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

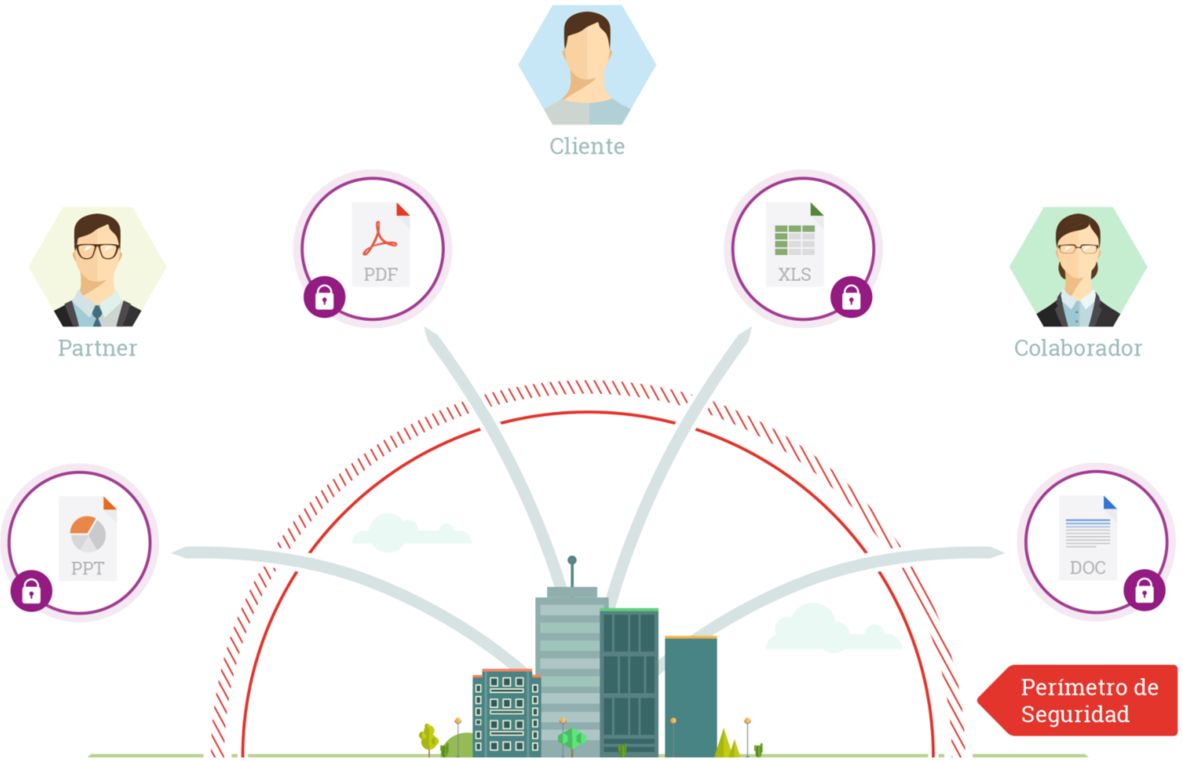
OBJECTIVE: Protect information inside and outside the company's network

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

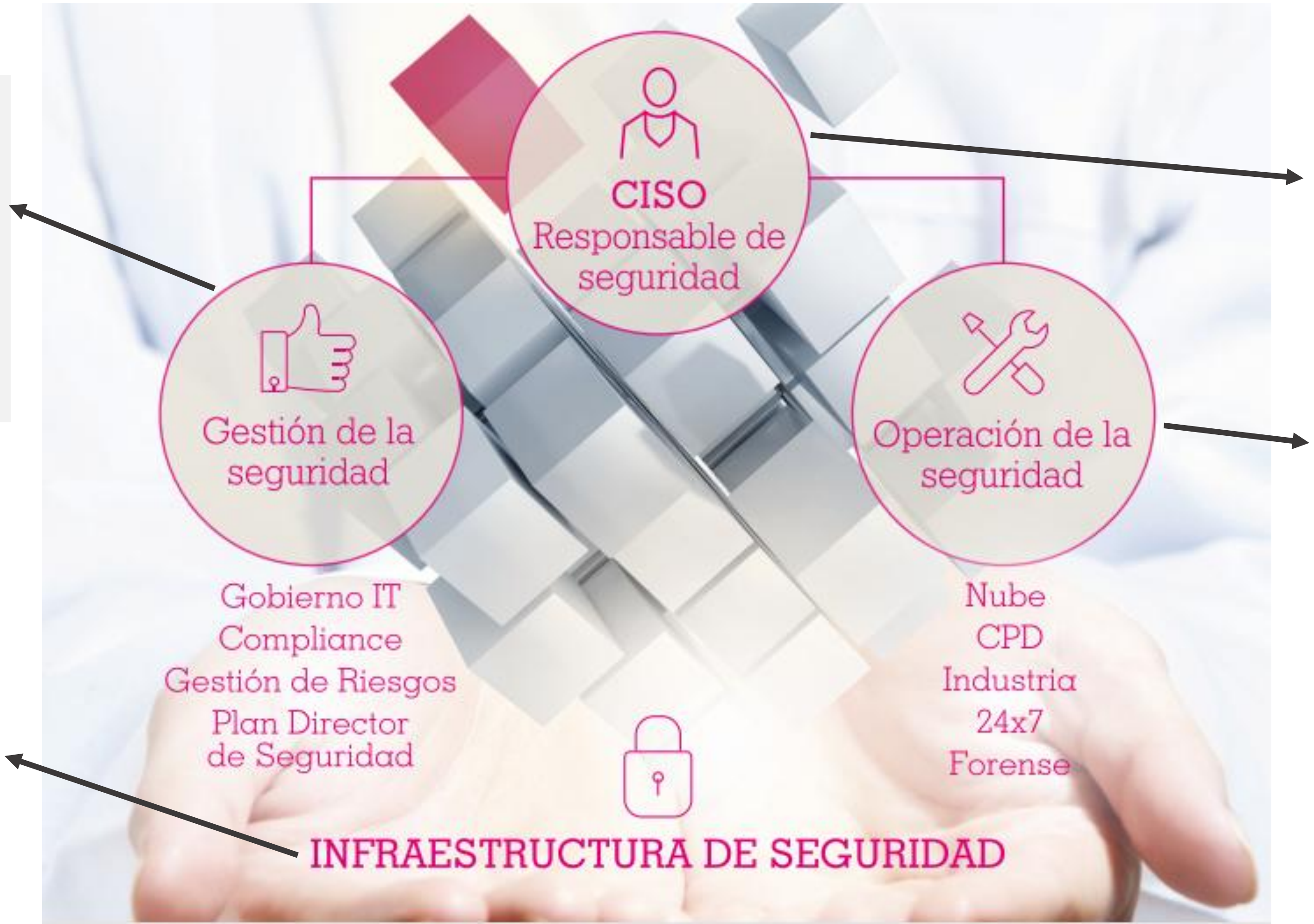
Information Protection

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).

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

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

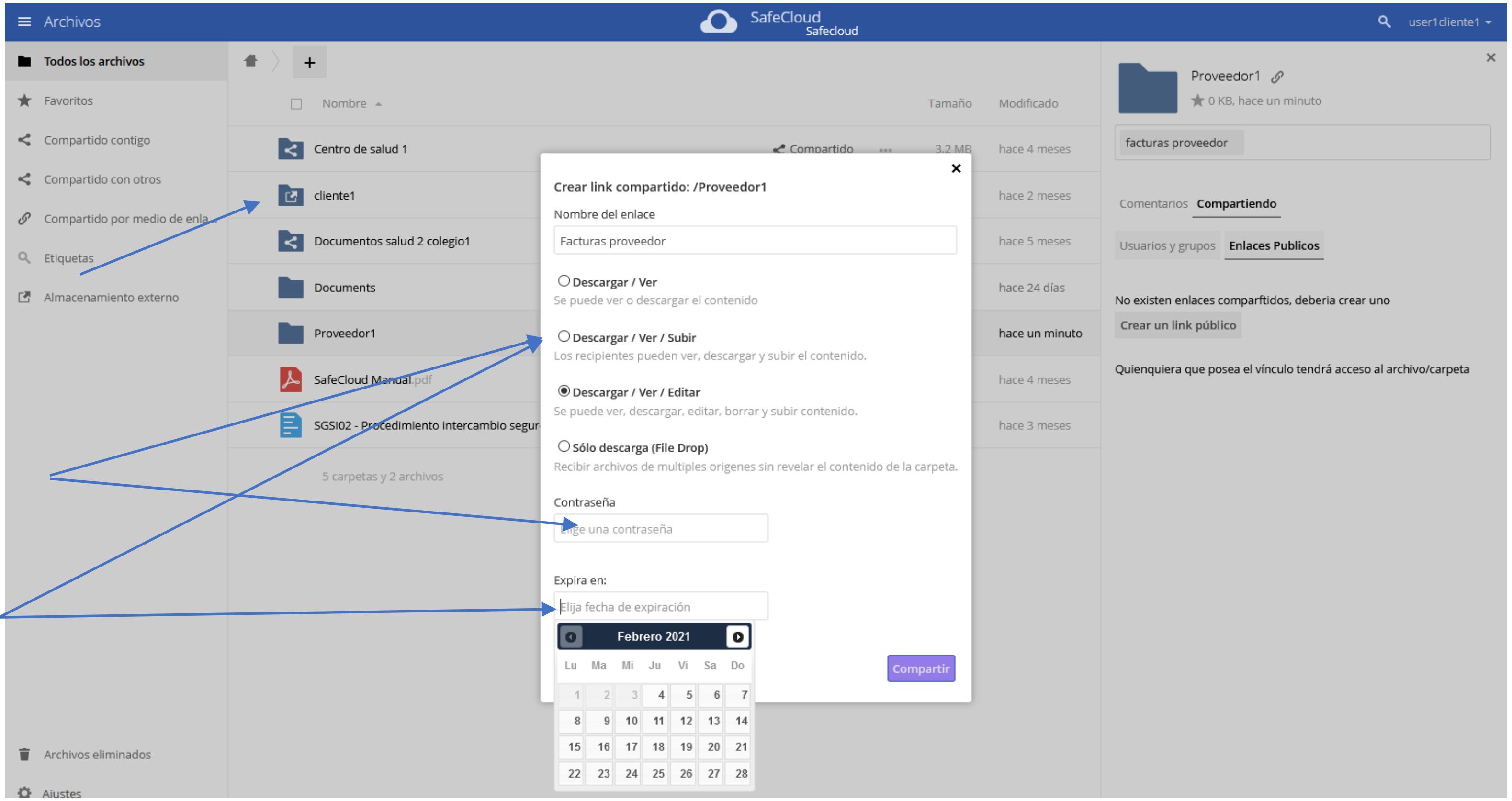
Information Protection

- 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.



Nombre		Tamaño	Modificado
Centro de salud 1	Compartido •••	3.2 MB	hace 4 meses
cliente1			hace 2 meses
Documentos salud 2 colegio1			hace 5 meses
Documents			hace 24 días
Proveedor1			hace un minuto
SafeCloud Manual.pdf			hace 4 meses
SGSI02 - Procedimiento intercambio segur			hace 3 meses

5 carpetas y 2 archivos

Crear link compartido: /Proveedor1

Nombre del enlace: Facturas proveedor

○ **Descargar / Ver**
Se puede ver o descargar el contenido

○ **Descargar / Ver / Subir**
Los recipientes pueden ver, descargar y subir el contenido.

● **Descargar / Ver / Editar**
Se puede ver, descargar, editar, borrar y subir contenido.

○ **Sólo descarga (File Drop)**
Recibir archivos de multiples origenes sin revelar el contenido de la carpeta.

Contraseña: Elige una contraseña

Expira en: Elija fecha de expiración

Febrero 2021

Lu	Ma	Mi	Ju	Vi	Sa	Do
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28

Compartir

Proveedor1
0 KB, hace un minuto
facturas proveedor

Comentarios | **Compartiendo**

Usuarios y grupos | **Enlaces Publicos**

No existen enlaces comparftidos, deberia crear uno

Crear un link público

Quienquiera que posea el vínculo tendrá acceso al archivo/carpeta

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

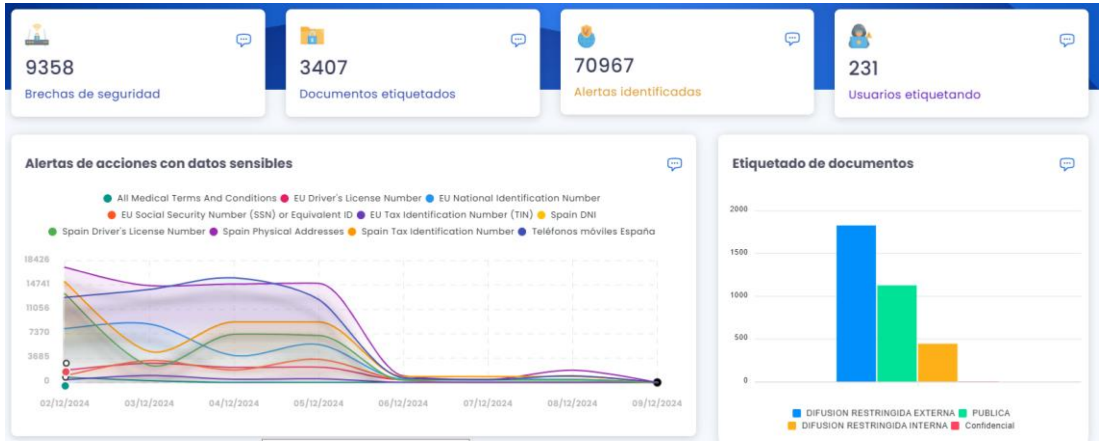
CAU Services

- 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.



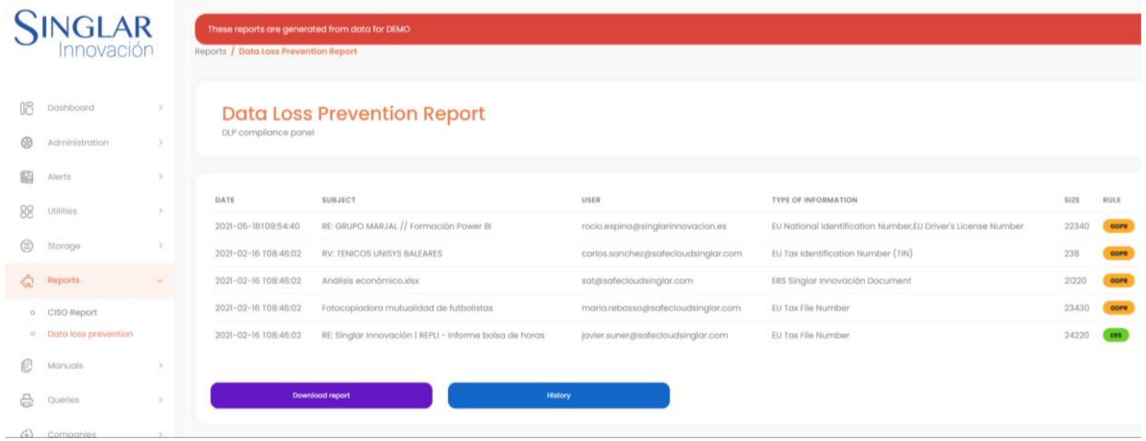
9358 Brechas de seguridad

3407 Documentos etiquetados

70967 Alertas identificadas

231 Usuarios etiquetando

Alertas de acciones con datos sensibles
● All Medical Terms And Conditions ● EU Driver's License Number ● EU National Identification Number
● EU Social Security Number (SSN) or Equivalent ID ● EU Tax Identification Number (TIN) ● Spain DNI
● Spain Driver's License Number ● Spain Physical Addresses ● Spain Tax Identification Number ● Teléfonos móviles España
18426
14741
11056
7370
3685
0
02/12/2024
03/12/2024
04/12/2024
05/12/2024
06/12/2024
07/12/2024
08/12/2024
09/12/2024
Etiquetado de documentos
2000
1500
1000
500
0
DIFUSION RESTRINGIDA EXTERNA
PUBLICA
DIFUSION RESTRINGIDA INTERNA
Confidencial



These reports are generated from data for DEMO

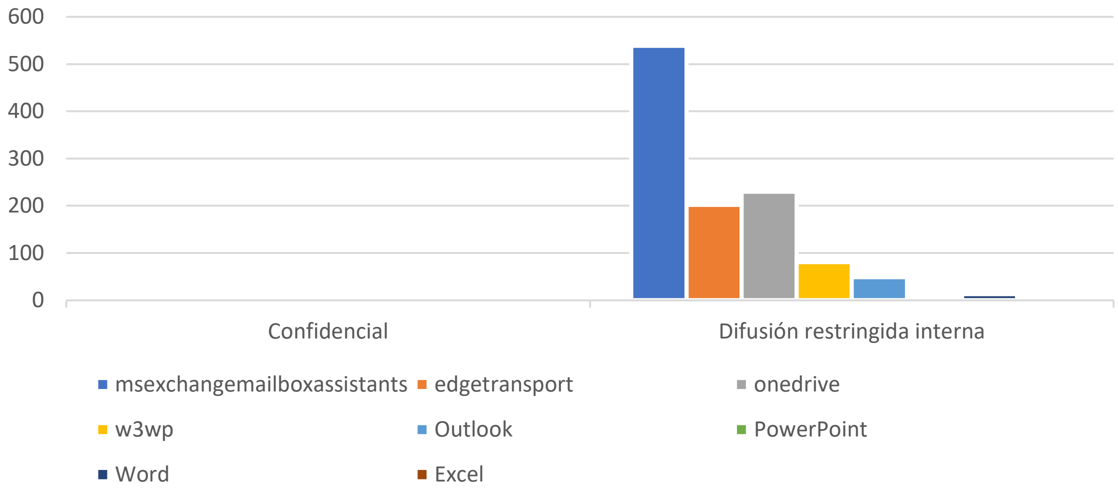
Data Loss Prevention Report

DLP compliance panel

DATE	SUBJECT	USER	TYPE OF INFORMATION	SIZE	RULE
2021-05-18T09:54:40	RE: GRUPO MARJAL // Formación Power BI	rocio.espina@singlarinnovacion.es	EU National Identification Number,EU Driver's License Number	22340	GDPR
2021-02-16 T08:46:02	RV: TENICOS UNISYS BALEARES	carlos.sanchez@safecloudsinglar.com	EU Tax Identification Number (TIN)	238	GDPR
2021-02-16 T08:46:02	Análisis económico.xlsx	sat@safecloudsinglar.com	ERS Singlar Innovación Document	21220	GDPR
2021-02-16 T08:46:02	Fotocopiadora mutualidad de futbolistas	maria.rebassa@safecloudsinglar.com	EU Tax File Number	23430	GDPR
2021-02-16 T08:46:02	RE: Singlar Innovación | REPLI - Informe bolsa de horas	javier.suner@safecloudsinglar.com	EU Tax File Number	24220	ERS

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!

Microsoft