LLAMADO A EXPRESIÓN DE INTERÉS

Evaluación de Mecanismos de Autenticación

Diciembre 2021

1. OBJETO

Centro Ceibal llama a interesados en realizar pruebas de concepto de soluciones tecnológicas, con foco en mecanismos de autenticación, que podrían ser aplicables a Plan Ceibal.

El interesado se obliga en los términos de la política de confidencialidad y protección de datos de Centro Ceibal, especificadas en el *Anexo I: Confidencialidad y protección de datos*.

2. CATEGORÍAS

Las soluciones de interés se dividen en dos categorías y los interesados podrán proponer tanto soluciones de equipamiento como servicios asociados.

2.1. Mecanismos de Autenticación para Beneficiarios

La categoría Mecanismos de Autenticación para Beneficiarios comprende cualquier producto, de software, de hardware o combinado, destinado a resolver de manera parcial o completa la autenticación de los beneficiarios del Plan Ceibal (estudiantes, docentes, entre otros actores). Es deseable que los mecanismos presentados sean alternativas novedosas a la autenticación tradicional realizada con credenciales del tipo usuario - contraseña.

2.2. Mecanismos de Autenticación para Funcionarios de Plan Ceibal

La categoría Mecanismos de Autenticación para Funcionarios de Plan Ceibal comprende cualquier producto, de software, de hardware o combinado, destinado a resolver el control de acceso, tanto lógico como físico, de los funcionarios y otras personas al edificio, a determinadas áreas y a soluciones tecnológicas, con distintos niveles de restricción.

3. MODALIDAD

En la categoría Mecanismos de Autenticación para Beneficiarios (2.1), dependiendo del tipo de solución propuesta, ésta podrá evaluarse tanto en laboratorio como en determinados centros educativos a modo de piloto, de forma de emular en contexto real el uso de los mecanismos.

En la categoría Mecanismos de Autenticación para Funcionarios de Plan Ceibal (2.2), la modalidad dependerá también de la naturaleza de las soluciones seleccionadas. En general, se realizarán pruebas a nivel de laboratorio y en el edificio de Centro Ceibal a modo de piloto.

3.1. Presentación

El oferente debe presentar su propuesta indicando, como mínimo, lo siguiente:

A. Especificaciones técnicas del mecanismo de autenticación.
B. Costo unitario del mecanismo de autenticación, a modo de referencia.
C. Costo de servicios ofertados, en caso que aplique, a modo de referencia.
D. Esquema y costo del licenciamiento, en caso que aplique (plano, por volumen, por equipo, por usuario, etc.).

3.2. Demostraciones, Muestras y Selección

Centro Ceibal podrá solicitar demostraciones ("*demos*") de las soluciones, así como muestras de hardware de los mecanismos propuestos si aplica, en cantidad a convenir con el oferente. En caso de que estas tengan un costo, el interesado deberá expresarlo al presentar su propuesta.

Centro Ceibal podrá seleccionar aquellas propuestas que considere adecuadas e interesantes (según su estrategia, necesidad, urgencia, conveniencia, etc.) para realizar pruebas de concepto, y propondrá un plan de implementación, que puede no ser de ejecución inmediata, para que sea evaluado por el oferente. El plan de implementación definitivo, así como los plazos asociados y los costos se definirán en cada caso de común acuerdo entre las partes.

ANEXO I: Confidencialidad y Protección de Datos

El interesado seleccionado, 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 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 por la Empresa de cualquier fuente o pudiera ser desarrollada como consecuencia del presente contrato.

Asimismo, y en caso de que tuviera acceso a datos personales, se obliga al tratamiento de los mismos 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 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.

En ningún caso el acceso a datos personales podrá entenderse como cesión o permiso para su libre utilización por parte de la Empresa, excepto en el marco de lo que fuere acordado y contratado.

La Empresa se obliga a no alojar datos personales, salvo comunicación y previa autorización de Ceibal, en cuyo caso los servidores deberán estar en Uruguay o bien 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, modificativas, concordantes y complementarias.

Asimismo, deberá 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.

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. 4.3

ANEXO II - Requisitos obligatorios y deseados de seguridad

Requisitos obligatorios

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.

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.

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.

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),

Comunicaciones

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

Para esto deberá:

- Publicar servicios a través de protocolos seguros (TLS o encriptación robusta) para todos los usuarios y sin importar la sensibilidad de la información transmitida.
- Se utilizarán protocolos y algoritmos considerados seguros por la industria y las buenas prácticas, dejando como último recurso o por temas de compatibilidad que sean expresamente autorizados por Centro Ceibal el uso de otros protocolos menos seguros.
- La solución deberá ser enteramente compatible con los certificados usados por Centro Ceibal (ver Documento) y en caso de usar certificados generados

internamente deberán ser validados por las autoridades de certificación que Centro Ceibal establezca.
- Todas las comunicaciones por fuera del protocolo HTTP, como por ej. accesos remotos, comunicación entre capas de la solución, middleware, bases de datos, fuentes externas de datos, monitoreo, herramientas de comunicación, etc. deberán ser comunicaciones seguras y en lo posible encriptadas.

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.

Requisitos deseados

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.

Código malicioso

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

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

Lógica de negocio

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

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

Configuración

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

Los mismos deberán incluir:

- Un entorno lo más seguro, repetitivo y automatizable posible a través de la incorporación de buenas prácticas (ej. modelo DevSecOps) con herramientas, procesos y tecnologías que la * implementen adecuadamente (ej. contenedores, despliegues automatizados, etc.).
- Herramientas y entornos de desarrollo actualizados y correctamente mantenidos.
- Herramientas y entornos de desarrollo correctamente configurados y verificados en su seguridad (hardening) como por ej. deshabilitar el modo debug en entornos de producción.
- Seguridad por defecto en las configuraciones de los usuarios y los permisos.

Certificaciones

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

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

Metodología

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

Análisis de vulnerabilidades

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

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

Matriz de cumplimiento

Nº Req.	Requerimiento	Tipo	Cumplimiento
1	Diseño y Arquitectura	Obligatorio	
2	Autenticación	Obligatorio	
3	Gestión de sesiones	Obligatorio	
4	Control de acceso	Obligatorio	
5	Manejo de errores y logs	Obligatorio	
6	Confidencialidad y protección de datos	Obligatorio	
7	Comunicaciones	Obligatorio	

8	Criptografía	Obligatorio	
9	Respaldos y contingencia	Obligatorio	
10	API y Web Services	Deseado	
11	Código malicioso	Deseado	
12	Lógica de negocio	Deseado	
13	Configuración	Deseado	
14	Certificaciones	Deseado	
15	Metodologías	Deseado	
16	Análisis de vulnerabilidades	Deseado	