Plan Ceibal

Information Security and Privacy Requirements

Solution in the cloud of Content Filtering by DNS

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

Telecommunications Management

Aim

This document details the Information Security and Privacy Requirements of the LPI " Solution in the Cloud for Content Filtering by DNS" so that the bidder can complete the "Compliance Matrix for Information Security and Privacy requirements".

Requirements

Mandatory Requirements

These requirements are mandatory for the offer to be accepted.

Desirable requirements

They are not mandatory but clarification is requested on the compliance of the product / service with respect to these requirements.

Description of requirements

1) Authentication (desirable)

It is requested to detail the secure authentication methods that allow verifying the identity of the users and protect the confidentiality of the information.

It must be specified whether it is possible to incorporate the following requirements:

- Authentication with username and password that complies with the password policies Centro Ceibal. (See document) (Ver documento)
- Compatibility with centralized authentication systems (SSO) used by Centro Ceibal as it corresponds:
- Unique Login System for beneficiaries. (CAS protocol)
- Support for authentication with any of the following identity providers (Google, Active Directory) detailing protocols and configurations used.
- Multi-factor authentication (MFA) capability for privileged accounts.

2) Session management (desirable)

Adequate management of user sessions allowing to know the current status of the user or the connected device.

For this it is desirable:

- To Maintain unique sessions for each user that cannot be guessed or shared.
- Sessions will be disconnected when they are no longer needed or during a period of inactivity (if possible, parameterizable).

3) Access control (mandatory)

The solution must provide adequate access control management in order to authorize access to functionalities and data in accordance with the profiles and roles that are defined.

For this, it must complied with:

- Users who want to access certain resources must have the correct credentials.
- Users are associated with an appropriate set of roles and privileges according to the functionalities provided by the solution and the accessible resources.

4) Confidentiality and Data Protection (mandatory)

The solution must ensure the confidentiality, integrity and availability of the information and personal data. To implement adequate data protection, the solution must ensure: legality, veracity, purpose, prior informed consent, data security, reservation, and responsibility. For this the solution must:

- Comply with current Uruguayan regulations on personal data (Law No. 18,331, of August 11, 2008 and Decree No. 414/2009, of August 31, 2009). Information of any kind referring to specific or determinable natural or legal persons is considered personal data, by way of example, any numerical, alphabetical, graphic, photographic, voice and image, acoustic or any other type of information that refers to them directly or indirectly, in accordance with the provisions of Article 4 of Law No. 18,331 and Articles 1 and 4 of Decree No. 414/009.
- Adopt the necessary security measures to guarantee the security and confidentiality of the data and avoid its adulteration, loss, consultation or unauthorized treatment, as well as detecting deviations of information.
- Protect information and data created, edited, deleted or accessed without the corresponding authorizations, particularly in massive amounts of data.
- Take the necessary precautions and controls so that information and personal data are not available in browsers, load balancers, temporary copies, cookies and other structures where it is not necessary.
- Ensure the confidentiality of all information that is processed or used. Confidential Information includes, among others and by way of example, the following information: any business strategy, plan and procedure, proprietary information, software, tool, process, images, personal data, methodology, information and trade secret, and other information and material from Ceibal, as well as from the students, beneficiaries, teachers, study centers, that could be obtained from any source or could be developed.
- Host the data in Uruguayan territory, or in the case of international transfer, ensure that the server is located in countries considered with adequate levels in accordance with Directive 95/46 / CE. Otherwise, it is necessary to have the consent of the owner of the data for the transfer to an inappropriate territory, or that the importer has signed standard contractual clauses with the exporter or has a registered Code of Conduct, with the consequent authorization of international data transfer processed before the Regulatory and Control Unit of Personal Data, in the last two cases.

- Do not use the information / data for a purpose other than the one contracted, nor for their own benefit, whether free or onerous, nor assign, communicate or transfer them to third parties.
- Centro Ceibal will be responsible for the database and its treatment, being the awarded Company and its subcontracted companies, in charge of treatment, in accordance with the provisions of literals H) and K) of article 4 of Law No. 18,331 .
- Allow the publication of the privacy policies and terms and conditions of use of Centro Ceibal in development.
- Allow the right of access, rectification, updating, inclusion or deletion of personal data.
- Return or delete from all its physical and logical systems and files, whether owned or contracted to third parties, the personal data accessed, obtained or processed, as well as the associated metadata, at the request of Ceibal.

5) API and Web services (desirable)

The solution that makes use of APIs (commonly through the use of JSON, XML, GraphQL or other formats) must detail compliance with:

- Maintain adequate authentication, session management and authorizations for all web services.
- Input validation for all parameters that are entered.
- Effective security controls over all types of APIs, including cloud and serverless APIs.

6) Business logic (desirable)

The solution that provides a business layer developed in a secure way and that allows to avoid the most frequent cyberattacks must detail if:

- The flow of business logic must be sequential, consistent and cannot be altered.
- The business logic includes controls and limits to detect and prevent automated attacks.
- The business logic must take into account use cases that include malicious actors, abuse cases and must also contain protections against spoofing attacks, manipulation, repudiation, information disclosure and elevation of privileges, among others.

7) Certifications (desirable)

Certifications and compliance with standards related to secure development, information security and privacy will be valued, such as:

- 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

8) Vulnerability analysis (desirable)

Solutions that have undergone standardized vulnerability checks and / or penetration tests will be evaluated. Proof of the same must be provided by means of a summary report or corresponding certificate.

Report detailing threat coverage on the latest OWASP Top Ten in force will be valued.