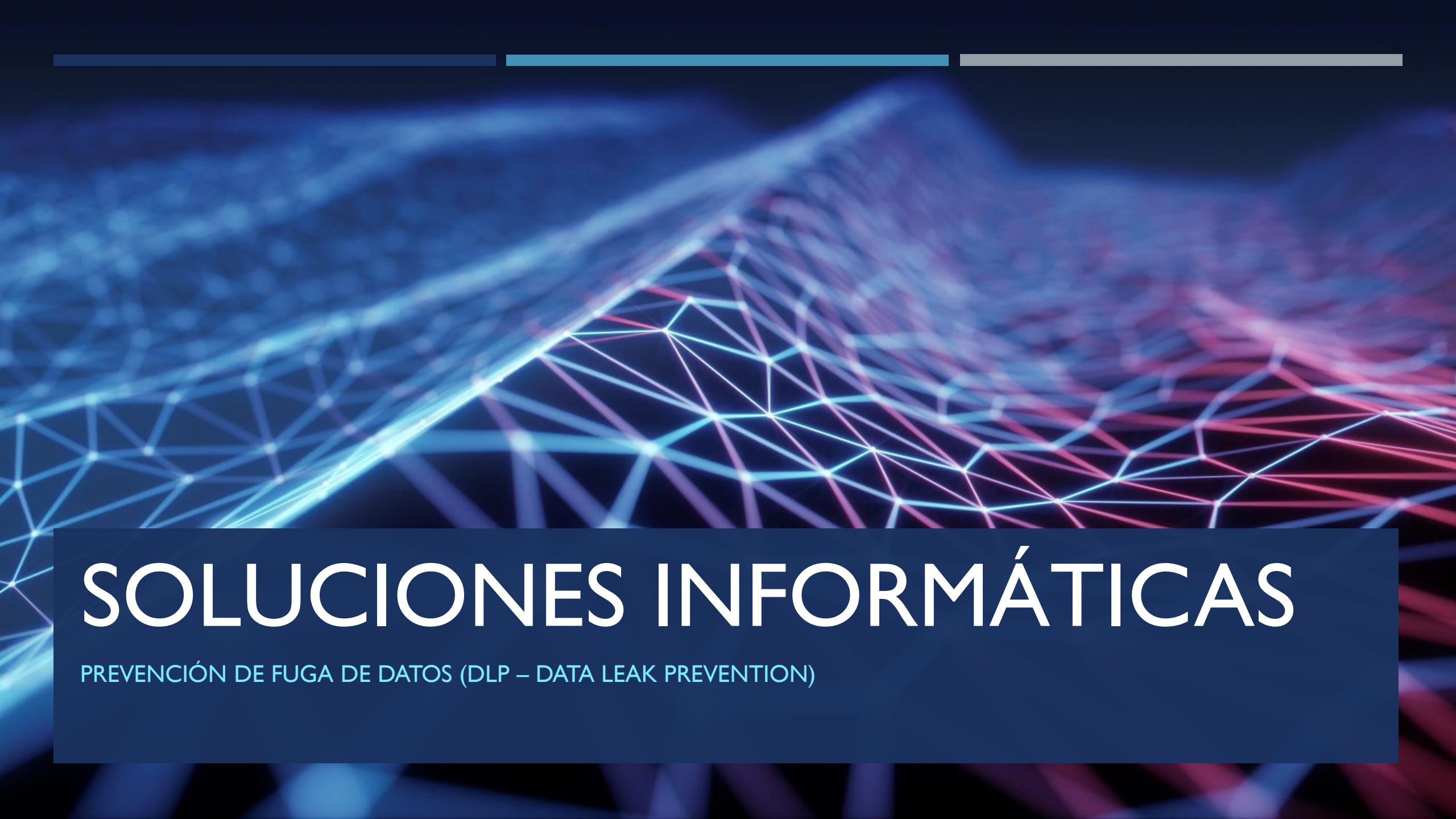
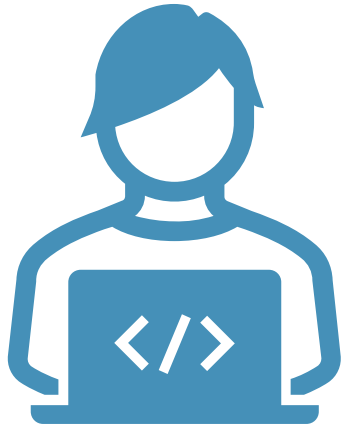


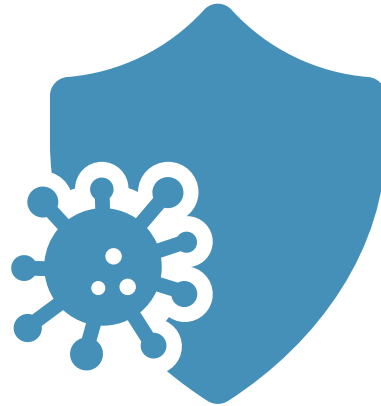


SOLUCIONES INFORMÁTICAS

PREVENCIÓN DE FUGA DE DATOS (DLP – DATA LEAK PREVENTION)



Fuga de información
Personal interno/temporal
Intencionadas o involuntarias



Fuga de información
Cibercrimen



Mejor cumplimiento normativo
Mejoras de calidad

¿POR QUÉ IMPLEMENTARLO?

CASO DE USO I: EMPLEADO EN PRÁCTICAS

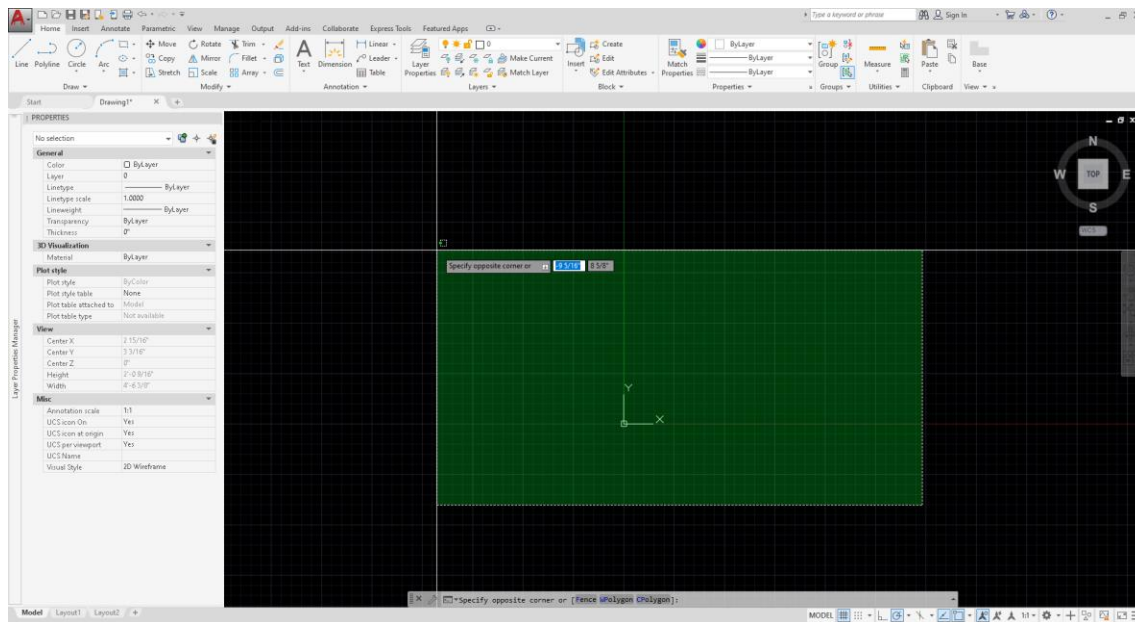


Ante la necesidad de un nuevo empleado, la empresa PAPELOSA, decide contratar a un empleado joven en prácticas

Este empleado va a trabajar con plantillas y procedimientos que a la empresa le ha llevado años desarrollar.

Desde la dirección de PAPELOSA temen que ese conocimiento adquirido salga de la empresa y acabe en la competencia.

CASO DE USO 2: PUENTOSA



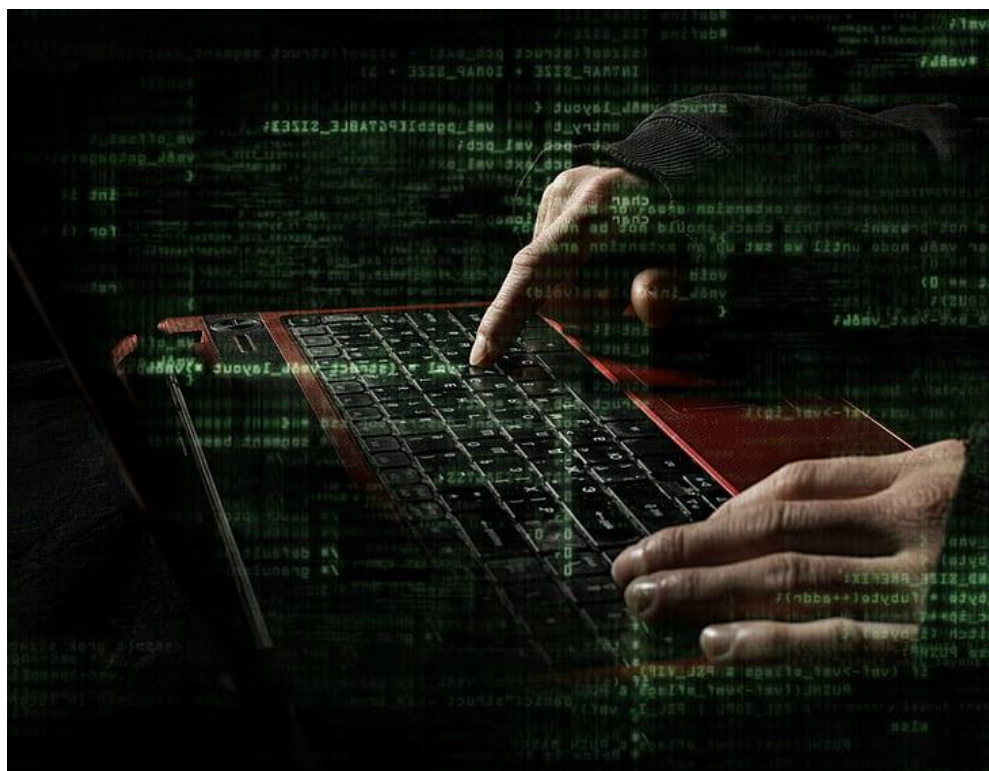
Esta foto de Autor desconocido está bajo licencia [CC BY-NC](#)

Una empresa que se dedica a al diseño de puentes sobre ríos en Asturias, PUENTOSA, participa en un concurso para la construcción de un puente y debe presentar una propuesta.

Contrata a un equipo que trabajará con el conocido programa AUTOCAD para hacer algunos diseños.

Desde la dirección de PUENTOSA temen que esos archivos, que ese trabajo por el que han pagado, y que podría servir también para otros proyectos futuros, salga de la empresa y acabe en la competencia.

CASO DE USO 3: EQUIPO INFECTADO



El hacker “Medianoche” es contratado por un intermediario para hacerse con una base de datos de clientes con problemas de obesidad, posiblemente para mandarles spam con productos adelgazantes.

“Medianoche” consigue saltarse la seguridad de la WiFi de la empresa DIETAFACIL e infectar uno de los equipos.

De manera silenciosa, va a extraer la información requerida sin causar ningún daño, pasará totalmente inadvertido.

Un mes después es detenido por la policía nacional, y se descubre que DIETAFACIL tuvo una filtración de datos, que ni fue detectada, ni reportada ante la Agencia Española de Protección de Datos.

¿CÓMO FUNCIONA?



1

Interceptación: Cuando un usuario envía un archivo, por cualquier medio de comunicación, ese mensaje es interceptado por la solución.

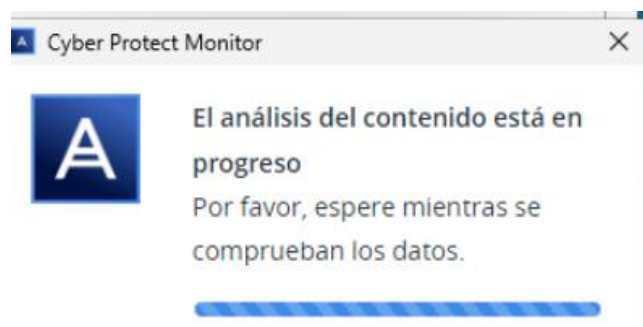
2

Análisis: Según los detectores de contenido que haya establecidos, determinará si el documento es confidencial o si no lo es.

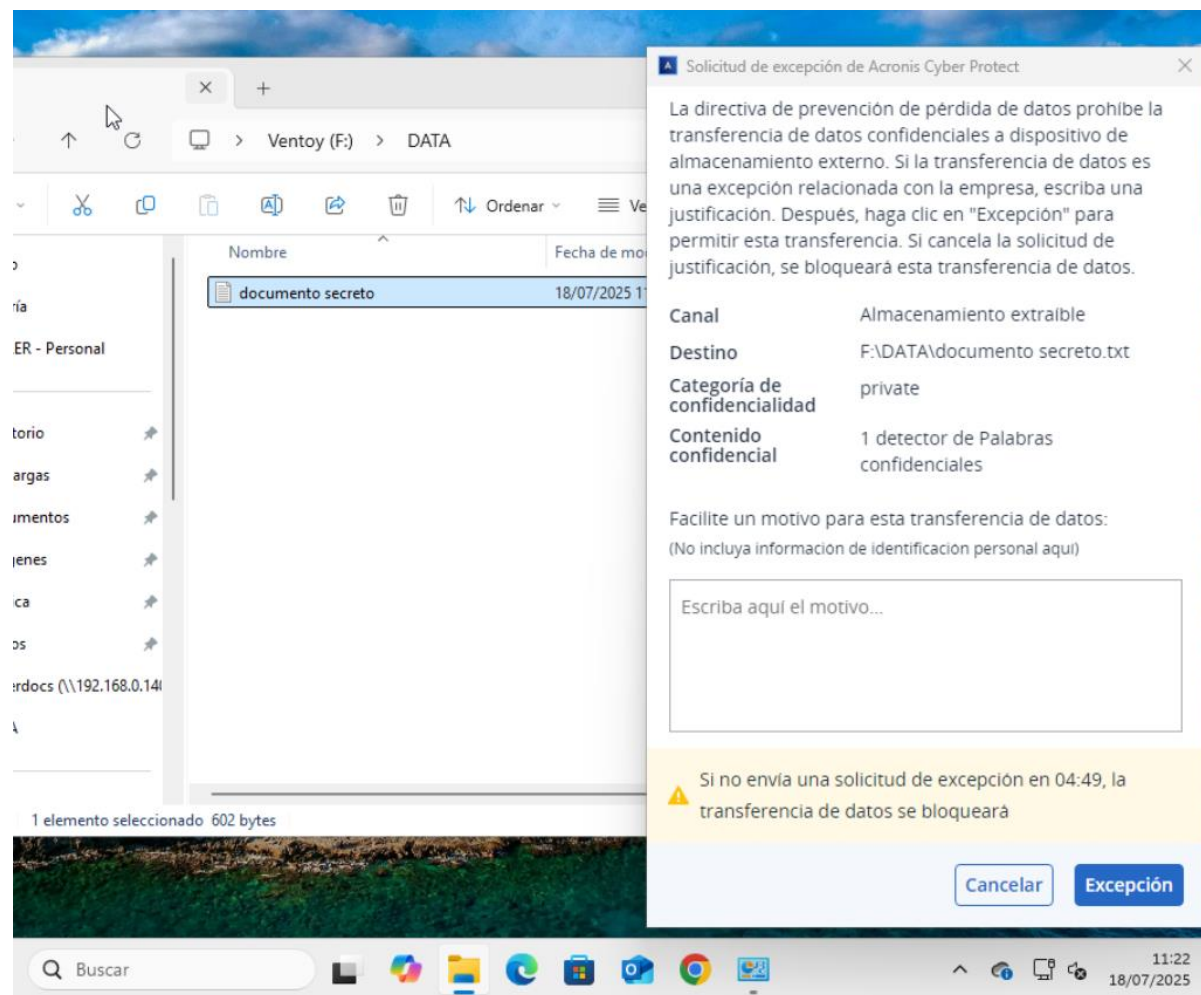
3

Acción: Si el documento es confidencial aplicará la acción que hayamos establecido en la directiva: detenerlo, registrarlo, ...

PODER DISUASORIO



Todo archivo saliente es analizado.



DETECTORES DE CONTENIDO

Para determinar si un documento es confidencial, la solución lo “lee” en busca de coincidencias con los detectores de contenido establecidos.

Ejemplo: Creamos un detector de contenido de tipo extensión de fichero para los .doc y .docx.

Todo .doc o .docx interceptado será identificado como confidencial y se le aplicará una directiva.

Diccionario

- Listas de palabras relacionadas
- Palabras clave

Extensión de fichero

- Identifica por el tipo de documento.
- Pdf, Word, Excel, Autocad, Photoshop...

Patrones

- Longitud, composición, frecuencia...
- Un IBAN siempre se compone del mismo número de dígitos y tiene una estructura, igual que un DNI.

COMBINACIONES COMPLEJAS

EJEMPLO DE UN DETECTOR DE DICCIONARIO

Nombre

detector de Palabras confidenciales

Descripción (opcional)

Confidencialidad (opcional)

private

Condición

Coinciden cualesquiera [number] palabras clave

Numero de palabra clave que debe coincidir

1

☐

Contar coincidencias idénticas como una sola coinciden...

Introduzca la palabra clave...

Agregar

Importar ⓘ

Keyword	Case sensitive	
confidencial	☐	

DIRECTIVAS

En las directivas establecemos “lo que se hace” cuando se intercepta un archivo confidencial.

También se usan para hilar más fino sobre como restringir ese trafico.

Ejemplo: podemos crear una directiva que bloquee la salida desde cualquier origen a cualquier destino para los documentos confidenciales contables.

Creamos otra que permita enviarlos a admon@miempresa.com

 **Rechazar**

 **Permitir**

 **Justificar**



REGISTRO DE ACTIVIDAD

Se le puede indicar a la directiva que registre la operación, dando lugar a un listado con todos los flujos salientes de información confidencial de la organización.

Ese listado está dotado de potentes filtros para realizar búsquedas.

DLP events

 Filter

Status	Date	Workload	User	Sensitivity	Destination	Channel	Reason
 Allowed	Apr 02 12:05:54	qa-gw3t68hh	DL\nick	PCI DSS	Jane Cooper 	Webmail (Gmail)	—
 Denied	Apr 15 11:26:35	MF_2012_R2	DL\nick	PCI DSS	Esther Howard 	SMTP	Reason ...
 Denied	Apr 17 19:02:04	accountant-pc12	DL\nick	PII, PHI	Brook Simmons 	Webmail (Yahoo)	Reason ...
 Justified	May 04 05:47:29	accountant-pc11	DL\nick	PII, PHI	Leslie Alexander 	Webmail (Gmail)	Reason ...
 Allowed	May 10 09:30:03	accountant-pc10	DL\nick	PII, PHI	Leslie Alexander 	Webmail (Gmail)	—
 Denied	May 11 12:17:34	dc_w2k12_r2	DL\nick	PII, PHI	Jane Cooper, Wade Warren 	Webmail (Gmail)	Reason ...
 Justified	May 18 12:05:54	dc_w2k12_r1	DL\john.p	PCI DSS	Guy Hawkings	Webmail (Gmail)	Reason ...
 Allowed	May 19 12:05:54	MF_2012_R2	DL\ydia.cr	Confidential	<u>\\fileserver\share\file.doc</u>	SMB	—
 Allowed	May 20 12:05:54	vm-sql_2012	DL\nick	PHI, PII, PCI DSS, Confidential	file.doc	File sharing (OneDrive)	—
 Justified	May 25 16:41:12	qa-gw3t68hh	DL\nick	PHI, PII, PCI DSS	https://server/path/file.doc	HTTP	Reason ...
 Justified	Jun 07 13:11:26	qa-gw3t68hh	DL\nick	PHI, PII, PCI DSS	\\fileserver\share\file.doc	SMB	Reason ...
 Justified	Jun 09 13:23:22	qa-gw3t68hh	DL\nick	PHI, PII, PCI DSS, Confidential	file.doc	File sharing (Dropbox)	Reason ...

COMPONENTES CLAVE PARA UNA CORRECTA IMPLEMENTACIÓN

Autoprotección

- El usuario no debe poder detener la solución.
- El usuario no debe poder desinstalar la solución.

Control de dispositivos

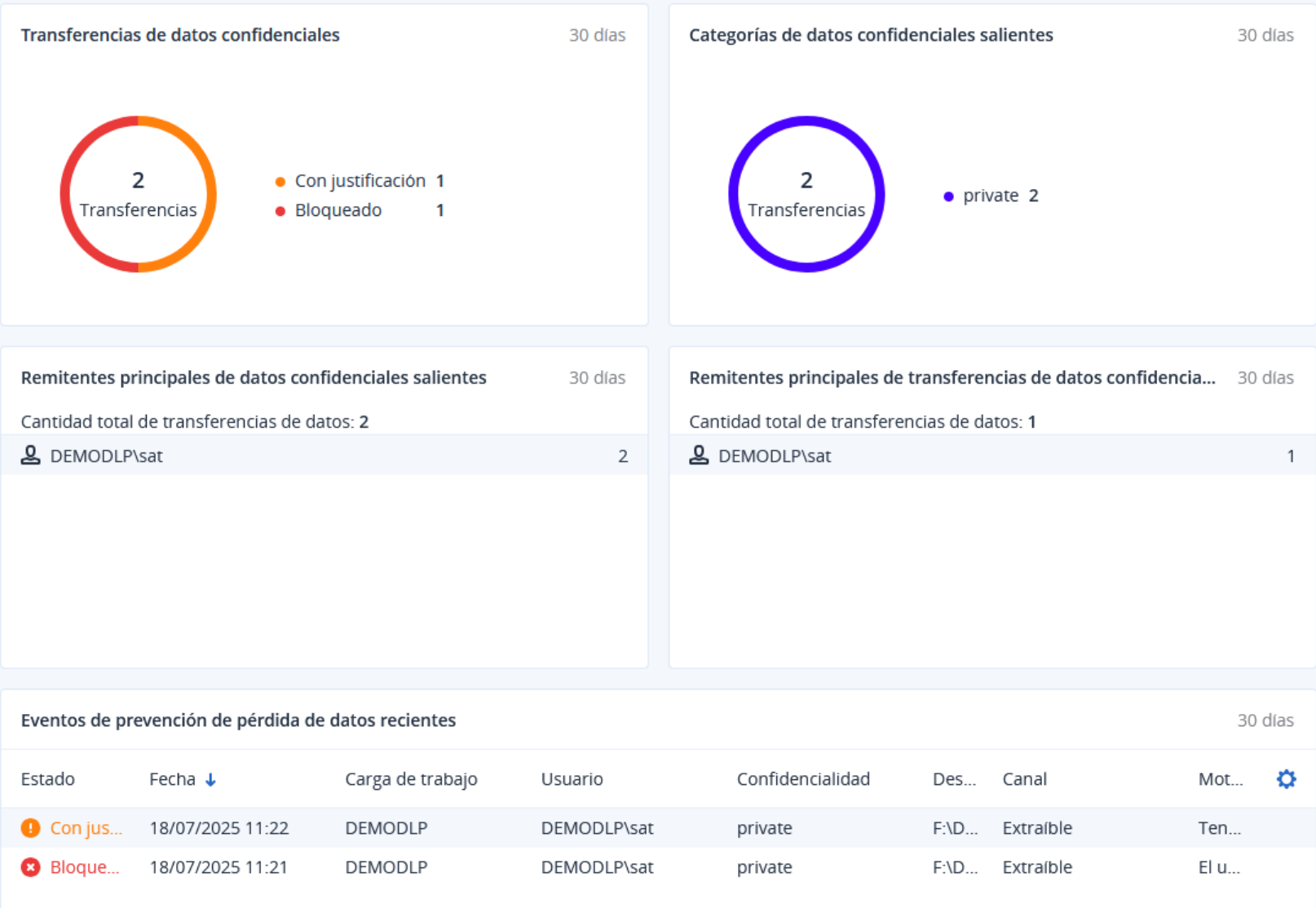
- De manera complementaria se deben bloquear los dispositivos “no necesarios” para el usuario.
- Algunos como la impresión no es práctico desactivarlos.

Solución de prevención de fuga de datos.

- Requiere reuniones previas para determinar los detectores de contenido iniciales.
- La colección de detectores se va mejorando con el tiempo, lo que va haciendo la solución cada vez mas eficaz. Reuniones periódicas.

FUNCIONES AVANZADAS

- OCR en 20 Idiomas.
- Modo aprendizaje y modo estricto.
- Bloquea comprimidos con contraseña.
- Bloquea en caso de error.
- Informes





GRACIAS

ARCO@ARCOOFIMATICA.COM

+34 985 258 151