXO

5.1 PRESENTACIÓN DE ANTECEDENTES

Tecnología utilizada	N° de proyecto /s (1)	Nombre/s del proyecto (2)	Total horas por tecnología	Total de horas acumuladas (últimos 3 años) >= 20.000
Especificaciones excluyentes				
October CMS	1.. 2.. 3..			
Wordpress				
PHP				
Bootstrap				
Google Analytics				
Javascript,				
Css, html, responsive design.				
Git	Al menos			



	3			
Especificaciones no excluyentes				
Linux				
Percona mysql				
Google Tag Manager				
Sketch, Figma				
Mysql ,				
Seo				
API REST				
Proyectos vinculados a educación				
Proyectos que resuelvan necesidades de usabilidad/accesibilidad				

Ordenar del más reciente al más antiguo, por tecnología. Se valorarán sólo antecedentes de los últimos 3 años.

N° proyecto (1)	Nombre del proyecto (2)	Institución contratante	Contacto responsable de dicha institución, cargo, teléfono, mail	Descripción y alcance del proyecto	Período en el que fue realizado Duración en meses	Cantidad de integrantes del equipo de trabajo Nombres y roles de los responsables	Proyectos derivados (si los hubiera) tomado como insumo o realizado por el proyecto	Horas dedicadas en total	Lenguajes y Bases de datos (incluidas versiones usadas)	Hipervínculo a la carta de recomendación (si hubiera)

5.2 ACUERDOS DE CALIDAD DEL SERVICIO

5.2.1 CALIDAD DEL SERVICIO

En cada proyecto asignado, el proveedor será responsable de realizar todas las pruebas que considere pertinentes para garantizar el funcionamiento correcto del sitio 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 que hubieran podido detectarse durante el proceso de testing del proveedor adjudicado, deberá ejecutarse nuevamente el ciclo de pruebas diseñado sin costo extra así como solucionar el problema bajo su costo.

5.2.2 ACUERDOS DE NIVEL DE SERVICIO

Se establecerán previamente un conjunto de parámetros para medir la calidad mínima y aceptable de los servicios prestados durante la vigencia de la relación entre las partes que se mencionan continuación.

5.2.2.1 PARÁMETROS DE EVALUACIÓN

1. Cumplimiento del plazo: se busca determinar si la provisión del producto (bien o servicio) fue entregado por el proveedor en el plazo acordado. Para ello se considerará::

- a. Cumplimiento de plazos acordados. Para mantenimiento correctivo, el SLA presentado en la sección 6.2.3.
- b. Seguimiento de pendientes
- c. Notificación oportuna de posibles retrasos

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

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

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 incumplimientos sobre cualquiera de los parámetros descritos anteriormente (punto 6.2.2.1 anterior) que impacten de forma negativa sobre la continuidad del proyecto.

Se considera una No conformidad cuando se incumplan los plazos acordados con el Centro Ceibal de cualquiera de los hitos descritos en el punto 6.2.2.2, cuando se acumulen 5

Reclamos, o ante otros incumplimientos a los términos acordados y obligaciones asumidas, según la gravedad e impacto de dicho incumplimiento.

La sumatoria de 3 No conformidades, se considera incumplimiento grave, lo que podría habilitar la rescisión del contrato por incumplimiento, ejecución de la garantía de cumplimiento de contrato y aplicación de las penalidades correspondientes según punto 6.2.2.3

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 punto 6.2.2.3..

5.2.2.2

HITOS

- Inicio de Proyecto

Hito comprometido	Retraso Aceptable
Cronograma de trabajo con hitos identificados con responsables	Una semana desde la fecha acordada

- Análisis y Diseño

Hito comprometido	Retraso Aceptable
Documento de diseño para los requerimientos solicitados	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	Una semana desde la fecha acordada
Documentación de Liberación de proyecto con instructivo de instalación	Una semana desde la fecha acordada
Documentación técnica actualizada	Una semana desde la fecha acordada
Código Fuente	Una semana desde la fecha acordada
Transferencia de conocimiento a Ceibal realizada (en caso de ser requerida)	Una semana desde la fecha acordada
Pedido de ejecución de proyecto con BRIEF	Una semana desde la fecha acordada. Entrega total del sitio / proyecto solicitado.
Pedido ajustes concretos como actualización de links, contenidos (video, imagen, banner), corregir un error, etc de sitios / micrositos ya funcionando.	24hs desde la fecha acordada.

5.2.2.3

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.

5.2.3

SLA - NIVEL DE SERVICIO

TIEMPO DE RESPUESTA

Urgencia del incidente	SLA (Tiempo de Respuesta en horas)	Observaciones
Urgente		Son aquellos incidentes ⁴ presentados en producción sobre el aplicativo que detienen o afectan la operación, colocando en riesgo la operación de CEIBAL o el servicio brindado por CEIBAL a sus usuarios.
Alta		Son aquellos incidentes presentados en producción sobre el aplicativo que no detienen la operación, pero sí impiden que algunos recursos cumplan con su función básica.
Media /Baja		Son aquellos incidentes presentados en producción sobre el aplicativo que no impiden que cumpla con su función básica, pero sí les dificulta la operación.

TIEMPO DE RESOLUCIÓN

Las partes acordarán para cada incidente el tiempo de solución del mismo. Especificar indicadores de resolución de incidentes mensual según nivel de urgencia.

Ejemplo: Porcentaje de incidentes resueltos en el plazo comprometido, en el mes y según nivel de criticidad.

⁴

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



El oferente puede añadir información que le parezca relevante en su propuesta de SLA..

5.3 PRESENTACIÓN DE CVS

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

Cuadro Resumen

Roles: Project Manager, Arquitecto de Software, Desarrollador, Tester, diseñador UX/UI.

Rol	Nombre y Apellido	Dedicación (parcial o completa)

Cuadro por integrante

Cargo propuesto			
Perfil			
Educación			
Certificaciones/ Cursos relevantes			
Experiencia relevante para el llamado	Tecnología	Tiempo de experiencia: Proyectos URL (si corresponde)	
Historia Laboral	Desde	Hasta	Empresa/Rol/Principales actividades
Certificados (si corresponde)			

5.4 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 N° 18.331, de 11 de agosto de 2008 y Decreto N° 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. .
- Alojamiento de los datos en territorio uruguayo, o en caso de transferencia internacional asegurar que el servidor se encuentre en países considerados con niveles adecuados de acuerdo con la Directiva 95/46/CE. En caso contrario, contar con el consentimiento del titular del dato para la transferencia a un territorio no adecuado, o a que el importador haya suscripto cláusulas contractuales tipo con el exportador o posea un Código de Conducta inscripto, con la consecuente autorización de transferencia internacional de datos tramitada ante la Unidad Reguladora y de Control de Datos Personales, en los dos últimos supuestos.
- No utilizar la información / datos para una finalidad distinta a la contratada, ni en beneficio propio ya sea gratuito u oneroso, ni cederlos, comunicarlos o transferirlos a terceros.
- Centro Ceibal será el responsable de la base de datos y del tratamiento, siendo la Empresa adjudicada y sus empresas sub contratadas, encargados de tratamiento, de acuerdo con lo dispuesto en los literales H) y K) del artículo 4 de la Ley 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 Estandar Godaddy	Godaddy	256 bits
Certificado SSL Estandar 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.

- **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	Criptografía	Deseado		
12	Código malicioso	Deseado		
13	Lógica de negocio	Deseado		
14	Configuración	Deseado		
15	Certificaciones	Deseado		
16	Metodologías	Deseado		
17	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.

5.5 REQUERIMIENTOS PROYECTO PORTAL CENTRO CEIBAL

Sobre el proyecto:

El portal (ceibal.edu.uy) es un importante canal de acercamiento a la institución para toda la sociedad. Pretende ser un lugar de consulta 24/7 a las propuestas y contenidos para docentes, estudiantes, y un medio informativo para referentes, prensa y público general.

El **objetivo** del rediseño del portal es garantizar el correcto acceso y difusión del trabajo que las distintas áreas de Ceibal generan día a día, mejorar y personalizar la experiencia de usuario para incentivar el rol funcional del portal (contenido personalizado, acceso a plataformas, información actualizada, etc.)

Requerimientos:

Login único Ceibal

Integrar 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, que ya cuenta con contenido para los diferentes perfiles de acuerdo a las franjas de edad.
- Si el usuario es docente el sistema deberá desplegar el contenido personalizado para su perfil.

Administración de usuario

El portal deberá contar con con Login/logout al portal, cambio de contraseña, restablecimiento de contraseña, editar información personal.

Plataforma

El sitio está construido sobre [October CMS](#) y será un requisito trabajar sobre este gestor de contenidos.

Buscador

El buscador debe contemplar todos los contenidos del sitio: artículos, páginas, etiquetas, etc. Los resultados deberán estar jerarquizados y mostrar además contenido relacionado a la búsqueda.

Menú

Este es el [mapa del sitio](#) según el organigrama de la institución.

Contenido dinámico

Página principal

En la home del sitio van a convivir todo tipo de contenidos. Los sectores a definir serán:

Destacados principal

Sector de destacados donde pueden convivir contenidos de tipo noticias, videos, eventos, convocatorias, etc. Necesitamos que esta sección pueda mutar según las necesidades del momento permitiendo elegir entre al menos 3 variables de grilla ([ejemplo ilustrativo](#))

Acceso directo a las plataformas educativas

Sección convocatorias/eventos según calendario

Sector para destacar convocatorias que tenga posibilidad de ordenarse automáticamente por fecha y/o de manera manual.

Sección noticias

Sector donde se destacan las principales noticias por fecha y/o manualmente

Sección Videoteca

Sector para destacar contenido de tipo video con filtro por área de Ceibal o tipo de contenido

**Páginas de referencia por especificidad en el tipo de contenido y dinámicas institucionales: [FIC](#), [UdelaR](#), [FCEA](#), [UNTREF](#)*

Páginas

Es necesario contar con distintos templates según el tipo de contenido. Cada área de trabajo deberá contar con una página principal que nucleee toda la información relacionada a sus actividades (información general, convocatorias, noticias, etc). Siempre que sea necesario, deberá contar con acceso directo a las plataformas educativas.

Artículos

Es necesario contar con distintos tipos de contenido y varias posibilidades dentro de la carga. Todos estos artículos estarán cargados con el [plugin Blog de October](#)

Flujo de publicación

Los contenidos deben contar con un flujo de publicación con diferentes permisos según usuario (habilitados solo para creación y edición, y habilitados para edición y publicación)

Etiquetas

Todos los contenidos (noticias, videos, etc) deben contar con la opción de etiquetar temas para relacionarse entre sí. Estas etiquetas se deben poder crear desde el artículo, o permitir seleccionarlas si ya están creadas.

Noticias / artículos

Sectores requeridos:

1. Título
2. Copete/resumen
3. Texto destacado (para utilizar en sectores como el destacado de home)
4. Desarrollo de texto.
5. Imagen adjunta
6. Galeria de imagenes
7. Video asociado a este contenido (con posibilidad de adjuntar más de 1)
8. Documentos adjuntos (pdf, doc etc.)
9. Links
10. Fecha de publicación (posibilidad de tener una fecha de vencimiento y que deje de estar visible)
11. Etiquetas

Artículo con link exterior

Actualmente se necesita muchas veces tener un artículo que redirija a un sitio exterior y este destacado en la home. Para ello necesitamos cambiar a mano la plantilla principal del portal. Para solucionarlo, necesitamos un tipo de contenido que realice automáticamente los cambios en el código.

Sectores requeridos:

1. Título
2. Copete/resumen
3. Imagen
4. Link exterior (que se abra en una nueva pestaña)
5. Fecha de publicación (posibilidad de tener una fecha de vencimiento)
6. Etiquetas

Videos

Sectores requeridos:

1. Título
2. Copete/resumen
3. Imagen
4. Url del video
5. Desarrollo de texto
6. Fecha de publicación y vigencia (posibilidad de tener una fecha de vencimiento y que deje de estar visible)
7. Etiquetas
8. Identificar a qué área/s de trabajo de Ceibal pertenece ese contenido y linkearlo con contenidos similares

Calendario

Debe contar con filtros por tipo de actividad, área de trabajo, fecha, vigencia, todas.

Look and feel

Ceibal proveerá de materiales (logos, tipografía, paleta de colores institucional, etc) que el proveedor deberá aplicar con criterio.

MVP (fecha de entrega a convenir según calendario de trabajo)

- Registro con login/logout
- Home con destacado principal, sección de convocatorias actualizada según calendario (con posibilidad de destacar manualmente), sección videoteca
- Desarrollo de calendario dinámico, con perfiles de usuarios con distintos permisos
- Acceso directo a plataformas
- Acceso a información institucional y soporte técnico

Requerimientos no funcionales

- Framework de desarrollo: [October CMS](#)
 - Ceibal proveerá un template con determinados estilos y plugins por defecto.
- Sistema Operativo: Centos 7
- Se deberán migrar los artículos del sitio actual al nuevo sitio.
- 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.

Debe estar construida siguiendo los estándares Html5 y CSS3 del W3C según las pautas de Accesibilidad para el Contenido Web (WCAG), lo cual incluye WCAG 2.0 y WCAG 2.1. con un nivel de conformidad no menor al AA (considerando el sitio completo); deberá garantizar asimismo la separación del contenido de las páginas (código HTML5), del diseño de las mismas (CSS3).

Reunión informativa

Se realizará reunión informativa virtual el día 12 de marzo a las 10:00 hs. Los interesados manifestarán su interés escribiendo a la casilla compras@ceibal.edu.uy.



Plan Ceibal