SINGLAR Innovación

SAFECLOUD
PROTECT YOUR COMPANY

Protección de la información

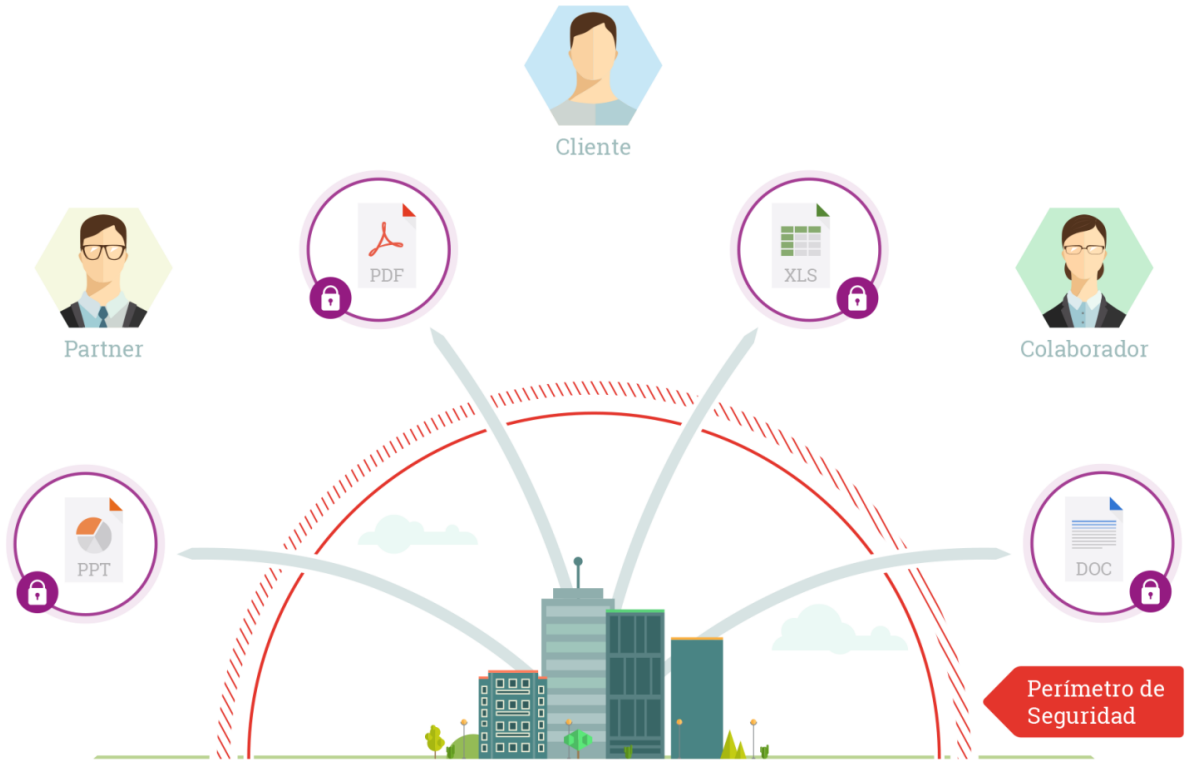
Toma el control y protege el activo más crítico, pasa de la gestión al gobierno

¿Por qué la Protección de la Información?

El usuario final es el principal riesgo para la información de una organización

OBJETIVO: Proteger la información dentro y fuera de la red de la empresa

1. Envío de archivos fuera de la organización
2. Descargar archivos desde correos personales
3. Subir archivos a la nube sin cifrar
4. Dispersión de la información corporativa



Componentes principales

Protección de la información

Gestión de la seguridad:

- Clasificación.
- Reglas de uso y custodia.
- Ciclo de vida del dato.
- Seguimiento mensual de etiquetado y DLP.
- Pericial y defensa jurídica.

Infraestructura:

- Fuentes de información, comunicaciones y repositorios.
- Seguimiento de la información: IRM, DLP, auditoría de accesos.

SafeCloud

CIO y DPO:

- Gobierno de la información.

Operación de la seguridad:

- Atención de alertas, etiquetas y fuga de datos.
- Atención a usuarios (CAU).

Gestión de la Seguridad

Gobierno IT, Compliance, Gestión de Riesgos
y Plan Director de Seguridad

01

Gestión de la Seguridad de la Información: Metodología P&P

Plan de Protección de la Información. Reglas de uso y custodia.

- Etiquetado automático o manual de documentos
- Gestión email según el tipo de información
- Como compartir información con clientes y proveedores de manera segura
- Almacenamiento en local (portátil / móvil)
- Cifrado en almacenamiento / intercambio
- Introducción progresiva de etiquetas por departamentos
- Desarrollo de un marco documental
- Monitorización del uso de la información
- Procedimiento de atención de incidencias

ASEGURAMOS EL ÉXITO
EN LA IMPLANTACIÓN DE
TECNOLOGÍAS IRM Y DLP

Infraestructura de Seguridad

Fuentes de Información, Comunicaciones, Repositorios,
Seguimiento de la información, IRM, DLP o Auditoría de Accesos

02

Soluciones

Protección de la información

Generación de documentos	Etiquetado	Prevención fuga Información (DLP)	Protección de la Información (IRM)	Atención de incidencias
				
CRM, ERP, Local	Manual automático (Plantillas)	Requiere agente	Protección del propio documento	Alertas de comportamiento, alerta exfiltración
Presupuestos, contratos y pedidos	Metadatos, marca de agua y pie de página	Ajuste fino, equipos propios	Máximo control	Atendido por CIO, operador o CyberSOC
Auditar accesos	Etiquetar	Dentro de la organización	Fuera de la organización	SafeCloud PROTECT YOUR COMPANY

Partner / Integrador

Intercambio seguro

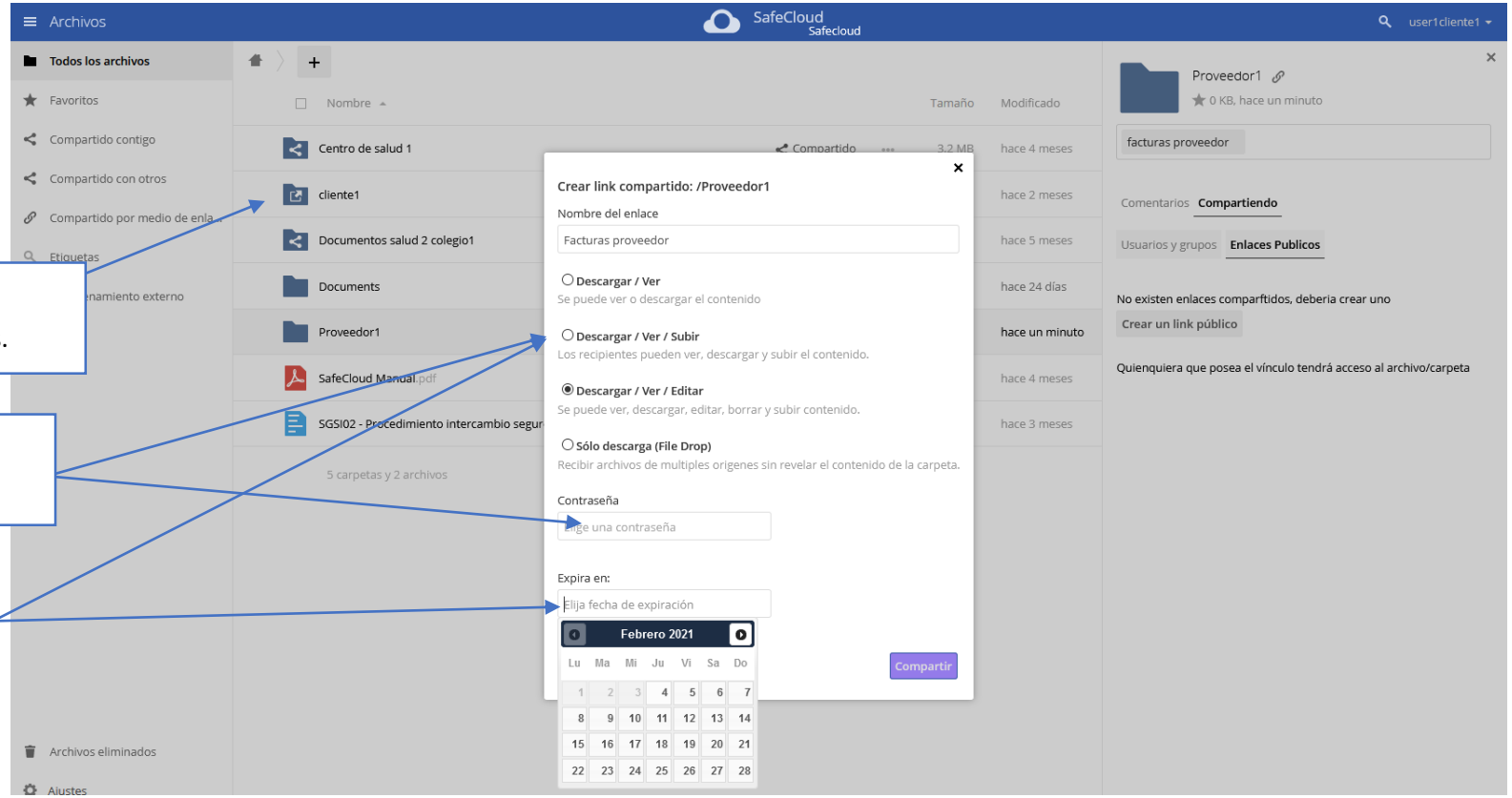
Protección de la Información

- Intercambio de documentos con clientes y proveedores
- Control de la información dentro y fuera de la organización
- Evitar fraudes de phishing y fraude del CEO

Colaborador habitual.
Creo usuarios específicos para acceso a carpetas.

Proveedor habitual.
Compartir directorio con contraseña conocida.

Proveedor esporádico.
Compartir directorio con caducidad 24h.



CIO y DPO

Gobierno de la Información

03

Portal CIO y DPO

SafeCloud PROTECT YOUR COMPANY

Acceso unificado y Procedimientos

CAS

- A Almacenamiento
- A Procedimientos
- A Paneles de gestión
- A Paneles de alertas

Acceso repositorios de intercambio seguro

OneDrive

- Almacenamiento
- Intercambio seguro
- Protección avanzada
- Fácil administración

IRM

- Clasificación y etiquetado de información
- Metodología fácil para despliegue IRM por fases
- Cuadros de seguimiento y gobierno

DLP

- Prevención de fuga de datos
- Reglas preestablecidas de fácil adopción
- Cuadros de seguimiento de datos sensibles (p.e. RGPD)
- Cuadros de seguimiento de fugas de información

Servicios de vCIO y vDPO

- El integrador puede prestar servicios de análisis de los cuadros de mando y mejora continua
- Incorporación progresiva de etiquetas (p.e. por departamento) y de reglas de DLP

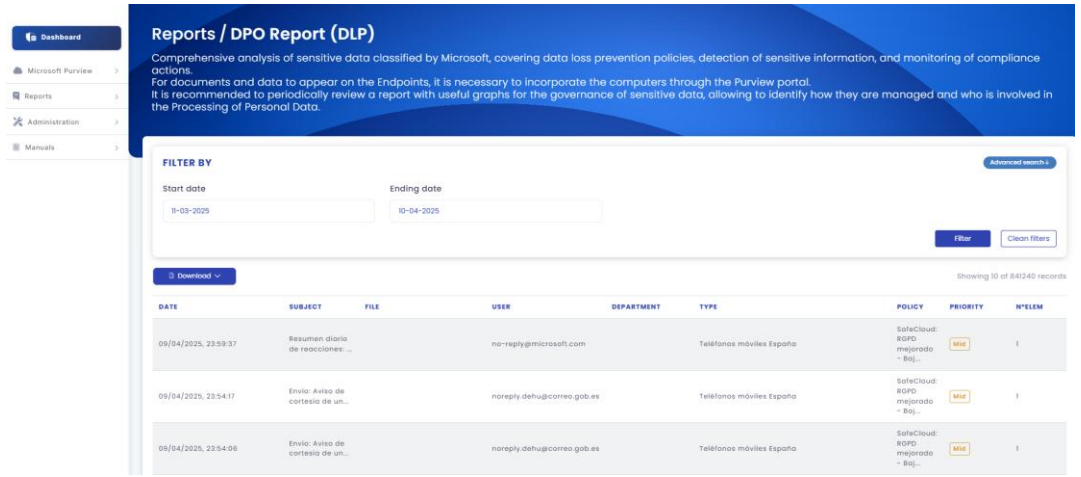
Servicios de CAU

- Servicios de atención a usuarios que clasifican, intercambian y acceden a información

Gestión de la Protección de la Información

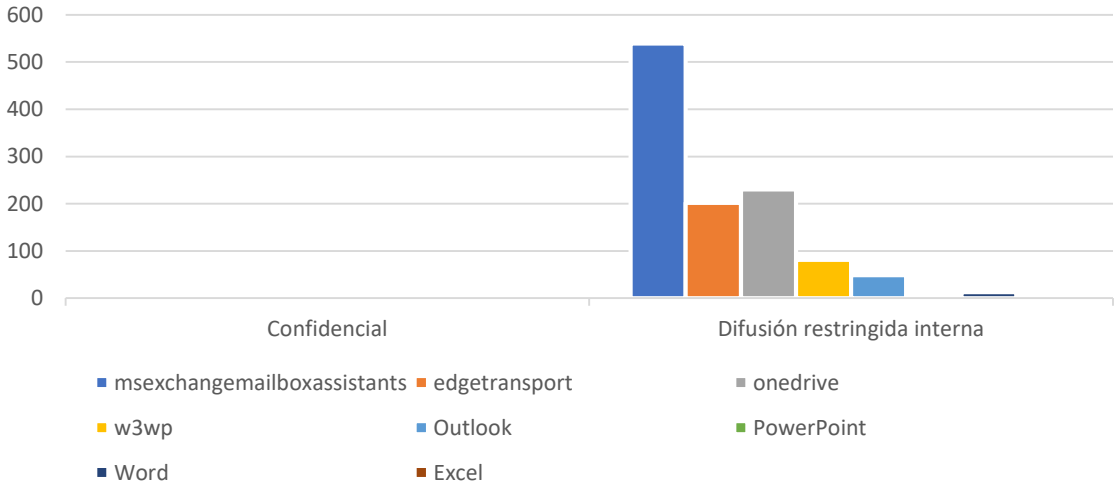
Las tareas que se proponen delegar al CIO o DPO virtual son:

- Administrar centralizadamente paneles de AIP / Auditoría a ficheros / DLP / IRM / Otras soluciones.
- Revisión periódica de informes para el CISO y DPO:
  - Quien etiqueta y clasifica documentos, y como, y su evolución en el tiempo.
  - Quien accede o intentar acceder a la información clasificada.
  - Donde está la información sensible (p.e. RGPD) y por donde se mueve.
  - Exfiltración de datos, quien y como.
  - Trazabilidad de documentos, podemos conocer todo lo que ha pasado con un documento.
- Seguimiento mensual del uso correcto de las etiquetas (basado en hoja de Excel dinámica).
- Revisiones informes de usuarios que comparten datos RGPD con el exterior.



Valor añadido sobre IRM y DLP

- Portal para entender y revisar el depliegue de estas tecnologías en la empresa, su éxito y correcta adopción por los usuarios y terceros
- Informes evolutivos donde poder comprobar como emplean y adoptan los empleados las tecnologías
- Revisión para el DPO que toma el control de toda la información sensible y quien la comparte
- Posibilidad de concienciar a los usuarios que no hacen buen uso de la información, al ritmo que el CIO y/o el DPO puedan



Cuadros de mando SafeCloud

Informes en tiempo real

SafeCloud proporciona informes en tiempo real acerca de:

- Documentos y datos protegidos de la empresa.
- Quién produce documentos, quién los gestiona y a quién se le deniega el acceso.
- Datos sensibles y mapa de calor de los usuarios y aplicaciones que los gestionan.
- Datos filtrados al exterior por tipología de datos sensibles (salud, económica, datos personales…)
- Documentos clasificados y gestionados por empleados y por departamento.
- Acceso a los documentos permitidos, denegados, y desde fuera de la organización.

Difusión restringida externa

SINGLAR
Innovación

SAFECLOUD
PROTECT YOUR COMPANY

¡Gracias!