Plan Ceibal

Pliego Técnico

SOLUCIÓN DE BACKUP Y RECUPERACIÓN

Gerencia de Telecomunicaciones

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

Plan Ceibal

Indice de contenido

1. OBJETO **3**

2. PRODUCTOS A COTIZAR **4**

3. ESPECIFICACIONES TÉCNICAS **4**

A - El software de la solución propuesta debe 4

B - El hardware de la solución debe: 6

C - Soporte y mantenimiento 8

D - Capacitación 9

E - Instalación y Puesta en funcionamiento básico 9

F - Opcional: conversión de datos históricos 9

4. PRESENTACIÓN DE OFERTAS **9**

4.1 Documentación técnica 10

4.2 Formato 10

4.3 Plazos de entrega y puesta en funcionamiento 11

5. Seguridad de la información **11**

5.1 Requisitos de seguridad obligatorios 11

Diseño y arquitectura 11

Autenticación 11

Gestión de sesiones 12

Control de acceso 12

Codificación y validación 12

Manejo de errores y verificación de logs 12

Confidencialidad y Protección de datos 13

Comunicaciones 14

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

Uso de archivos y recursos 14
API y Web services 15
Respaldos y contingencia 15
5.2 Requisitos de seguridad deseables 15
Criptografía 15
Código malicioso 15
Lógica de negocio 16
Configuración 16
Certificaciones 16
Metodología 17
Análisis de vulnerabilidades 17
6. GARANTÍA 17
6.1 Condiciones generales 17
7. CRITERIOS DE EVALUACIÓN 17
7.1 Técnica 17
ANEXO I - Tabla de Cumplimiento de Especificaciones 19
ANEXO II - Tabla de Cotizaciones 26

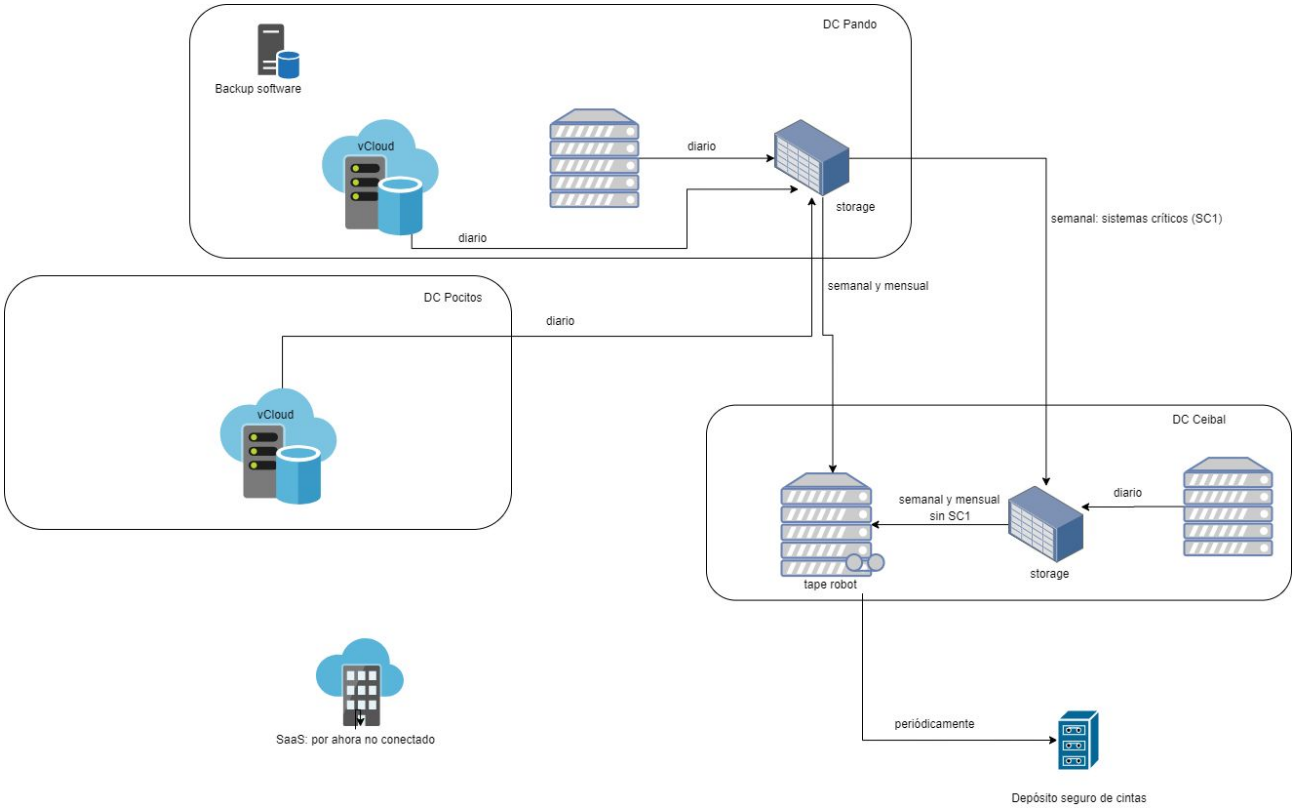
+598 2601 5773 | Av. Italia 6201, Edificio Los Ceibos, LATU, C. P. 11.500
www.ceibal.edu.uy

1. OBJETO

El objeto de este llamado es reemplazar la solución existente por una nueva solución de respaldo / continuidad de negocio / recuperación ante desastres.

Implementar un sistema que proporcione copias redundantes de protección / respaldo de datos locales y en la nube eficiente contra desastres y la pérdida de datos con distintos niveles de rapidez de acuerdo a la clasificación de la información proporcionada por Ceibal y que contemple todas las ubicaciones físicas de la información .

A continuación se encuentra el diagrama de la solución esperada:



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

2. PRODUCTOS A COTIZAR

Los productos comprendidos en este proceso son una solución para la realización de respaldos y recuperación que contemple:

A- Solución de backup y continuidad del negocio (software)
B - Hardware dedicado B.i Robot de cintas B.ii Disk Storage
C - Soporte y mantenimiento
D - Capacitación
E- Instalación y puesta en funcionamiento básico
F- Opcional: conversión de datos históricos

3. ESPECIFICACIONES TÉCNICAS

La solución a presentar se debe adaptar a la arquitectura mostrada en el diagrama del punto 1.

En todos los casos el producto ofertado deberá cumplir con **la totalidad de las especificaciones obligatorias**.

En caso de que el producto ofertado no cumpla con una o más especificaciones obligatorias la oferta de dicho producto será descartada.

A - El software de la solución propuesta debe

A.1	Permitir la protección / respaldo de entornos físicos y virtuales propios y en la nube.
A.2	Permitir la gestión centralizada basada en GUI que permita la configuración, ver el estado del sistema, la supervisión de copias de seguridad y la gestión de toda la actividad.
A.3	Admitir varios niveles de respaldo como, por ejemplo: completo, incremental, diferencial, sintético.
A.4	Administrar distintas plataformas de backup: debe tener la capacidad de

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

	realizar copias de seguridad en almacenamiento, como por ej. en disco, y robot de cinta (LTO) o virtual tape.
A.5	Proporcionar una restauración en 60 minutos para 1 TB o 7 VMs de aplicaciones y 2 TB y 2 VMs de bases de datos.
A.6	La solución debe permitir una copia de seguridad local de 2 TB (en 60 minutos o menos).
A.7	Admitir archivos / estructuras de datos / imágenes en Windows y Linux y múltiples aplicaciones en Windows y Linux, en una implementación física y / o virtual que admita hipervisores VMware.
A.8	Incluir el uso de tecnologías: ● Deduplicación ● Creación de instancias únicas ● Compresión de datos ● Función de cifrado
A.9	Proporcionar rendimiento, escalabilidad y extensibilidad.
A.10	Proporcionar una solución de respaldo / recuperación ante desastres que sea compatible o pueda integrarse con el entorno de red y TI existente de CEIBAL.
A.11	Contar con Interfaz amigable para administrar, monitorear y rastrear toda la actividad y ofrecer mecanismos de alerta.
A.12	Permitir personalizar las políticas de retención. La política actual de Ceibal es la siguiente: **Retención:** ● 6 meses (30 diarios y después de los 30 días guardar semanales) ● 1, 5 y 10 años (30 respaldos diarios; después del 1er mes sólo semanales hasta 3 meses, y después de los 3 meses guardar mensuales)
A.13	El sistema debe prever un crecimiento del 50% anual, es decir que por diseño debe estar preparado para soportar esa tasa de crecimiento.
A.14	Los sistemas operativos que maneja Ceibal y que deben ser soportados son Windows y Linux, versiones: Windows 2019, 2016, 2012R2, 2012. Linux- Centos 8, 7. Debian 8 y 9. Ubuntu 18, 16. RedHat 7.
A.15	La solución de copia de seguridad debe tener la capacidad de realizar copias de seguridad en nubes públicas y desde ellas.

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

A.16	El software debe ser 100% compatible con el hardware ofertado.
A.17	Indicar los requerimientos técnicos para el/los servidores que soporten la solución de software, ya sea virtual o físico.
A.18	La solución propuesta no debe tener el end-of-life ya programado, o debe ser superior a 5 años.
A.19	Bases de Datos que deben ser soportadas: Mysql Server 5.6, 5.7 y 8, SQL Server Standard 2014.
A.20	El sistema debe admitir un límite configurable en el ancho de banda de red que utiliza entre los sitios.
A.21	Funcionalidad de réplica de volúmenes dentro del mismo sistema de almacenamiento en distintos grupos de discos

B - El hardware de la solución debe:

B.1	Soportar sistema de monitoreo y gestión remota tipo IDRAC, iLO o equivalente.
B.2	Mostrar pruebas de implementaciones en empresas de similares dimensiones.
B.3	Soportar SNMP.
B.4	Ser rackeable.
B.5	Contar con fuentes redundantes (hot-swap).
B.6	Capacidad para respaldar servidores con la siguiente lista de plataformas:

HOSTS	Lugar	VMs	Sockets	Disco Usado (APROVISIONADO)	Datos adicionales
3	DC Ceibal	88	6	14TB	1 vcenter (3 hosts) ESXi-6.0.0, 6.7.0
8	DC Ceibal	93	13	5TB	8 servidores indiv. ESXi-6.0.0, 6.7.0

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

	<table><tr><td>22</td><td>DC Pando</td><td>145</td><td>44</td><td>76TB</td><td>1 vcenter con 3 DCs VMware ESXi, 6.5.0, 6.0.0, 6.7.0</td></tr><tr><td></td><td>Nube</td><td>153</td><td></td><td>30TB</td><td>vCloud Director</td></tr></table> ★ esto no incluye cantidades significativas de multimedia
B.7	Capacidad para realizar copias de seguridad de datos, con la siguiente configuración de política de retención para la copia de seguridad local: • Alta criticidad, requiere restauración rápida: 125 TB (es la suma de la tabla anterior, independientemente de cuánto ocupe en la solución de backup propuesta) - ver B.ii.9. • Copias de seguridad con retención 6 meses - 2 TB • Copias de seguridad con retención 1 año - 108 TB • Copias de seguridad con retención 5 años - 7 TB • Copias de seguridad con retención 10 años – 8 TB
B.8	El sistema propuesto debe ser escalable de acuerdo a la conveniencia para Ceibal y prever un crecimiento del 50% anual en 5 años, es decir que por diseño debe estar preparado para soportar esa tasa de crecimiento. Se deberá incluir el plan de crecimiento previsto (ej. cantidad de gabinetes/discos en el caso de storage).
B.9	La solución propuesta no debe tener el end-of-life ya programado, o debe ser superior a 5 años.

B.i Requerimientos específicos robot de cintas

B.i.1	Mínimo 32 slots
B.i.2	2 drives LTO8
B.i.3	Kit de montaje en rack de 19”

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

B.ii Requerimientos específicos disk storage

B.ii.1	Debe tener tolerancia a falla de 2 discos simultáneamente, sin contar compresión o deduplicación
B.ii.2	Discos Hot Swap
B.ii.3	Interfaz SAS o NL-SAS de al menos 12 Gbps
B.ii.4	- Respaldo de la memoria caché por baterías o similar a un medio no volátil
B.ii.5	- Soporte de actualización de microcódigo sin interrumpir el acceso de los servidores al sistema
B.ii.6	Administración del equipo vía web y consola
B.ii.7	- Redundancia en el camino de acceso a datos por cada controladora - Al menos 1 puerto de red Ethernet por controladora para administración (cobre RJ45). - Se deben incluir todos los elementos necesarios (transceiver, cables, etc) para el conexionado con el storage
B.ii.8	- Controladoras, fuentes de energía y ventiladores redundantes del tipo hot swap
B.ii.9	Debe poder almacenar en forma completa los 125 TB de la tabla especificada en B.6, pudiendo utilizar algoritmos de compresión para que finalmente ocupe menos espacio, siempre que cumpla con A.5 y A.6.

C - Soporte y mantenimiento

C.1	Describir plan de soporte y mantenimiento. Incluyendo SLA ante fallas con las siguientes opciones de horarios: ● de lunes a viernes de 9:00 a 17:00 ● de lunes a viernes de 8:00 a 22:00 ● de lunes a sábado de 8:00 a 22:00
C.2	Indicar características del servicio de actualización de versiones y tareas de

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

	mantenimiento preventivo durante el periodo de garantía.
C.3	Describir el tiempo de reemplazo de componentes críticos y redundados.

D - Capacitación

D.1	Proporcionar plan de transferencia de conocimiento para que el personal de Ingeniería de CEIBAL pueda operar la solución.

E - Instalación y Puesta en funcionamiento básico

E.1	El alcance de los servicios a cotizar comprende las etapas de instalación, configuración básica de la solución y la puesta en funcionamiento.

F - Opcional: conversión de datos históricos

F.1	Conversión de datos históricos que están en cintas LTO6 y LTO7.
F.2	Conversión de datos históricos que están en cintas LTO5 y LTO4.

4. PRESENTACIÓN DE OFERTAS

Cada oferente deberá cotizar la totalidad de los ítems A a E, solicitados en el presente documento.

El oferente deberá realizar un buen estudio, análisis y cálculo de los requisitos de almacenamiento local y en la nube, a fin de cumplir con nuestras políticas de retención y proporcionar una hoja de ruta técnica para la solución propuesta.

El oferente deberá indicar explícitamente qué Dispositivos / Software y funciones se proporcionan con la solución propuesta para administrar esa solución y cuáles funciones no solicitadas y que podrían ser de interés para Ceibal se ofrecen a un costo adicional, y declarar el fin de vida útil proyectado para la solución.

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

El oferente deberá indicar la lista de materiales junto con el precio del artículo por línea para todos los componentes propuestos, e indicar los costos por única vez y los recurrentes.

En el caso del software, indicar el modelo de licenciamiento y mantenimiento y soporte anual, considerando el escenario de 3 años.

El oferente deberá mostrar evidencia de implementaciones en empresas de similares dimensiones.

Indicar los costos de licencias de upgrade por TB o el esquema de licenciamiento propuesto.

Proporcionar una metodología de prueba detallada utilizada para garantizar que el sistema / proyecto esté funcionando según las especificaciones del fabricante con su respuesta.

Proporcionar un diagrama que describa la arquitectura propuesta (conectividad de red, configuración de respaldo / recuperación ante desastres, configuración de la política de retención local y en la nube etc.).

4.1 Documentación técnica

Junto con la oferta se deberá entregar toda la información necesaria para que Plan Ceibal comprenda en su totalidad los aspectos de la solución. Esta documentación deberá contar por lo menos con los siguientes ítems:

- Descripción de la solución y arquitectura.
- Listado y descripción de los componentes que integran la solución.
- Hojas de datos con las especificaciones técnicas del producto ofertado. Éstas deberán ser provistas por el fabricante del producto, permitiendo verificar el cumplimiento de los requerimientos propios del producto ofertado y coincidir con el mismo.
- Guía de instalación de todos los componentes de la solución.
- Guía de administración de toda la plataforma.
- Manuales de uso.
- Detallar los requisitos de hardware / software para que los servidores puedan ser respaldados por la solución.

Indicar cualquier característica adicional incluida en el sistema recomendado, así como cualquier característica que distinga la solución propuesta.

Centro Ceibal se reserva el derecho de descartar aquellas ofertas que no presenten alguno de los documentos indicados o que estos no se correspondan con el producto ofertado.

4.2 Formato

La oferta deberá ser presentada completando las tablas incluídas en los Anexos I y II.

El oferente completará todos los campos bajo el título A COMPLETAR POR EL OFERENTE de la Tabla de Cumplimiento de Especificaciones y de la Tabla de Cotizaciones.

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

En caso de que el oferente quiera ofrecer más de una opción para un mismo producto deberá agregar en las Tablas antes mencionadas las filas necesarias respetando el formato propuesto.

4.3 Plazos de entrega y puesta en funcionamiento

El oferente deberá especificar el plazo de entrega de los productos y a partir de la fecha de notificación de adjudicación. Es deseable un plazo no mayor a 60 días corridos a partir de dicha fecha. Se deberá indicar los plazos estimados de puesta en funcionamiento de la solución.

5. Seguridad de la información

Ceibal verificará que los productos ofertados cumplan con las políticas de seguridad institucionales, que se expresan en la siguiente lista de requisitos.

5.1 Requisitos de seguridad obligatorios

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. (largo mínimo 8 caracteres, letras y números, mayúsculas y minúsculas, bloqueo ante múltiples intentos fallidos)

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

- Compatibilidad con los sistemas de autenticación centralizados (SSO) usados por Centro Ceibal según corresponda: 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

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

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

Para lograr esto la solución deberá:

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

Confidencialidad y Protección de datos

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

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

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

- No utilizar la información / datos para una finalidad distinta a la contratada, ni en beneficio propio ya sea gratuito u oneroso, ni cederlos, comunicarlos o transferirlos a terceros.
- Centro Ceibal será el responsable de la base de datos y del tratamiento, siendo la Empresa adjudicada y sus empresas sub contratadas, encargados de tratamiento, de acuerdo con lo dispuesto en los literales H) y K) del artículo 4 de la Ley Nº 18.331.
- Permitir la publicación de las políticas de privacidad y términos y condiciones de uso de Centro Ceibal en el desarrollo.
- Permitir el derecho de acceso, rectificación, actualización, inclusión o supresión de los datos personales.
- Devolver o suprimir de todos sus sistemas y archivos físicos y lógicos, sean propios o contratados a terceros, los datos personales accedidos, obtenidos o tratados, así como los metadatos asociados, a requerimiento de Ceibal.

Comunicaciones

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

Para esto deberá:

- Publicar servicios a través de protocolos seguros (TLS o encriptación robusta) para todos los usuarios y sin importar la sensibilidad de la información transmitida.
- Se utilizarán protocolos y algoritmos considerados seguros por la industria y las buenas prácticas, dejando como último recurso o por temas de compatibilidad que sean expresamente autorizados por Centro Ceibal el uso de otros protocolos menos seguros.
- La solución deberá ser enteramente compatible con los certificados usados por Centro Ceibal (Certificados SSL comodín y estándar) y en caso de usar certificados generados internamente deberán ser validados por las autoridades de certificación que Centro Ceibal establezca.
- Todas las comunicaciones por fuera del protocolo HTTP, como por ej. accesos remotos, comunicación entre capas de la solución, middleware, bases de datos, fuentes externas de datos, monitoreo, herramientas de comunicación, etc. deberán ser comunicaciones seguras y en lo posible encriptadas.

Uso de archivos y recursos

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

Para esto debe cumplir con:

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

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

API y Web services

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

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

Respaldos y contingencia

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

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

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

5.2 Requisitos de seguridad deseables

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.

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

- 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

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

- 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.

6. GARANTÍA

6.1 Condiciones generales

El oferente garantiza que en caso de adjudicación los productos a suministrar serán nuevos, completos, sin uso y del modelo ofertado. Que estarán libres de defectos atribuibles al diseño, los materiales, la fabricación, las condiciones de almacenamiento (empaque, temperatura y humedad apropiados), traslado o cualquier acto u omisión del oferente o fabricante que pudiera manifestarse en ocasión del uso normal de los bienes en las condiciones imperantes en el país. **El oferente deberá especificar el plazo de garantía, el cual deberá ser como mínimo de 36 (treinta y seis) meses** a partir de la fecha en que los productos hayan sido recibidos por Centro Ceibal. La garantía deberá incluir todos los componentes de los productos ofertados. Se deberán especificar claramente otras condiciones y límites de la garantía. En caso de que el oferente no especifique plazo de garantía se asumirá que el mismo es de 36 (treinta y seis) meses.

7. CRITERIOS DE EVALUACIÓN

7.1 Técnica

La evaluación técnica de ofertas se realizará según las siguientes etapas:

1) Se verifica que la información presentada sea completa, coherente con el producto cotizado y que cumpla con el formato pedido.
2) Se verifica si el producto ofertado cumple con las Especificaciones Obligatorias.
3) Se verificará que el producto se adapte a las arquitecturas utilizadas por Plan Ceibal.
4) Se verificará que las funcionalidades del producto presenten un valor agregado al equipamiento y los sistemas existentes.

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

La no verificación de una o más condiciones mencionadas en las etapas 1 a 4 habilita a Centro Ceibal a no incluir la oferta en las siguientes etapas de evaluación.

Ceibal se reserva el derecho a solicitar una demostración del producto ofertado.

Luego de que la oferta sea evaluada y aprobada técnicamente pasará a la etapa de evaluación económica. La propuesta técnica se evaluará de forma integral, es decir se considerará la solución tomando en cuenta software (A) + hardware (B) + servicios (C,D,E).

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

ANEXO I - Tabla de Cumplimiento de Especificaciones

TABLA DE CUMPLIMIENTO DE ESPECIFICACIONES		A COMPLETAR POR EL OFERENTE
Producto: A – software		(en cada especificación marcar con una cruz (X) cuando corresponda)
Especificaciones Obligatorias		CUMPLE
# Esp.	**Descripción**	**SÍ**
A.1	El sistema propuesto debe permitir la protección / respaldo de entornos físicos y virtuales propios y en la nube.	
A.2	Permitir la gestión centralizada basada en GUI que permita la configuración, ver el estado del sistema, la supervisión de copias de seguridad y la gestión de toda la actividad.	
A.3	El software de respaldo debe admitir varios niveles de respaldo como, por ejemplo: completo, incremental, diferencial, sintético.	
A.4	El software de respaldo debe administrar distintas plataformas de backup: debe tener la capacidad de realizar copias de seguridad en almacenamiento, como por ej. en disco, y robot de cinta (LTO) o virtual tape.	
A.5	Proporcionar una restauración en 60 minutos para 1 TB o 7 VMs de aplicaciones y 2TB y 2 VMs de bases de datos.	
A.6	La solución debe permitir una copia de seguridad local de 2 TB (en 60 minutos o menos)	

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

A.7	Admitir archivos / estructuras de datos / imágenes en Windows y Linux y múltiples aplicaciones en Windows y Linux, en una implementación física y / o virtual que admita hipervisores VMware.	
A.8	Incluir el uso de tecnologías: ● Deduplicación ● Creación de instancias únicas ● Compresión de datos ● Función de cifrado	
A.9	Proporcionar rendimiento, escalabilidad y extensibilidad.	
A.10	Proporcionar una solución de respaldo / recuperación ante desastres que sea compatible o pueda integrarse con el entorno de red y TI existente de CEIBAL.	
A.11	Interfaz amigable para administrar, monitorear y rastrear toda la actividad y ofrecer mecanismos de alerta.	
A.12	Permitir personalizar las políticas de retención. La política actual de Ceibal es la siguiente: **Retención:** ● 6 meses (30 diarios y después de los 30 días guardar semanales) ● 1, 5 y 10 años (30 diarios; después semanales hasta 3 meses, y después de los 3 meses guardar mensuales)	
A.13	El sistema debe prever un crecimiento del 50% anual, es decir que por diseño debe estar preparado para soportar esa tasa de crecimiento.	
A.14	Los sistemas operativos que maneja Ceibal y que deben ser soportados son Windows y Linux, principalmente las siguientes versiones: Windows 2019, 2016, 2012R2, 2012. Linux- Centos 8, 7. Debian 8 y 9. Ubuntu 18, 16. RedHat 7.	
A.15	La solución de copia de seguridad debe tener la capacidad de realizar copias de seguridad en nubes	

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

	públicas y desde ellas.	
A.16	El software debe ser 100% compatible con el hardware ofertado.	
A.17	Indicar los requerimientos técnicos para el/los servidores que soporten la solución de software, ya sea virtual o físico.	
A.18	La solución propuesta no debe tener el end-of-life ya programado, o debe ser superior a 5 años..	
A.19	Bases de Datos que deben ser soportadas: Mysql Server 5.6, 5.7 y 8, SQL Server Standard 2014.	
A.20	El sistema debe admitir un límite configurable en el ancho de banda de red que utiliza entre los sitios.	
A.21	Funcionalidad de réplica de volúmenes dentro del mismo sistema de almacenamiento en distintos grupos de discos	
TABLA DE CUMPLIMIENTO DE ESPECIFICACIONES		**A COMPLETAR POR EL OFERENTE**
Producto: B – hardware		(en cada especificación marcar con una cruz (X) la opción que corresponda)
Especificaciones Obligatorias		CUMPLE
# Esp.	Descripción	SI
B.1	Soportar sistema de monitoreo y gestión remota tipo IDRAC, iLO o equivalente.	
B.2	Mostrar pruebas de implementaciones en empresas de similares dimensiones.	
B.3	Soportar SNMP.	

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

<table>
<tr><td>B.4</td><td>Ser rackeable.</td><td></td></tr>
<tr><td>B.5</td><td>Contar con fuentes redundantes (hot-swap).</td><td></td></tr>
<tr><td>B.6</td><td>Capacidad para respaldar servidores con la siguiente lista de plataformas:

<table>
<tr><th>HOSTS</th><th>Lugar</th><th>VMs</th><th>Sockets</th><th>Disco Usado (APROVISIONADO)</th><th>Datos adicionales</th></tr>
<tr><td>3</td><td>DC Ceibal</td><td>88</td><td>6</td><td>14TB</td><td>1 vcenter (3 hosts) ESXi-6.0.0, 6.7.0</td></tr>
<tr><td>8</td><td>DC Ceibal</td><td>93</td><td>13</td><td>5TB</td><td>8 servidores indiv. ESXi-6.0.0, 6.7.0</td></tr>
<tr><td>22</td><td>DC Pando</td><td>145</td><td>44</td><td>76TB</td><td>1 vcenter con 3 DCs VMware ESXi, 6.5.0, 6.0.0, 6.7.0</td></tr>
<tr><td></td><td>Nube</td><td>153</td><td></td><td>30TB</td><td>vCloud Director</td></tr>
</table>

★ esto no incluye cantidades significativas de multimedia</td><td></td></tr>
<tr><td>B.7</td><td>Capacidad para realizar copias de seguridad de datos, con la siguiente configuración de política de retención para la copia de seguridad local:
• Alta criticidad, requiere restauración rápida: 125 TB
• Copias de seguridad con retención 6 meses - 2 TB
• Copias de seguridad con retención 1 año - 108 TB
• Copias de seguridad con retención 5 años - 7 TB
• Copias de seguridad con retención 10 años – 8 TB</td><td></td></tr>
<tr><td>B.8</td><td>El sistema propuesto debe ser escalable de acuerdo a la conveniencia para Ceibal y prever un crecimiento del 50% anual en 5 años, es decir que por diseño debe estar preparado para soportar esa tasa de crecimiento. Se deberá incluir el plan de</td><td></td></tr>
</table>

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

	crecimiento previsto (ej. cantidad de gabinetes/discos en el caso de storage).	
B.9	La solución propuesta no debe tener el end-of-life ya programado, o debe ser superior a 5 años.	
	Robot de cintas	
B.i.1	Mínimo 32 slots	
B.i.2	2 drives LTO8	
B.i.3	Kit de montaje en rack de 19"	
	Disk Storage	
B.ii.1	Debe tener tolerancia a falla de 2 discos simultáneamente, sin contar compresión o deduplicación	
B.ii.2	Discos Hot Swap	
B.ii.3	Interfaz SAS o NL-SAS de al menos 12 Gbps	
B.ii.4	- Respaldo de la memoria caché por baterías o similar a un medio no volátil	
B.ii.5	- Soporte de actualización de microcódigo sin interrumpir el acceso de los servidores al sistema	
B.ii.6	Administración del equipo vía web y consola	
B.ii.7	- Redundancia en el camino de acceso a datos por cada controladora - Al menos 1 puerto de red Ethernet por controladora para administración (cobre RJ45).	

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

	- Se deben incluir todos los elementos necesarios (transceiver, cables, etc) para el conexionado con el storage	
B.ii.8	- Controladoras, fuentes de energía y ventiladores redundantes del tipo hot swap	
B.ii.9	Debe poder almacenar en forma completa los 125 TB de la tabla especificada en B.6, pudiendo utilizar algoritmos de compresión para que finalmente ocupe menos espacio, siempre que cumpla con A.5 y A.6..	
TABLA DE CUMPLIMIENTO DE ESPECIFICACIONES		**A COMPLETAR POR EL OFERENTE**
Producto: C – Soporte y mantenimiento		(en cada especificación marcar con una cruz (X) cuando corresponda)
# Esp.	Descripción	SI
C.1	Describir plan de soporte y mantenimiento. Incluyendo SLA ante fallas con las siguientes opciones de horarios: ● de lunes a viernes de 9:00 a 17:00 ● de lunes a viernes de 8:00 a 22:00 ● de lunes a sábado de 8:00 a 22:00	
C.2	Indicar características del servicio de actualización de versiones y tareas de mantenimiento preventivo durante el periodo de garantía.	
C.3	Describir el tiempo de reemplazo de componentes críticos y redundados.	
TABLA DE CUMPLIMIENTO DE ESPECIFICACIONES		**A COMPLETAR POR EL OFERENTE**
Producto: D – Capacitación		(en cada especificación marcar con una cruz (X) cuando corresponda)

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

# Esp.	Descripción	SI
D.1	Proporcionar plan de transferencia de conocimiento para que el personal de Ingeniería de CEIBAL pueda operar la solución.	
TABLA DE CUMPLIMIENTO DE ESPECIFICACIONES		**A COMPLETAR POR EL OFERENTE**
Producto: E – Instalación y puesta en funcionamiento básico		(en cada especificación marcar con una cruz (X) cuando corresponda)
# Esp.	Descripción	SI
E.1	El alcance de los servicios a cotizar comprende las etapas de instalación, configuración básica de la solución y la puesta en funcionamiento.	
TABLA DE CUMPLIMIENTO DE ESPECIFICACIONES		**A COMPLETAR POR EL OFERENTE**
Producto: F – Migración de datos históricos (Opcional)		(en cada especificación marcar con una cruz (X) cuando corresponda)
# Esp.	Descripción	SI
F.1	Conversión de datos históricos que están en cintas LTO6 y LTO7.	
F.2	Conversión de datos históricos que están en cintas LTO5 y LTO4.	

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

ANEXO II - Tabla de Cotizaciones

TABLA DE COTIZACIONES		A COMPLETAR POR EL OFERENTE								
		Producto Cotizado		Precio unitario	marcar con una cruz (X) la opción que corresponda					
Producto	Descripción	Marca	Modelo	Precio	CIF	Plaza	UYU	USD	s/IMP	Tiempo de entrega
A	Software									
B.i	Robot de Cintas									
B.ii	Disk Storage									
C	Soporte y mantenimiento									
D	Capacitación									
E	Instalación y puesta en funcionamiento básico									
F	Migración de datos históricos (opcional)									
G	Licenciamiento									

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