REQUEST FOR INFORMATION N°90009707 – DATA LOSS PREVENTION
Multi-platform Data Loss Prevention (DLP) Tool

1. Objective

The Central Bank of Chile is currently evaluating technological solutions to reinforce its Data Loss Prevention (DLP) capabilities in multi-platform environments, including AIX/Linux-based systems, corporate storage, and public cloud services not dependent on a specific vendor.

The purpose of this Request for Information (RFI) is to identify vendors that can provide a robust and scalable solution aligned with the Bank's functional, regulatory, and operational requirements, specifically in relation to:

- Technical compatibility
- Detection, classification, and labeling capabilities
- Multi-platform support
- Adaptability to distributed and critical environments
- Compliance with security regulations and standards (both domestic and international)
- Scalability

2. Questions and Questionnaire answers Process

The Vendors or Companies interested in participating in this RFI process must send an email to cguajard@bcentral.cl with a copy to cotizaciones@bcentral.cl, indicating in the subject: "INTEREST IN PARTICIPATING: 90009707 RFI Data Loss Prevention", no later than the date indicated in the Calendar of Activities.

Should the Company have any questions or comments regarding this process and its Questionnaire, they must be submitted no later than the date indicated in the Calendar of Activities, to the email address: cguajard@bcentral.cl with a copy to cotizaciones@bcentral.cl, indicating in the subject "QUESTIONS: 90009707 RFI Data Loss Prevention" which will be answered on the date indicated in the Calendar of Activities, ensuring the anonymity of those Companies that have sent questions.

Subsequently, the Company must send its responses to the Questionnaire detailed in section number 4 of this document, no later than the date indicated in the Calendar of Activities, to the following email addresses: cguajard@bcentral.cl with a copy to cotizaciones@bcentral.cl, indicating in the subject "RESPONSE: 90009707 RFI Data Loss Prevention".

Companies must submit a structured response including:

- Overview of the company and the product being offered
- Functional Compliance Matrix (section number 4.1)
- Positioning in Industry Rankings (section number 4.2)
- Specific Technical Questions (section number 4.3)
- Information of the Vendor/Company (section number 4.4)

The Bank reserves the right to ask for further clarifications from all or any of the Vendors.

In addition to the written response, the Bank may request to all or some of the participating Vendors to make an online presentation of the proposed solution, lasting approximately 30 minutes, for further exploration on technical aspects and to clarify any queries the evaluation team of the Bank may have. Vendors must provide a copy of this presentation.

2.1. Calendar of Activities

Actividades	Fechas Máximas
RFI publication	2 October 2025
Questions reception	20 October 2025
Answers and clarifications	27 October 2025
Questionnaire answers reception	10 November 2025
Process close notification	1 December 2025

2.2. Considerations

- **Please note that this process does not constitute a Quotation, and therefore Vendors should refrain from submitting financial proposals.**
- This application is for informational purposes only and in no way commits the Central Bank of Chile to acquire or contract the Products and/or Services specified in this document.
- Should the Central Bank of Chile require the acquisition or contracting of these Products and/or Services, a Quotation or Bidding Process will be initiated through its Procurement Department.

3. Functional Scope

A DLP solution is required that covers the following areas:

3.1. Expected Platforms and Environments

- Enterprise Linux/AIX distributions widely supported in the market
- Relational databases commonly used in the financial industry
- Enterprise storage with NFS or SMB connectivity and API access
- Web applications, SaaS services, and non-Microsoft public cloud services

3.2. Expected Capabilities

- Discovery of sensitive data at rest, in use, and in transit
- Automatic classification and persistent labeling of files and structured data
- Definition of adaptive policies based on content type or behavior
- Automated actions (block, quarantine, alert)
- Integration with external tools (SIEM, SOAR, CMDB)
- Centralized management and distributed operation
- Dynamic policy updates without operational downtime

4. Questionnaire

4.1 Functional Compliance Matrix

Please complete the following table by marking Compliant, Partially Compliant, or Non-Compliant, and provide the corresponding justification or technical evidence:

Category	Technical / Functional Criterion	Compliant	Partially Compliant	Non-Compliant	Technical Details / Evidence Reference
Detection and Classification	Discovery of structured data in relational databases.				
	Automatic classification based on content and context.				
	Detection of data in use, in transit, and at rest.				
Technical Compatibility	Native support for enterprise Linux and AIX systems.				
	Granular support for encrypted databases (e.g., TDE encryption at rest).				
	Integration with enterprise storage via NFS/SMB or secure API.				
Policies and Control	Policies based on data type, user group, or behavior.				
	Automated actions: block, quarantine, alert.				
Data Labeling	Persistent labels on files and structured data fields.				
	Interoperability with external classification engines (e.g., Titus, Varonis).				

Category	Technical / Functional Criterion	Compliant	Partially Compliant	Non-Compliant	Technical Details / Evidence Reference
Regulatory Compliance	Support for applicable national regulations (Law 21459, 21180, 21733).				
	Compatibility with international standards (ISO/IEC 27001, NIST, GDPR).				
Administration and Scalability	Centralized console with distributed architecture.				
	Policy updates without service disruption ("hot updates").				
Experience and Support	Proven experience in institutions of the public sector or the financial sector.				
Big Data and Mass Storage	Native support for Big Data platforms (Hadoop, Spark, Cloudera, etc.)				
	Discovery and classification in Data Warehouses (e.g., Teradata, Snowflake, BigQuery, Redshift).				
	Compatibility with Datamarts and OLAP environments.				
	Ability to process large data volumes without performance degradation.				
Functional and Technical Constraints	Supported data types (plain text, JSON, XML, images, logs, semi-structured data, unstructured data).				
	Technical constraints (maximum size per file, indexing speed, and latency in bulk classification).				

Category	Technical / Functional Criterion	Compliant	Partially Compliant	Non-Compliant	Technical Details / Evidence Reference
	Policy enforcement restrictions (e.g., inability to apply tags to binary columns, encrypted fields, media data)				

4.2 Positioning in Industry Rankings

Recognition in Market Reports. Please state whether your solution has been reviewed in any of the following reports and in which category it is currently listed:

Industry Report	Included? (Yes/No)	Category (Leader, Visionary, etc.)	Year of Publication	URL / Public Link / PDF attachment
Gartner Magic Quadrant (DLP)				
Forrester Wave				
GigaOm Radar				

4.3 Specific Technical Questions

Please answer the following questions in a clear and structured manner:

A. Technical Capabilities of the Solution

1. Does your solution provide native agents for enterprise Linux/AIX distributions? From which version onwards?
2. Does your solution support discovering, classifying, and labeling structured data in encrypted databases (e.g., TDE)?
3. Does your solution allow direct labeling of fields, tables, or schemas within databases?
4. What integration mechanisms does it use to access enterprise storage (APIs, remote mounts, specific connectors)?
5. Does the solution support automatic classification based on content, context, and user behavior?
6. Does it feature mechanisms based on artificial intelligence or machine learning for advanced detection or contextual categorization?
7. What capabilities does it deliver for discovery and classification in SaaS and public cloud (non-Microsoft) environments?
8. Can it integrate with external classification engines (Titus, Varonis, others)? Under which standards or APIs?

9. Is your product technically certified (FIPS 140-2, Common Criteria, ISO/IEC 27001, or others)?
10. Does it support integration with monitoring platforms such as Splunk, QRadar, Azure Sentinel, or others?
11. Does it support integration with Active Directory, Azure AD, and Single Sign-On (SSO)? What are the requirements?
12. Does your solution support integration with Big Data platforms (Hadoop, Spark, Hive, Cloudera, etc.)? Please detail integration mechanisms.
13. Is the solution capable of discovering, classifying, and enforcing policies in Data Warehouses (e.g., Teradata, Snowflake, BigQuery, Redshift) and corporate Datamarts?
14. What types of data does the solution support (structured, semi-structured, unstructured, images, logs, binary data)? Are there any documented limitations?
15. What are the functional and technical constraints for processing large volumes of data (>1 TB, >10 million records)?
16. How does the solution handle real-time data classification and control on massive information streams (streaming, IoT, Kafka)?

B. Deployment, Management, and Scalability

17. What deployment modes does the solution support (on-premise, SaaS, hybrid, containers)?
18. What is the estimated standard implementation time for critical environments, including installation, configuration, and training?
19. What methodology does your company use for implementing this kind of project?
20. What type of management do you provide: centralized console, segmentation by organizational units, policy delegation?
21. Is it possible to update policies without rebooting or affecting availability ("hot updates")?
22. What are the minimum infrastructure requirements for basic and scaled operation?
23. What professional profiles are needed for implementation and operation? Is there a leveling plan or knowledge transfer plan?

C. Security, Support, and Life Cycle

24. What security mechanisms does the solution include (encryption, access control, traceability, auditing, secure disposal)?
25. Does the vendor agree to delete any information stored during PoC or implementation phases and to provide evidence of this deletion?
26. Does the solution provide mechanisms to export outputs (logs, evidence, reports, labels, event flows)?
27. What is the scope of technical support to be provided? Please specify language, time frame, availability, and modalities (remote, on-site, hybrid).
28. What is the licensing model proposed (per user, per node, per volume, per module, hybrid)?
29. Does it include a laboratory environment for practical demonstrations (PoC)? What capabilities does it offer?
30. Has the solution been implemented in institutions of the financial sector or the public sector before? Please describe at least one case.

4.4. Information of the Vendor/Company

Please complete the following information:

4.4.1. General information

- Company name:
- Tax ID / RUT:
- Domicile:
- Country:
- Official website:

4.4.2. Commercial contacts

Main business contact

- Full name:
- Position:
- E-mail address:
- Mobile phone number:

Secondary business contact

- Full name:
- Position:
- E-mail address:
- Mobile phone number:

4.4.3. Technical Experience and Resources

- Years in the market:
- Years in DLP solutions:
- Company certifications (ISO 27001, FIPS, Common Criteria, others):
- Total number of employees:
- Number of certified consultants, broken down by specialty field:

4.4.4. Relevant References

- Success stories in the financial sector or public sector (name, institution, and year):
- Similar services implemented in Chile or other countries, central banks (specify):

Santiago, 2 October 2025.

Procurement Department
CENTRAL BANK OF CHILE