Concurso Público de precios

Adquisición de un Sistema de Gestión Humana

ANEXO A: PLIEGO ESPECÍFICO

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

ÍNDICE

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

www.ceibal.edu.uy

1. OBJETIVO

Este llamado tiene como objeto la adquisición e implantación de un Sistema integral de Gestión Humana (GH) en modalidad On premise (instalación en servidores de Ceibal) o SaaS (Software As A Service).

La solución estará orientada a colaborar en la optimización de los procesos y en la mejora de las capacidades institucionales en relación a la gestión humana, a través de la generación de reportes e indicadores, para el análisis de la información y la toma decisiones,

1.1 REQUERIMIENTOS

El software de Gestión Humana deberá cumplir con los siguientes requerimientos funcionales (módulos) y no funcionales. Esta lista no es taxativa, pudiendo modificarse durante la extensión del contrato.

Centro Ceibal se reserva el derecho de adjudicar total o parcialmente los módulos,

REQUERIMIENTOS FUNCIONALES OBLIGATORIOS

Módulos:

Gestión completa del legajo de la persona (de todo el staff, aprox. 550 empleados).

- Gestión de datos personales de cada funcionario (nombre, apellido, dirección, y detalles de dirección, departamento, género, discapacidad, grupo étnico racial, teléfono, celular, a quien contactar, Cred Civ, CI, estudios, carné de salud y datos de salud, restricciones alimentarias, certificados, constancias, contratos firmados, archivos adjuntos, cuentas bancarias, datos de afiliación al BPS, y deducciones al IRPF y a la CJPPU, entre otros).
- Autogestión de cada ficha personal (cada usuario final podrá modificar actualizar datos personales, archivos adj, y el usuario administrador gestionar todos los campos).
- Gestión por parte del supervisor de los legajos de sus funcionarios a cargo.

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

- El sistema debe permitir hacer una gestión de la información que respete la protección de datos personales. Adicionalmente, debe permitir que los resguardos digitales se hagan siguiendo la normativa vigente en la materia, de forma tal que los mismos ofrezcan respaldo legal ante posibles reclamos.
- Generación de Organigrama de forma automática y líneas jerárquicas, que se vincule con la ficha personal, de tal modo que las modificaciones que se realicen en cualquier línea de información impacten en todo el sistema. Este organigrama debe ser exportable en más de un formato, al menos PDF y Excel.
- Control Horario por RRHH con interfaz con el control de acceso y consultas para líneas Jerárquicas.
- Gestión de conceptos liquidables por horas o días (ej. viajes al interior o exterior) con un flujo de autorización jefe-empleado para pagos de compensaciones en 3 niveles.
- Flujos de autorización jefe-empleado de licencias (regulares, maternidad/paternidad, cuidados parentales, enfermedad, estudio, sin goce de sueldo) configurables en varios niveles. El sistema debe permitir gestionar los flujos de solicitud, las autorizaciones, la presentación de las constancias necesarias (certificaciones médicas y constancias de estudio), la contabilización de los días tomados y el saldo restante, así como la extracción de información para su posterior procesamiento (Excel).
- Registro de días no trabajados por ausencias de diferente naturaleza
- Gestión de cambio de aportación y deducciones BPS: Cambios en tipos de aportes. Cambios en declaraciones de IRPF entre otros, generando reportes de modificaciones exportables a Excel.
- Gestión de suministro de accesos, permisos a sistemas/herramientas de uso interno de la organización (ej. Mail corporativo, intranet, etc)
- Gestión de asignación de herramientas de trabajo (laptop, PC, etc)
- Trayectoria profesional e histórico de modificaciones (por empleado, cargos, conocimientos y desempeño).

Ver detalle en tabla 6.2

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

Reclutamiento y Selección

- Debe contar con un Portal de Reclutamiento y Selección de autogestión de usuario con interfaz responsive de modo que pueda ser utilizada tanto vía web como en dispositivos móviles.
- Flujo configurable de aprobación -de al menos cinco (5) niveles- del proceso de reclutamiento y selección integrado a la ficha del postulante seleccionado. El flujo de aprobaciones debiera contemplar el envío de notificaciones en cada paso de aprobación que se requiera.
  Una vez aprobado, se debe contar con una funcionalidad que facilite el armado del aviso y su publicación en el portal institucional, intranet y redes sociales (ej: Linkedin).
- Debe contar con un proceso de postulación guiado y de fácil uso bajo los requerimientos preestablecidos.
- El sistema web de postulaciones debe posibilitar a los postulantes la creación y autogestión de un usuario, que permita visualizar las posiciones abiertas, efectuar su postulación y dar seguimiento a las aplicaciones realizadas. El sistema debe posibilitar al usuario ingresar su CV en hojas pre-definidas que lo guíen en la tarea, cargar documentación, y realizar actualizaciones en el momento que lo considere oportuno.
- El sistema debe contar con la posibilidad que el administrador gestione tanto llamados internos como externos y su combinación.
- Contar con la posibilidad de campos de información (obligatoria) específica o particular de cada llamado que puedan utilizarse como filtro en el proceso de selección.
- El equipo de GH debe contar con informes/reportes de seguimiento que muestran el estado de avance de los procesos de selección.
- Los solicitantes deben contar con visibilidad al estatus de cada proceso en curso.
- Gestión de Selección de candidatos: el sistema debe contar con la posibilidad de realizar búsquedas en la base de datos generada con los postulantes, y en los documentos adjuntos, por diferentes características o habilidades requeridas para la posición.
- El sistema debe alimentar una única base de datos, independientemente del medio en el que se publicó el llamado. Debe ofrecer funcionalidades de filtrado de los postulantes a partir de los campos relevados, facilitando la conformación de una primera lista de candidatos, para luego descargar la información que será necesaria para su evaluación. Y permitir la descarga de archivos y postulantes masiva por llamado o por grupo de llamados.

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

- El sistema debe permitir cargar el informe psicotécnico realizado (alimentando su legajo personal) y, finalmente, dar la aprobación del candidato seleccionado.
- Motores de búsqueda dentro de la base general por palabras en archivos.
  Ver tabla 6.2

Ingreso y Baja de Personal

- Para efectuar el alta del candidato seleccionado, el sistema debe levantar la información ingresada durante el proceso de postulación. pudiendo corregirse los datos que sean necesarios.
- Si hubiera modificaciones en el salario aprobado en la solicitud para el ingreso, deberá disparar un flujo de aprobación similar al proceso de ingreso de solicitud de personal. Esa información se consolida dentro del sistema de GH para dar el alta del nuevo empleado y formular la ficha de ingreso. Esta ficha se arma con la información contenida en la aprobación recibida, la información que el postulante ingresó en el momento de la aplicación y otra que deberá aportar.
- Pasado el plazo predefinido desde el ingreso, el sistema debe emitir una notificación de confirmación sobre su continuidad. Aquí el sistema debe ofrecer un paso de aprobación por parte del superior (Jefe o Gerente).
  El sistema enviará un formulario a completar (de tipo evaluación) que lo recibirá ambos y deberá ser firmado digitalmente. El formulario de Evaluación cerrado será otro documento accesible desde el legajo personal.
- El sistema debe permitir procesar bajas por desvinculación (según las causales legales) o por vencimiento de contrato (para lo cual es necesario que envíe notificaciones a los interesados). En este sentido, en caso de desvinculación voluntaria, debe permitir presentar cartas de renuncia, y almacenarlas en su legajo enviando una notificación de este ingreso de información a Gestión Humana. Asimismo, deberá disparar un proceso para completar un formulario de egreso preestablecido. En caso de desvinculación por otras causales, se deberá desplegar campos preestablecidos como por ejemplo; causal, información detallada o notas (entre otras).

- El sistema debe contar con reportes de novedades con los cambios que se procesaron en las fichas de personal, ya sea por ingresos, bajas o modificaciones en cargos, sectores, remuneración, entre otras.
- El sistema deberá emitir resumen de datos necesarios (preestablecidos) de ingresos, bajas y modificaciones de funcionarios, disparando diversos mails con dicha información de acuerdo a las necesidades.

Evaluación de Desempeño

- Debe permitir realizar evaluación por competencias y por objetivos.
- Asignación de objetivos por cascada a grupos por jerarquía.
- Reporte, acceso y visualización individual de las evaluaciones (tanto del ciclo en curso como de los ciclos pasados).
- Reporte, acceso y visualización grupal para jefes y gerentes (tanto del ciclo en curso como de ciclos pasados).
- Roles diferenciados de evaluado, evaluador y administrador.
- Alertas/Notificaciones de status de evaluaciones a RRHH y Evaluadores.
- Integración con otros procesos claves en los que se modifica la información del personal (ingresos, desvinculaciones y legajo del personal).
- Calibración de evaluaciones por grupo.
- Feedback recurrente individual y grupal.
- Matrices de talentos.
- El sistema deberá permitir generar reportes de las diversas evaluaciones realizadas y sistematización de información vinculada a objetivos, resultados, plan de desarrollo, formación o capacitaciones necesarias, perfiles de evaluadores, etc.
- Planes de trabajo que contengan objetivos y las acciones previstas para lograrlos. Se valorará que este módulo se integre con el módulo de capacitación.
- El sistema deberá emitir alertas y notificaciones de seguimiento de los planes definidos en el proceso de evaluación de desempeño. Ver tabla 6.2

Generales a todo el sistema

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

- Seguridad: deberá cumplirse con lo solicitado en el Anexo 6.6.

- El sistema debe poder utilizarse en dispositivos móviles. El sistema se debe poder usar en estos dispositivos con una resolución y formato acorde al dispositivo que se está utilizando.
- Se deberá poder exportar información en formatos PDF y Excel como mínimo siendo todos los datos e información del sistema visualizados o convertibles a reportes exportables.
- En cada módulo del sistema se debe poder visualizar información contando con múltiples filtros de modo de poder segmentar la información que sea requerida.
- El producto debe contar con servicios que permitan la interoperabilidad con los sistemas corporativos y de explotación de datos de Centro Ceibal (se entiende por esto, interoperabilidad vía servicios web, intercambio de archivos, bases de datos, entre otros).

Requerimientos de Usabilidad:

- El sistema deberá utilizar escritura simple y breve, ya que los usuarios deben poder leer y saber interpretar rápidamente a dónde ir y qué hacer.
- El sistema deberá cumplir con "Nivel A" de accesibilidad web (https://www.w3.org/WAI/WCAG21/quickref/?currentsidebar=%23col_customize&levels=aa%2Caaa).
- El sistema deberá ser navegable e informar al usuario en todo momento sobre dónde se encuentra y en caso de errores, orientar al usuario a continuar con el uso del sistema.
- El producto deberá contar con una interfaz de usuario de fácil uso e intuitiva que evite errores o dificultades en la experiencia.
- El sistema deberá ser de fácil adaptación y apropiación por parte del usuario tanto en la gestión del sistema como en el uso final.
- El diseño y estética deberán ser sencillos de modo de facilitar la experiencia del usuario. Una acción concreta de un usuario no deberá exceder en promedio de 4 interacciones del usuario. Ver tabla 6.2.

Todos los requerimientos descritos como obligatorios deben preexistir en el producto propuesto. No serán evaluados aquellos productos que requieran desarrollar cualquiera de las funcionalidades requeridas como obligatorias.
El producto propuesto debe contar con un plan de evolución continua que asegure su sustentabilidad en el tiempo.

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

Requerimiento Deseable no excluyente

- Extracción de información deberá ser performante en tiempos de respuesta.
- Con la información contenida en el sistema, posibilita la creación de forma automática (o pseudo automática) de un contrato en base a un formato tipo preestablecido y contenido en el sistema. El que posteriormente será firmado digitalmente y cargado en su legajo digital.
- Configuración de distintos tipos de alertas según procesos y flujos de aprobaciones (gestionada por los administradores).

1.2 IMPLANTACIÓN DE LA SOLUCIÓN

El oferente deberá considerar todas las actividades relativas a la puesta en marcha de la solución propuesta, entre ellas la migración de la información existente en sistemas actuales y configuraciones requeridas para el cumplimiento de los requerimientos expuestos en el punto anterior.

La propuesta deberá incluir:

- Estrategia de implantación y Metodología de trabajo propuesta
- Actividades y Responsabilidades que correspondan para las partes
- Cronograma a alto nivel incluyendo los hitos principales
- Estrategia de capacitaciones a usuarios finales y transferencia de conocimientos a los administradores del sistema
- Estrategia de migración de datos del sistema anterior al sistema propuesto

Una vez adjudicado, deberá presentarse un *Plan de Trabajo* que incluya como mínimo:

- Plan de Comunicación de Proyecto
- Riesgos identificados con su plan de contingencia
- Plan de Calidad y Testing
- Cronograma detallado de proyecto que incluya detalle de entregables/hitos
- Plan de transferencia de conocimiento a administradores del sistema y de sustentabilidad a funcionales y técnicos
- Plan de Capacitación a usuarios finales

Documentación Requerida del producto:

Se deberá entregar documentación del proyecto de la implantación de la herramienta, que contenga como mínimo:

- Documentación técnica de la solución
- Documentación de Arquitectura de la solución
- Documentación de desarrollos adicionales que sean identificados en el proyecto
- Manuales de usuarios en español y actualizaciones regulares.

Debe considerarse en la propuesta que se deberá contar con un ambiente de pruebas y un ambiente productivo de forma permanente.

El ambiente de pruebas quedará disponible luego de la implantación definitiva de modo de contar con este para futuros cambios y pruebas.

1.3 SERVICIO DE SOPORTE Y MANTENIMIENTO DE LA SOLUCIÓN

La oferta debe detallar el alcance del servicio de soporte tanto correctivo como evolutivo de la solución propuesta.

El servicio de soporte correctivo se entiende por el soporte referido a la solución de errores o incidentes reportados en ambiente productivo.

Las evolución del producto se entenderá incluido en el costo del licenciamiento o del servicio de soporte y mantenimiento de la solución quedando a disposición de Centro Ceibal la posibilidad de actualizar la versión siempre que así lo considere oportuno.

1.4 MANTENIMIENTO EVOLUTIVO PERSONALIZADOS

El oferente deberá cotizar valor unitario hora de desarrollos específicos para Centro Ceibal.

Las horas de desarrollo serán demandadas en caso que Centro Ceibal requieran ajustes o personalizaciones con un tope anual de hasta 500 horas dentro del horario de oficina y hasta 200 horas fuera del horario de oficina.

Se utilizará una herramienta de gestión provista por Centro Ceibal para el seguimiento de incidentes, donde se realizará el control de horas. Las horas consumidas no pueden superar la estimación previamente aprobada en cada caso, salvo razones fundadas con aprobación del Centro Ceibal.

1.5 LICENCIAMIENTO

Para dimensionar el licenciamiento debe considerarse 80 usuarios supervisores (cómo mínimo), 550 usuarios finales (cómo máximo) y 10 usuarios administradores (cómo máximo).

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

2 CARACTERÍSTICAS DEL SERVICIO

2.1 FORMA DE TRABAJO

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.

Se entiende que todo producto/entregable deberá testearse de forma fiable, en base al criterio de aceptación acordado. Los errores encontrados, deberán solucionarse a costo asumido por el proveedor.

Se establecerá con el proveedor un período de garantía post implementación en producción.

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

3 OFERTA

3.1 MODALIDAD DE COTIZACIÓN

El oferente deberá cotizar obligatoriamente según el siguiente cuadro:

Cotización[1]	
	Completar todas las celdas en blanco
	Costo (imp. incl.)
Implantación de la solución (cotización obligatoria por módulo)	
Gestión completa del legajo de la persona -Ficha personal de todo el staff. (incluido altas, modificaciones y bajas de personal).	
Reclutamiento y selección	
Evaluación de desempeño	
Total Implantación :	
Servicio de Soporte y Mantenimiento (Costo Anual[2]) - (en caso de estar incluido en el licenciamiento se deberá aclarar)	1 año:
	3 años:
	5 años:
Licenciamiento Anual[3] - cotización unitaria	1 año:
	3 años:
	5 años:
Mant. Evolutivo Personalizado: Cotizar valor[4] hora de desarrollo (hasta 500 horas anuales). -	

[1] Se podrá cotizar en moneda local o extranjera, haciendo la aclaración pertinente en cada campo, impuestos incluidos.

[2] Se debe cotizar obligatoriamente considerando un lapso de 1 año y luego para 3 años y 5 años siempre el precio unitario sea un diferencial

[3] Se debe cotizar obligatoriamente considerando un lapso de 1 año y luego para 3 años y 5 años siempre el precio unitario sea un diferencial. Detallar en caso que se requiera más de un tipo de licenciamiento para contar con los perfiles requeridos según lo especificado en el llamado.

[4] El horario sería de oficina: lunes a viernes (excepto feriados no laborables) de 9:00 a 17:00hs, hora local Uruguay. Cotización que contemple todos los roles: Account Manager, Project Manager, Consultor Técnico Senior, Consultor Técnico Junior, Consultor Funcional y Tester, tanto en modalidad remota como in situ.

Cotizar valor fuera de hora [5] (hasta 200 horas anuales)	
Otros costos (si corresponde) - especificar	

Se adjudicará a un único producto y único proveedor para todos los módulos mencionados, reservándose Centro Ceibal el derecho de no adjudicar alguno de los módulos si así lo considera necesario.

3.2 PRESENTACIÓN DE LA OFERTA

La oferta debe incluir en forma obligatoria los siguientes elementos:

✓ **Antecedentes** relativos a experiencias en proyectos similares a las que son objeto del presente llamado:

a. **obligatorias excluyentes**: el oferente deberá tener al menos 3 implantaciones de soluciones similares en los últimos 4 años.

b. Se valorará tener experiencia acreditada en implantaciones en Uruguay de sistemas/soluciones de gestión humana específicamente.

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

El oferente se podrá 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.

(Deberá presentarse de acuerdo al Anexo 6.1)

✓ **Propuesta Técnica-Funcional,** Deberá presentar de forma obligatoria:

a. Tabla completada de requerimientos, de acuerdo al Anexo 6.2.

[5] Se considera horario fuera de oficina: lunes a viernes de 8 a 9 hs y de 17 a 22 hs y sábados de 8 a 17 hs, hora local Uruguay, excepto feriados no laborables,

b. Propuesta de trabajo (desglose por módulos) incluyendo, supuestos, equipo del proyecto, metodología de trabajo, responsabilidades, cronograma a alto nivel, estrategia de capacitación y de migración de datos.

c. Demo y acceso al producto: Como parte de la presentación de la oferta se coordinará una demo específica para Centro Ceibal en la que deberá presentar todas las funcionalidades obligatorias. Asimismo el oferente debe habilitar el acceso temporal al producto para realizar pruebas por parte de Centro Ceibal como parte de la evaluación técnica. Centro Ceibal podrá excluir de la evaluación (descalificar), aquellos productos que no cumplan con los requisitos de usabilidad básicos establecidos en el ítem de Requerimientos de usabilidad mencionados en el punto 1.1.

d. Se valorarán especialmente los productos ofertados en modalidad SaaS.

✓ **Tabla de cumplimiento de perfiles requeridos,** (Deberá presentarse de acuerdo al Anexo 6,5)

✓ **Oferta económica** (Deberá presentarse de acuerdo a la sección 3.1 - Modalidad de cotización)

✓ **Tabla de Cumplimiento de SLA** deberá presentarse de acuerdo Anexo 6.4

✓ **Tablas de Cumplimiento de requisitos de Seguridad** deberá presentarse de acuerdo al Anexo 6.6

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). 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
Antecedentes	15
Cvs	5
Propuesta técnica-Funcional	40
Oferta económica	40
TOTAL	100

4 PROPIEDAD INTELECTUAL

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

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

5 CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

La empresa debe informar en la propuesta el territorio donde aloja los datos, y los subcontratos a los que adhiera para el tratamiento de los mismos. En caso que los datos personales se alojen, aun temporalmente, fuera del territorio nacional, la Empresa se obliga a que el importador se encuentre en países considerados con niveles adecuados a los estándares europeos de protección de datos, de acuerdo con el Reglamento General de Protección de Datos 2016/679, del Parlamento Europeo y del Consejo, modificatorias, concordantes y complementarias. Caso contrario, la Empresa se compromete a contar con el consentimiento del titular del dato para la transferencia a un territorio no adecuado, o a que el importador haya suscrito cláusulas contractuales tipo con el exportador o posea un Código de Conducta inscripto, con la consecuente autorización de transferencia 18 internacional de datos tramitada ante la Unidad Reguladora y de Control de Datos Personales, en los dos últimos supuestos.

El oferente que resulte adjudicado se obliga en forma expresa a conservar en la más estricta confidencialidad toda la información que procese o utilice durante su relación con Centro Ceibal. La Empresa se obliga a tratar los datos a los que tuviere acceso en virtud de este contrato, de conformidad con la Ley Nº 18.331, de 11 de agosto de 2008 y Decreto Nº 414/2009, de 31 de agosto de 2009, únicamente para la prestación y en el marco del servicio contratado, no pudiendo utilizarlos para otra finalidad, ni en beneficio propio ya sea gratuito u oneroso, ni cederlos, comunicarlos o transferirlos a terceros, salvo previa autorización de Centro Ceibal.

Centro Ceibal es responsable de la base de datos y del tratamiento, siendo el oferente adjudicado encargado de tratamiento, de acuerdo con lo dispuesto en los literales H) y K) del artículo 4 de la Ley Nº 18.331. Por tanto, en ningún caso el acceso a datos podrá entenderse como cesión o permiso para su libre utilización por parte de quien resulte adjudicado.

El oferente adjudicado se obliga a adoptar las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de los datos y evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información.

Al término del contrato el oferente deberá suprimir de todos sus sistemas y archivos físicos y lógicos, sean propios o contratados a terceros, los datos personales accedidos, obtenidos o tratados en virtud de la contratación con Ceibal, así como los metadatos asociados, en caso de corresponder.

Se considera dato personal la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, a modo enunciativo, cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que refiera a ellas directa o indirectamente, conforme con lo dispuesto en el artículo 4 de la Ley Nº 18.331 y artículos 1 y 4 del Decreto Nº 414/009.

6 ANEXO

6.1 PRESENTACIÓN DE ANTECEDENTES

Ordenar del más reciente al más antiguo. Se valorarán sólo antecedentes de los últimos 4 años.

Tabla

Nº proyecto	Nombre del proyecto	Institución contratante	Contacto responsable de dicha institución /proyecto, cargo, télefono, mail	Descripción y alcance del proyecto Cantidad de empleados	Período en el que fue realizado Duración en meses Equipo de trabajo	Horas dedicadas en total	Producto implantado	Hipervínculo a la carta de recomendación (si hubiere)

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

6.2 TABLA DE CUMPLIMIENTO DE REQUERIMIENTOS

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Obligatorios				
Ficha personal				
Gestión de datos personales de cada funcionario (nombre, apellido, dirección, y detalles de dirección, departamento, género, discapacidad, grupo étnico racial, teléfono, celular, a quien contactar, Cred Civ, CI, estudios, carné de salud y datos de salud, restricciones alimentarias , certificados, constancias, contratos firmados, archivos adjuntos, cuentas bancarias, datos de afiliación al BPS, y deducciones al IRPF y a la CJPPU, entre otros).				
Autogestión de cada ficha personal (cada usuario final podrá modificar actualizar datos personales, archivos adj, y el usuario administrador gestionar todos los campos).				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Gestión por parte del supervisor de los legajos de sus funcionarios a cargo.				
El sistema debe permitir hacer una gestión de la información que respete la protección de datos personales. Adicionalmente, debe permitir que los resguardos digitales se hagan siguiendo la normativa vigente en la materia, de forma tal que los mismos ofrezcan respaldo legal ante posibles reclamos.				
Generación de Organigrama de forma automática y líneas jerárquicas, que se vincule con la ficha personal, de tal modo que las modificaciones que se realicen en cualquier línea de información impacten en todo el sistema. Este organigrama debe ser exportable en más de un formato, al menos PDF y Excel.				
Control Horario por RRHH con interfaz con el control de acceso y consultas para líneas Jerárquicas.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Gestión de conceptos liquidables por horas o días (ej. viajes al interior o exterior) con un flujo de autorización jefe-empleado para pagos de compensaciones en 3 niveles.				
Flujos de autorización jefe-empleado de licencias (regulares, maternidad/paternidad, cuidados parentales, enfermedad, estudio, sin goce de sueldo) configurables en varios niveles. El sistema debe permitir gestionar los flujos de solicitud, las autorizaciones, la presentación de las constancias necesarias (certificaciones médicas y constancias de estudio), la contabilización de los días tomados y el saldo restante, así como la extracción de información para su posterior procesamiento (Excel).				
Registro de días no trabajados por ausencias de diferente naturaleza.				
Gestión de cambio de aportación y deducciones BPS: Cambios en tipos de aportes. Cambios en declaraciones de IRPF entre otros, generando reportes de modificaciones exportables a Excel.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Gestión de suministro de accesos, permisos a sistemas/herramientas de uso interno de la organización (ej. Mail corporativo, intranet, etc).				
Gestión de asignación de herramientas de trabajo (laptop, PC, etc).				
Trayectoria profesional e histórico de modificaciones (por empleado, cargos, conocimientos y desempeño).				
Reclutamiento y Selección				
Debe contar con un Portal de Reclutamiento y Selección de autogestión de usuario con interfaz responsive de modo que pueda ser utilizada tanto vía web como en dispositivos móviles.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Flujo configurable de aprobación -de al menos cinco (5) niveles- del proceso de reclutamiento y selección integrado a la ficha del postulante seleccionado. El flujo de aprobaciones debiera contemplar el envío de notificaciones en cada paso de aprobación que se requiera. Una vez aprobado, se debe contar con una funcionalidad que facilite el armado del aviso y su publicación en el portal institucional, intranet y redes sociales (ej: Linkedin).				
Debe contar con un proceso de postulación guiado y de fácil uso bajo los requerimientos preestablecidos.				
El sistema web de postulaciones debe posibilitar a los postulantes la creación y autogestión de un usuario, que permita visualizar las posiciones abiertas, efectuar su postulación y dar seguimiento a las aplicaciones realizadas. El sistema debe posibilitar al usuario ingresar su CV en hojas pre-definidas que lo guíen en la tarea, cargar documentación, y realizar actualizaciones en el momento que lo considere oportuno.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
El sistema debe contar con la posibilidad que el administrador gestione tanto llamados internos como externos y su combinación.				
Contar con la posibilidad de campos de información (obligatoria) específica o particular de cada llamado que puedan utilizarse como filtro en el proceso de selección.				
El equipo de GH debe contar con informes/reportes de seguimiento que muestran el estado de avance de los procesos de selección.				
Los solicitantes deben contar con visibilidad al estatus de cada proceso en curso.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Gestión de Selección de candidatos: el sistema debe contar con la posibilidad de realizar búsquedas en la base de datos generada con los postulantes, y en los documentos adjuntos, por diferentes características o habilidades requeridas para la posición.				
El sistema debe alimentar una única base de datos, independientemente del medio en el que se publicó el llamado. Debe ofrecer funcionalidades de filtrado de los postulantes a partir de los campos relevados, facilitando la conformación de una primera lista de candidatos, para luego descargar la información que será necesaria para su evaluación. Y permitir la descarga de archivos y postulantes masiva por llamado o por grupo de llamados.				
El sistema debe permitir cargar el informe psicotécnico realizado (alimentando su legajo personal) y, finalmente, dar la aprobación del candidato seleccionado.				
Motores de búsqueda dentro de la base general por palabras en archivos.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Ingreso y baja de personal				
Para efectuar el alta del candidato seleccionado, el sistema debe levantar la información ingresada durante el proceso de postulación. pudiendo corregirse los datos que sean necesarios.				
Si hubiera modificaciones en el salario aprobado en la solicitud para el ingreso, deberá disparar un flujo de aprobación similar al proceso de ingreso de solicitud de personal. Esa información se consolida dentro del sistema de GH para dar el alta del nuevo empleado y formular la ficha de ingreso. Esta ficha se arma con la información contenida en la aprobación recibida, la información que el postulante ingresó en el momento de la aplicación y otra que deberá aportar.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Pasado el plazo predefinido desde el ingreso, el sistema debe emitir una notificación de confirmación sobre su continuidad. Aquí el sistema debe ofrecer un paso de aprobación por parte del superior (Jefe o Gerente).				
El sistema enviará un formulario a completar (de tipo evaluación) que lo recibirá ambos y deberá ser firmado digitalmente. El formulario de Evaluación cerrado será otro documento accesible desde el legajo personal.				
El sistema debe permitir procesar bajas por desvinculación (según las causales legales) o por vencimiento de contrato (para lo cual es necesario que envíe notificaciones a los interesados). En este sentido, en caso de desvinculación voluntaria, debe permitir presentar cartas de renuncia, y almacenarlas en su legajo enviando una notificación de este ingreso de información a Gestión Humana.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Asimismo deberá disparar un proceso para completar un formulario de egreso preestablecido. En caso de desvinculación por otras causales, se deberá desplegar campos preestablecidos como por ejemplo; causal, información detallada o notas (entre otras).				
El sistema debe contar con reportes de novedades con los cambios que se procesaron en las fichas de personal, ya sea por ingresos, bajas o modificaciones en cargos, sectores, remuneración, entre otras.				
El sistema deberá emitir resumen de datos necesarios (preestablecidos) de ingresos, bajas y modificaciones de funcionarios, disparando diversos mails con dicha información de acuerdo a las necesidades.				
Evaluación de desempeño				
Debe permitir realizar evaluación por competencias y por objetivos.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Asignación de objetivos por cascada a grupos por jerarquía.				
Reporte, acceso y visualización individual de las evaluaciones (tanto del ciclo en curso como de los ciclos pasados).				
Reporte, acceso y visualización grupal para jefes y gerentes (tanto del ciclo en curso como de ciclos pasados).				
Roles diferenciados de evaluado, evaluador y administrador.				
Alertas/Notificaciones de status de evaluaciones a RRHH y Evaluadores.				
Integración con otros procesos claves en los que se modifica la información del personal (ingresos, desvinculaciones y legajo del personal).				
Calibración de evaluaciones por grupo.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Feedback recurrente individual y grupal				
Matrices de talentos.				
El sistema deberá permitir generar reportes de las diversas evaluaciones realizadas y sistematización de información vinculada a objetivos, resultados, plan de desarrollo, formación o capacitaciones necesarias, perfiles de evaluadores, etc.				
Planes de trabajo que contengan objetivos y las acciones previstas para lograrlos. Se valorará que este módulo se integre con el módulo de capacitación.				
El sistema deberá emitir alertas y notificaciones de seguimiento de los planes definidos en el proceso de evaluación de desempeño.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Generalidades				
Seguridad: deberá cumplirse con lo solicitado en el Anexo 6.6.				
El sistema debe poder utilizarse en dispositivos móviles. El sistema se debe poder usar en estos dispositivos con una resolución y formato acorde al dispositivo que se está utilizando.				
Se deberá poder exportar información en formatos PDF y Excel como mínimo siendo todos los datos e información del sistema visualizados o convertibles a reportes exportables.				
En cada módulo del sistema se debe poder visualizar información contando con múltiples filtros de modo de poder segmentar la información que sea requerida.				

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
El producto debe contar con servicios que permitan la interoperabilidad con los sistemas corporativos y de explotación de datos de Centro Ceibal (se entiende por esto, interoperabilidad vía servicios web, intercambio de archivos, bases de datos, entre otros).				
Usabilidad				
El sistema deberá utilizar escritura simple y breve, ya que los usuarios deben poder leer y saber interpretar rápidamente a dónde ir y qué hacer.				
El sistema deberá cumplir con "Nivel A" de accesibilidad web				
El sistema deberá ser navegable e informar al usuario en todo momento sobre dónde se encuentra y en caso de errores, orientar al usuario a continuar con el uso del sistema.				

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

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
El producto deberá contar con una interfaz de usuario de fácil uso e intuitiva que evite errores o dificultades en la experiencia.				
El sistema deberá ser de fácil adaptación y apropiación por parte del usuario tanto en la gestión del sistema como en el uso final.				
El diseño y estética deberán ser sencillos de modo de facilitar la experiencia del usuario. Una acción concreta de un usuario no deberá exceder en promedio de 4 interacciones del usuario.				
Deseables				
Extracción de información deberá ser performante en tiempos de respuesta.				

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

REQUERIMIENTOS	Incluido en la propuesta		REF. EN LA OFERTA	OBSERVACIONES
	SI	NO		
Con la información contenida en el sistema, posibilita la creación de forma automática (o pseudo automática) de un contrato en base a un formato tipo preestablecido y contenido en el sistema. El que posteriormente será firmado digitalmente y cargado en su legajo digital.				
Configuración de distintos tipos de alertas según procesos y flujos de aprobaciones (gestionada por los administradores).				

6.3 ACUERDOS DE CALIDAD DEL SERVICIO

6.3.1 Calidad del Servicio

El oferente será responsable de realizar todas las actividades que considere pertinentes para garantizar el funcionamiento correcto de la solución aplicativa propuesta, tanto en requerimientos funcionales como no funcionales definidos.

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 que hubieran podido ser detectados durante el proceso de testing del proveedor, deberá ejecutarse nuevamente el ciclo de pruebas diseñado sin costo extra..

6.3.2 Acuerdos de nivel de Servicio

Se establecerán 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 a continuación.

6.3.2.1 Parámetros de evaluación

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

- Cumplimiento de plazos acordados: Refiere a la ejecución de las distintas fases dentro de los plazos establecidos, así como las fechas acordadas en instancias de estimación e intercambio entre Ceibal y el proveedor.
- Seguimiento de pendientes: Se espera un intercambio fluído/acorde en base a los incidentes reportados y/o solicitudes de otra índole, así como la apropiación en la gestión de los mismos alineándose en base a las prioridades con Ceibal.
- Notificación oportuna de posibles retrasos: En consideración con las necesidades del negocio, los eventuales retrasos que se vayan previendo deberán ser notificados de forma inmediata, que permita a Ceibal gestionar el riesgo e impacto.

2. Calidad del servicio recibido: se busca medir si el 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:

- Calidad de la solución: Se espera que las soluciones brindadas no presenten errores que afecten los objetivos y transacciones de los distintos procesos de negocio. En el caso de existir errores bloqueantes en cualquier ambiente (priorizando aquellos que se presenten en ambiente productivo), se espera una gestión eficiente de los mismos.
- Trabaja según los procedimientos acordados con Ceibal: Alineado a las pautas de desarrollo y seguridad provistas por Ceibal.
- Calidad de la documentación provista: Ceibal proporcionará templates de documentación técnica, funcional, análisis y diseño, etc. Se espera que la documentación sea autocontenida y exhaustiva.
- Idoneidad del personal clave: Se espera que los miembros del equipo de trabajo cuenten con el expertise esperado, así como buena predisposición a la hora de emprender su labor.
- Seguridad, mantenibilidad, performance y usabilidad de la solución: se recomienda utilizar normas y estándares de seguridad OWASP. La solución deberá , de acuerdo a las reglas del negocio, ser performante y mantenible. Se espera además que se cumplan los estándares de usabilidad acordados en cada caso

3. Otros aspectos: se busca medir el grado de respuesta del proveedor en pro de satisfacer necesidades vinculadas con el servicio adquirido post producción. 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:

- Capacidad de trabajo: Se espera la comunicación temprana de aceptación / rechazo de trabajos de nuevas soluciones incluyendo en caso que corresponda, la justificación de dicho rechazo.
- Cumplimiento de garantías: Se evaluará el cumplimiento de garantías por parte de proveedor, en base a las líneas establecidas en el presente documento
- Coherencia de facturación: En base a las horas aprobadas y registradas en la herramienta provista por Ceibal.

El incumplimiento de los acuerdos del nivel de servicio o plazos comprometidos sobre cualquiera de los parámetros para cada fase o hito acordado con el Centro Ceibal, 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 que impacten de forma negativa sobre la continuidad del proyecto. En el caso de los errores bloqueantes en cualquier etapa, hito, sprint, ambiente: la tolerancia es cero.

Se considera una No conformidad cuando se incumplen los parámetros con mayor gravedad e impacto, cuando se acumulen 5 Reclamos, o ante otros incumplimientos a los términos acordados y obligaciones asumidas.

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.

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.

6.3.2.2 Penalización

El ingreso de una No conformidad podrá determinar la aplicación de una penalidad equivalente al 10% del precio acordado para esa fase, sprint o hito, 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.

6.4 SLA - NIVEL DE SERVICIO

TIEMPO DE RESPUESTA

En la columna de la siguiente tabla "Cumple con lo requerido" es donde el oferente deberá expresamente indicar "SI" o "No" con lo solicitado. En caso de que no se indique explícitamente el cumplimiento por parte del oferente, la oferta será rechazada.

Incidentes en Producción

Urgencia del incidente	SLA (en horas)	Observaciones	¿Cumple? [SI/NO]
Urgente	0,5 hs	Son aquellos incidentes[6] presentados en producción sobre la solución aplicativa que detienen o afectan la operación, colocando en riesgo la operativa de CEIBAL o el servicio brindado por CEIBAL a sus usuarios/beneficiarios	
Alta	2 hs	Son aquellos incidentes presentados en producción sobre la solución aplicativa que no detienen la operación, pero sí impiden que algunos recursos cumplan con su función básica.	
Media /Baja	4 hs	Son aquellos incidentes presentados en producción sobre la solución aplicativa que no impiden que cumpla con su función básica, pero sí les dificulta la operación.	

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

Atención a pedido de servicio

Prioridad De la Solicitud	SLA (días hábiles)	Observaciones	¿Cumple? [SI/NO]
Alta	2 días	Son aquellas solicitudes que por su naturaleza requieren una atención priorizada.	
Media	5 días	Son aquellas solicitudes que por su naturaleza pueden ser atendidas a mediano plazo	
Baja	8 días	Son aquellas solicitudes que por su naturaleza no forman parte del camino crítico por lo que pueden ser atendidas a largo plazo	

TIEMPO DE RESOLUCIÓN

Las partes acordarán para cada incidente/solicitud el tiempo de solución del mismo.

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

El oferente deberá enviar mensualmente el informe con los indicadores definidos del SLA, de acuerdo al formato que otorgue Ceibal.

6.5 PERFILES REQUERIDOS

Con el fin de aprobar la evaluación técnica, deberá afirmar que cumple con los requisitos mínimos de formación y la experiencia requerida para cada perfil. Para poder calificar como proveedor del Ítem deberá cumplir con todos los perfiles solicitados para el proyecto de implementación y posterior Soporte y Mantenimiento.

En la última columna de la siguiente tabla "Cumplo con lo requerido" es donde el oferente deberá indicar "SI" o "No" con lo solicitado. En caso de que no se indique explícitamente el cumplimiento por parte del oferente, la oferta será rechazada.

En la columna "Integrantes del equipo" deberá ingresar los nombres de quiénes brindarán el servicio al Centro Ceibal.

<table>
<tr><td colspan="5">Account Manager
Cantidad sugerida: 1</td></tr>
<tr><td>Descripción</td><td colspan="4">Responsable del relacionamiento Ceibal-Oferente
Indicadores y seguimiento generales de servicio y forma de trabajo
Propuestas de mejora de servicio y metodología de trabajo
Oportunidades de nuevos servicios/negocio</td></tr>
<tr><td colspan="3">Requisitos</td><td>¿Cumple? (SI/NO)</td><td>Integrantes del equipo</td></tr>
<tr><td>Formación</td><td>Sugerido</td><td>Podrá contar con al menos uno de los siguientes requisitos
• Egresado de cualquier carrera universitaria.
• Carrera técnica en sistemas de 4 años o más finalizada</td><td></td><td rowspan="2"></td></tr>
<tr><td>Experiencia</td><td>Excluyente</td><td>Experiencia en servicios vinculados a TICs y tecnologías Microsoft</td><td></td></tr>
</table>

Project Manager **Cantidad sugerida: 1**			
Descripción	• Responsable del proyecto • Planifica, monitorea, coordina y controla las actividades • Coordina la estrategia con el resto del equipo. • Escribe y revisa la estrategia definida • Estima el esfuerzo y costo de las actividades • Introduce métricas viables para medir el progreso de las actividades • Evalúa la calidad del trabajo realizado. • Gestiona los riesgos • Escribe los reportes basados en la información obtenida de las actividades. • Realiza las recomendaciones de mejora. • Verifica que se haya realizado la documentación necesaria y acordada. • Vela por la correctitud del servicio entregado y su sustentabilidad en el tiempo.		
Requisitos		¿Cumple? (SI/NO)	Integrantes del equipo

Formación	Excluyente	Deberá contar con al menos uno de los siguientes requisitos • Egresado de cualquier carrera universitaria. • Carrera técnica en sistemas de 4 años o más finalizada		
	Sugerido	Capacitación o certificado PMP, Ágil (o similar)		
Experiencia	Excluyente	Experiencia en al menos 3 proyectos en implementación del producto propuesto en los que ha participado en calidad de PM en los últimos 4 años al momento de la apertura de las ofertas.		

Consultor Funcional Cantidad sugerida: 1/n	
Descripción	• Analiza y evalúa las necesidades y requerimientos planteados, según contexto de la organización. • Propone, diseña e implementa soluciones. • Coordina y asiste al equipo técnico.

	• Documenta los requerimientos de desarrollo alineados a las necesidades planteadas por la organización. • Asesora y vigila el cumplimiento de las políticas y estándares de seguridad de la información. • Identifica oportunidades de optimización, monitoreo y demás aspectos técnicos que contribuyan a las distintas soluciones • Establece pautas de despliegue alineadas a las políticas de la organización y buenas prácticas para los distintos desarrollos

Requisitos			¿Cumple? (SI/NO)	Integrantes del equipo
Formación	Excluyente	Egresado o estudiante avanzado de carrera universitaria.		
	Sugerido	Certificación de calidad y/o gestión de proyectos		
Experiencia	Excluyente	Experiencia en al menos 3 proyectos en implementación del producto propuesto en los que ha participado en calidad de Consultor Funcional Senior en los últimos 4 años al momento de la apertura de las ofertas.		

Consultor técnico Senior **Cantidad sugerida: 1**				
Descripción	• Analiza y evalúa las necesidades y requerimientos planteados, según contexto de la organización. • Implementa el desarrollo de soluciones y colabora en el diseño de las mismas. • Coordina con áreas de apoyo a los procesos de desarrollo • Elabora documentación técnica de las soluciones • Asesora y vela por el cumplimiento de las políticas y estándares de seguridad de la información. • Identifica oportunidades de optimización, monitoreo y demás aspectos técnicos que contribuyan a las distintas soluciones			
Requisitos			¿Cumple? (SI/NO)	Integrantes del equipo
Formación	Excluyente	Egresado o estudiante de carrera técnica en sistemas de 4 años o más		
	Sugerido	Certificación técnicas		
Experiencia	Excluyente	Experiencia en al menos 3 proyectos en implementación del producto propuesto en los que ha participado en calidad de Técnico Senior en los últimos 4 años al momento de la apertura de las ofertas.		

Consultor técnico Junior **Cantidad sugerida: 1/n**				
Descripción	• Implementa el desarrollo de soluciones y colabora en el diseño de las mismas. • Elabora documentación técnica de las soluciones • Asesora y vela por el cumplimiento de las políticas y estándares de seguridad de la información. • Identifica oportunidades de optimización, monitoreo y demás aspectos técnicos que contribuyan a las distintas soluciones			
Requisitos			¿Cumple? (SI/NO)	Integrantes del equipo
Formación	Excluyente	Egresado o estudiante de carrera técnica en sistemas de 4 años o más		
	Sugerido	Certificación técnicas		
Experiencia	Excluyente	Experiencia en al menos 2 proyectos en implementación del producto propuesto en los que ha participado en calidad de Técnico en los últimos 4 años al momento de la apertura de las ofertas.		

<table>
<tr><td colspan="5">Tester
Cantidad sugerida: 2</td></tr>
<tr><td>Descripción</td><td colspan="4">• Analiza, revisa y evalúa los requerimientos proporcionados.
• Evalúa y Escribe y revisa la estrategia de pruebas
• Planifica, diseña y ejecuta las pruebas según la estrategia definida
• Define set de datos necesarios para la ejecución de las pruebas
• Implementa las pruebas en todos los niveles, ejecuta, registra y evalúa los resultados,
• Elabora documentación relativa al proceso de pruebas (casos de prueba, informes de avance, etc.)
• Elabora manuales de uso de las soluciones..</td></tr>
<tr><td colspan="3">Requisitos</td><td>¿Cumple? (SI/NO)</td><td>Integrantes del equipo</td></tr>
<tr><td rowspan="2">Formación</td><td>Excluyente</td><td>Deberá contar con alguna de las siguientes características
• Carrera técnica en sistemas finalizada
• Diploma Tester Profesional de Software CES o equivalente</td><td></td><td rowspan="3"></td></tr>
<tr><td>Sugerido</td><td>ISTQB Foundation Level o equivalente</td><td></td></tr>
<tr><td>Experiencia</td><td>Excluyente</td><td>Se deberá contar con al menos 2 años de experiencia en diseño y ejecución de pruebas funcionales.</td><td></td></tr>
</table>

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

6.6 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. Podrá 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)
- Compatibilidad para autenticación con alguno de los siguientes proveedores de identidades (Google, Active Directory) detallando protocolos y configuraciones usados.
- Posibilidad de autenticación con múltiples factores (MFA) para cuentas privilegiadas.

Gestión de sesiones

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

Para esto deberá:

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

Control de acceso

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

Para esto deberá cumplir que::

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

Codificación y validación

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

La solución deberá cumplir con:

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

Manejo de errores y verificación de logs

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

Para lograr esto la solución deberá:

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

Confidencialidad y Protección de datos

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

- Cumplir con la normativa vigente uruguaya en materia de datos personales (Ley Nº 18.331, de 11 de agosto de 2008 y Decreto Nº 414/2009, de 31 de agosto de 2009). Se considera dato personal la información de cualquier tipo referida a personas físicas o jurídicas determinadas o determinables, a modo enunciativo, cualquier información numérica, alfabética, gráfica, fotográfica, registro de voz e imagen, acústica o de cualquier otro tipo que refiera a ellas directa o indirectamente, conforme con lo dispuesto en el artículo 4 de la Ley 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 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 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.

API y Web services

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

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

Respaldos y contingencia

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

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

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

Criptografía

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

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

Código malicioso

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

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

Lógica de negocio

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

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

Configuración

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

Los mismos deberán incluir:

- Un entorno lo más seguro, repetitivo y automatizable posible a través de la incorporación de buenas prácticas (ej. modelo DevSecOps) con herramientas, procesos y tecnologías que la * implementen adecuadamente (ej. contenedores, despliegues automatizados, etc.).

- Herramientas y entornos de desarrollo actualizados y correctamente mantenidos.
- Herramientas y entornos de desarrollo correctamente configurados y verificados en su seguridad (hardening) como por ej. deshabilitar el modo debug en entornos de producción.
- Seguridad por defecto en las configuraciones de los usuarios y los permisos.

Certificaciones

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

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

Metodología

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

Análisis de vulnerabilidades

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

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

.

+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	¿Acepto lo requerido? [SI/NO]	Observaciones (si corresponde)
1	Diseño y Arquitectura	Obligatorio		
2	Autenticación	Obligatorio		
3	Gestión de sesiones	Obligatorio		
4	Control de acceso	Obligatorio		
5	Codificación y validación	Deseado		
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	Obligatorio		
14	Lógica de negocio	Deseado		
15	Configuración	Obligatorio		

16	Certificaciones	Deseado		
17	Metodologías	Deseado		
18	Análisis de vulnerabilidades	Deseado		

El campo Cumplimiento deberá completarse con "Cumple totalmente", "Cumple parcialmente" o "No cumple", con la observación que consideren pertinente añadir.

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.

Requisitos de seguridad de la información y privacidad a ser tenidos en cuenta al momento de firmar el contrato con el proveedor adjudicado y la contratación de horas de consultoría y desarrollo.

Requisitos obligatorios

Estos requisitos son obligatorios para todos los llamados de compras de horas de servicio, a ser adquiridas por Centro Ceibal. Podrán haber excepciones que deberán estar justificadas y aprobadas por quien corresponda.

Cumplimiento de Políticas

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

Todo proveedor debe conocer el Manual de Políticas de Seguridad de la Información

Acuerdo de confidencialidad

Se deberá incluir una cláusula de confidencialidad con el proveedor adjudicado que garantice la protección de la información de Ceibal.

Ejemplo de cláusula de confidencialidad:

El Proveedor se obliga a tratar la información a la que acceda de manera confidencial y únicamente en el marco del cumplimiento del presente contrato.

El término "Información Confidencial" incluye, sin que ello implique limitación toda información tangible o intangible de tipo cultural, técnico, económico, financiero, comercial, estratégico o de cualquier otro tipo (sea de las Instituciones, servicios, alumnos, beneficiarios, centros educativos o terceros), incluyendo, pero no limitado a datos personales, que sea revelada, por cualquier medio, de forma oral, escrita, o en cualquier soporte.

La "Información Confidencial" no podrá ser revelada por el Proveedor a ningún tercero, sin el consentimiento previo y por escrito del Centro Ceibal.

En este contexto, el Proveedor se obliga a:

(a) no revelar ninguna Información Confidencial a terceros, y no utilizarla en beneficio propio o de terceros ni aún luego de finalizado el contrato que las vincula;

(b) adoptar precauciones razonables de seguridad para conservar en secreto la Información Confidencial de acuerdo con los lineamientos que establezca Ceibal;

(c) no divulgar, reproducir, resumir ni distribuir Información Confidencial.

No quedará sujeta a la obligación de confidencialidad la información que:

(a) sea o deviniera de dominio público sin responsabilidad ni intervención de las partes del presente convenio; y (b) fuera requerida por una autoridad competente y siempre que la parte se encontrara legalmente obligado a divulgarla. De todas formas, ante un eventual requerimiento de Información Confidencial, emanado del Poder Judicial o de cualquier autoridad reguladora, el Proveedor se obliga a

notificar de inmediato al Centro Ceibal parte del requerimiento y remitirle sus antecedentes a fin de brindarle a la parte una oportunidad razonable para cuestionar, limitar y/o asistir en la forma de dicha divulgación.

Uso de la infraestructura del Centro Ceibal

En el caso que el servicio a contratar incluya el uso, instalación, configuración y/o mantenimiento de infraestructura de Ceibal tanto lógica como física, se deberán estipular claramente las condiciones, responsabilidades y usos adecuados de la información afectada de manera de asegurar la confidencialidad, integridad y disponibilidad de la misma. A tales efectos, se recomienda:

- Estipular claramente las responsabilidades y tareas que puedan quedar a cargo de los proveedores.
- Realizar una gestión adecuada de los usuarios generados a los proveedores. Esto debe incluir:
- Información de las altas, bajas y modificaciones de los funcionarios de los proveedores por parte de estos en tiempo y forma, incluyendo los perfiles y roles a ser generados, de manera de garantizar un acceso seguro a los recursos de Ceibal.
- Generar los usuarios de VPNs y demás componentes necesarios para un acceso seguro, usando los criterios de mínimos privilegios.
- Coordinar con los proveedores, las medidas de seguridad a ser configuradas en la infraestructura de Ceibal, como ser listas blancas de IPs permitidas, conexiones de administración remota permitidos y aplicaciones habilitadas.
- Informar y acordar en conjunto con los proveedores las configuraciones de seguridad en servidores, estaciones, dispositivos de red y demás componentes tecnológicos a ser usados y/o administrados por los proveedores. Esto incluye entre otros el hardening de componentes y las configuraciones de logs y auditoría.
- Detallar claramente los esquemas de comunicación y gestión de incidentes que permitan asegurar la continuidad del negocio del Centro Ceibal, tomando en cuenta la criticidad de los activos gestionados.

Protección de la información manejada

La información sobre el Centro Ceibal manejada por el proveedor deberá cumplir con los requisitos establecidos en el Manual de Políticas de Seguridad de la Información. Para ello deberá cumplir con las

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

medidas de seguridad que garanticen una confidencialidad, integridad y disponibilidad de la información tanto en reposo como en tránsito y en uso. En el caso que la información sea almacenada en servidores del proveedor ya sea en modalidad onpremise o en nubes, se deberán extremar los cuidados.

Protección de la información en reposo

La información en reposo deberá estar protegida de manera de garantizar la seguridad de la misma. De acuerdo al nivel de criticidad y sensibilidad de la información se podrán implementar distintos controles de seguridad. Se promueve:

- La encriptación a nivel de discos, dispositivos y/o base de datos.
- El uso de herramientas de DPL (data loss prevention) y CASB (cloud access security brokers).
- NO crear ni usar copias de la información, solamente en los casos que son necesarios.
- Cumplir con las distintas regulaciones en materia de protección de datos.

Protección de la información en tránsito

La información en tránsito deberá estar protegida, garantizando que no esté disponible para usuarios en general y no sea pasible de ataques de ciberseguridad como por ejemplo: "Man in the Middle";. Para ello se promueve:

- La encriptación para los datos en tránsito, por ejemplo al enviarlo como adjunto en un correo electrónico o un medio físico como un pendrive.
- El uso de SFTP en el caso de compartir información a través de servidores o transferencia gestionada de archivos a través de links encriptados seguros (con cifrado cifrado SSL y TLS).
- El uso de herramientas de DPL (data loss prevention) y CASB (cloud access security brokers).

Protección de la información en uso

La información en uso deberá estar protegido garantizando la confidencialidad, integridad y disponibilidad de la misma. Para ello se promueve:

● El uso adecuado de sistemas de gestión de identidades que permitan una correcta autenticación de usuarios en los sistemas del proveedor que incluyan por ejemplo: uso de políticas de contraseñas

adecuadas, doble factor de autenticación para cuentas privilegiadas y otras medidas habituales para asegurar la identidad de los usuarios con acceso a la información.

● El uso de sistemas de autorización de usuarios adecuados que garanticen que los usuarios con los perfiles y roles correctos puedan acceder a la información para la cual tienen los privilegios necesarios.

● La aplicación de políticas, procesos y controles tecnológicos que garanticen la seguridad de la información en uso.

Concientización y capacitación del personal

El personal del proveedor deberá estar informado y concientizado con el objetivo de gestionar de manera segura la información que manejen del Centro Ceibal y dar un adecuado tratamiento a posibles incidentes de seguridad. Para ello se recomienda:

● Capacitar y concientizar al personal en temas relacionados a la seguridad de la información y la privacidad.

● Informar al personal de los canales y procesos adecuados para poder reportar eventos de seguridad en Ceibal.

● Concientizar al personal en la correcta aplicación de los procesos asociados a la seguridad de la información, como por ejemplo: uso adecuado de contraseñas, uso seguro en entornos de teletrabajo, manejo responsable de dispositivos móviles y compartir información de manera segura.

Trazabilidad y auditoría

Centro Ceibal se reserva el derecho de auditar los procesos relacionados a la seguridad de la información y la privacidad con el objetivo de verificar que se cumpla lo estipulado entre las partes. Para ello podrá solicitar al proveedor la documentación respaldante que corresponda en cada caso. A estos efectos deberá preverse tal facultad en el contrato.

Ejemplo de cláusula:

Centro Ceibal se reserva el derecho de auditar los procesos relacionados a la seguridad de la información y la privacidad del Proveedor con el objetivo de verificar que se cumpla lo estipulado entre las partes. En este contexto podrá solicitar al proveedor la documentación respaldante que corresponda en cada caso.

Protección de datos personales

Incluir en el acuerdo con el proveedor una cláusula que regule la protección de datos personales, y en los casos que sea necesario firmar un acuerdo de encargado de tratamiento.

Ejemplo cláusula Protección de datos personales:

En caso de acceder a datos personales el Proveedor se obliga a su tratamiento 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, y a utilizarlos exclusivamente para los fines del acuerdo que vincula a las partes, no pudiendo utilizarlos para otra finalidad, ni cederlos, comunicar o transferirlos a terceros, salvo previa autorización por escrito del Centro Ceibal, y sus titulares o representantes.

Centro Ceibal es responsable de sus bases de datos, siendo el Proveedor, en caso de acceder a la base de datos, encargado de tratamiento, de acuerdo con lo dispuesto en los literales H) y K) del artículo 4 de la Ley Nº 18.331. No se autoriza la subcontratación de encargados de tratamiento de datos.

El Proveedor se obliga a adoptar las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de los datos personales y evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información.

En caso de que se alojen los datos personales, el Proveedor se obliga a que los servidores se sitúen en Uruguay. Sin perjuicio de lo anterior, en caso que los datos se alojen, aun temporalmente, fuera del territorio nacional, se obliga a que el servidor se encuentre en países considerados con niveles adecuados a los estándares europeos de protección de datos, de acuerdo con el Reglamento General de Protección de Datos 2016/679, del Parlamento Europeo y del Consejo, modificatorias, concordantes y complementarias.

Frente a requerimiento del Centro Ceibal, el Proveedor se obliga a 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, 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.

En la columna de la siguiente tabla "Acepto lo requerido"; es donde el oferente deberá expresamente indicar "SI" o "No" con lo solicitado. En caso de que no se indique explícitamente el cumplimiento por parte del oferente, la oferta será rechazada.

Matriz de cumplimiento de requerimientos de Seguridad de la Información Compra de horas de servicios (consultoría, desarrollo, soporte, etc.)		
A completar en conjunto por parte de Ceibal y el proveedor		
Requerimiento	**¿Acepto lo requerido? [SI/NO]**	**Observaciones (si corresponde)**
Cumplimiento de políticas		
Acuerdo de confidencialidad		
Uso de la infraestructura de Ceibal		
Protección de la información manejada		
Concientización y capacitación		
Trazabilidad y auditoría		
Protección de datos personales		

Fin del documento

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

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