SINGLAR Innovación

SAFECLOUD®

Information Protection

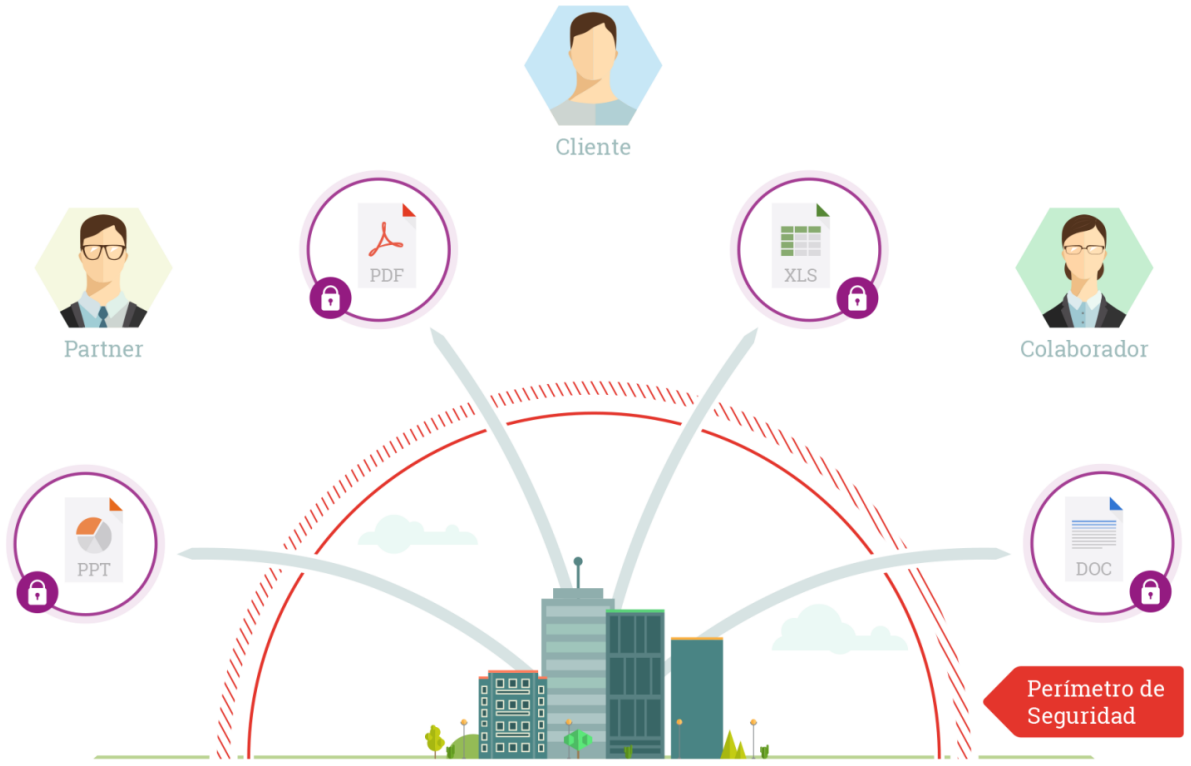
Take control and protect the most critical asset, move from management to governance.

Why Information Protection?

The end user is the main risk to an organization's information

OBJECTIVE: Protect information inside and outside the company's network

1. Sending files outside the organization
2. Downloading files from personal emails
3. Uploading files to the cloud without encryption
4. Dispersion of corporate information



Main Components

Information Protection

Security Management:

-Classification
-Rules of use and custody
-Data lifecycle
-Monthly monitoring of labeling and DLP.
-Forensic and legal defense.

Infrastructure:

- Information sources, communications, and repositories.
- Information monitoring: IRM, DLP, access auditing.

SafeCloud

CIO and DPO:

- Information Governance.

Security Operation

- Handling of alerts, labels, and data leakage..
- User support (CAU).

SINGLAR Innovación

Security Management

IT Governance, Compliance, Risk Management, and Security Master Plan

01

Information Security Management: P&P Methodology

Information Protection Plan. Rules of use and custody.

- Automatic or manual document labeling
- Email management according to the type of information
- How to share information with clients and suppliers securely
- Local storage (laptop / mobile)
- Encryption in storage / exchange
- Progressive introduction of labels by departments
- Development of a documentary framework
- Monitoring of information usage
- Incident response procedure

WE ENSURE SUCCESS IN THE IMPLEMENTATION OF CIO REPORTING AND DLP TECHNOLOGIES

SINGLAR Innovación

Security Infrastructure

Information Sources, Communications, Repositories, Information Tracking, IRM, DLP, or Access Auditing

02

Solutions

Information Protection

Document Generation	Labeling	Data Loss Prevention (DLP)	Information Protection (IRM)	Incident Response
				
CRM, ERP, Local	Automatic/manual (Templates)	Requires agent	Document-level protection	Behavior alerts, exfiltration alerts
Budgets, contracts, and orders	Metadata, watermark, and footer	Fine-tuning, dedicated teams	Maximum control	Managed by CIO, operator, or CyberSOC
Access auditing	Labeling	Within the organization	Outside the organization	SafeCloud

Partner / Integrador

Secure Exchange

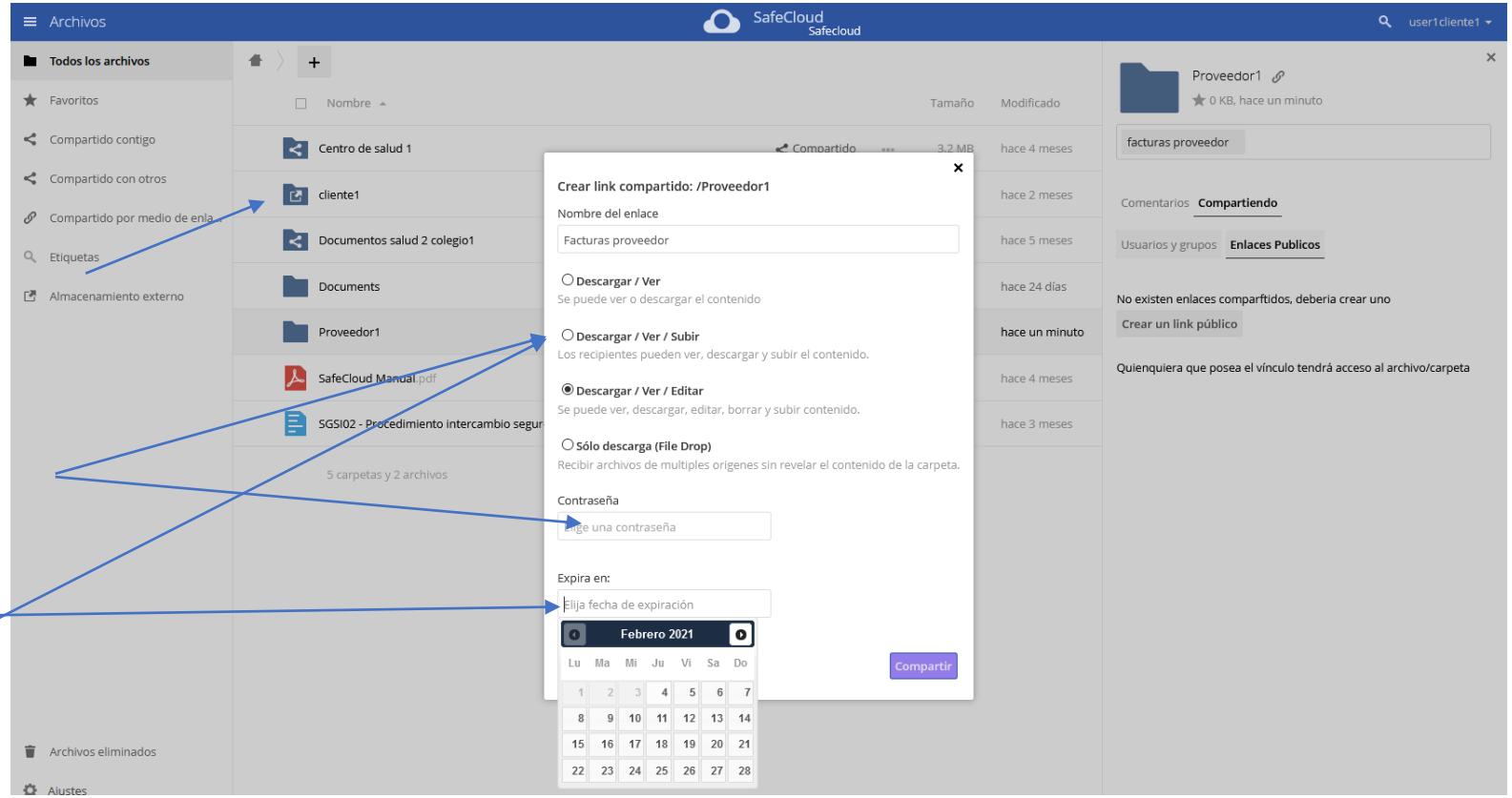
Information Protection

- Document exchange with clients and suppliers
- Information control inside and outside the organization
- Prevent phishing and CEO fraud attempts

Frequent collaborator
Create specific users for folder access

Regular supplier
Share directory with a known password.

Occasional supplier
Share directory with 24h expiration.



SINGLAR Innovación

CIO y DPO

Information Governance

03

CIO & DPO Portal

SafeCloud

Unified Access and Procedures

CAS

- To Storage
- To Procedures
- To Management Dashboards
- To Alert Dashboards

Secure Exchange Repositories Access

OneDrive

- Storage
- Secure Exchange
- Advanced Protection
- Easy Administration

IRM

- Information classification and labeling
- Easy methodology for phased IRM deployment
- Monitoring and governance dashboards

DLP

- Data loss prevention
- Predefined rules for easy adoption
- Monitoring dashboards for sensitive data (e.g., GDPR)
- Monitoring dashboards for data leakage

vDPO & vCIO Services

- The integrator can provide analysis services of dashboards and continuous improvement
- Progressive incorporation of labels (e.g., by department) and DLP rules

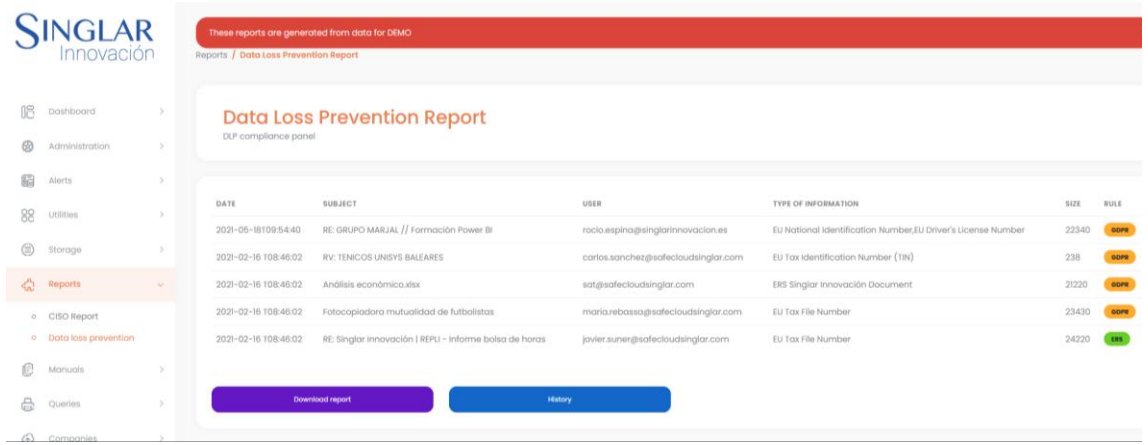
CAU Services

- User support services for classification, exchange, and access to information

Information Protection Management

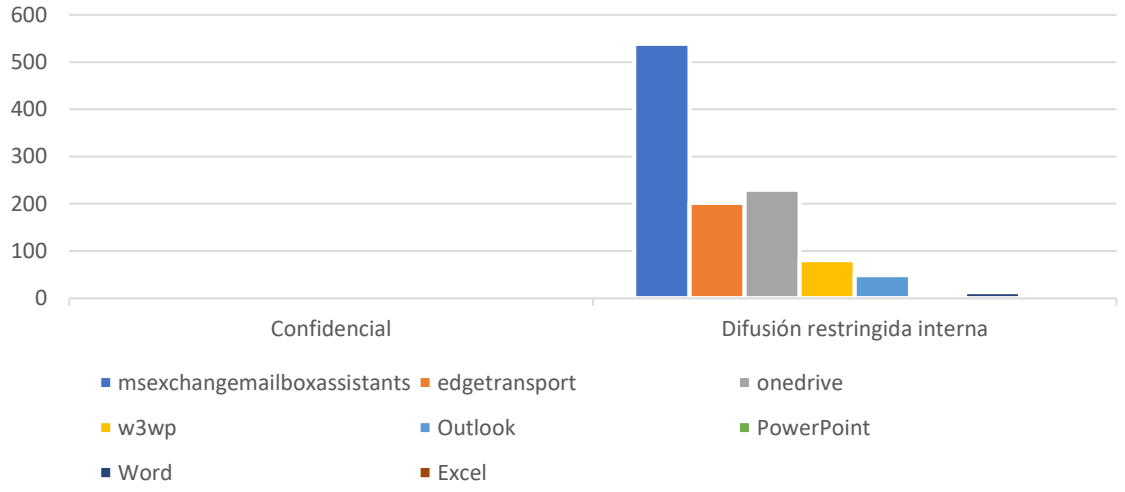
The tasks proposed to be delegated to the virtual CIO or DPO are:

- Centrally manage AIP dashboards / File Auditing / DLP / IRM / Other solutions.
- Periodic review of reports for the CISO and DPO:
  - Who labels and classifies documents, how, and their evolution over time.
  - Who accesses or attempts to access classified information.
  - Where sensitive information is located (e.g., GDPR) and how it moves.
  - Data exfiltration, who and how.
  - Document traceability: we can know everything that has happened to a document..
- Monthly monitoring of correct label usage (based on dynamic Excel sheet).
- Review of reports from users who share GDPR data externally.



Added Value on IRM and DLP

- Portal to understand and review the deployment of these technologies in the company, their success and proper adoption by users and third parties.
- Evolutionary reports to verify how employees use and adopt the technologies.
- Review for the DPO, who takes control of all sensitive information and who shares it.
- Possibility to raise awareness among users who misuse information, at the pace that the CIO and/or DPO can.



SINGLAR
Innovación

SAFECLOUD®

¡Thank you!