proofpoint.

RESUMEN DE LA SOLUCIÓN

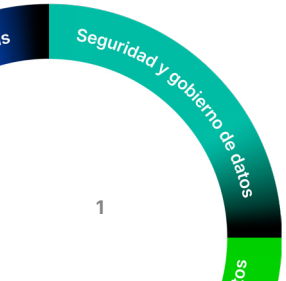
# Modernizar la seguridad de los datos del correo electrónico con un enfoque adaptable

Incorpore Proofpoint Adaptive Email DLP para disfrutar de una protección multicapa contra la pérdida de datos por correo electrónico

## Ventajas principales

- Prevenga la pérdida de datos accidental o intencionada a través del correo electrónico.
- Mitigue los riesgos de daños reputacionales y la pérdida de clientes.
- Reduzca las multas por infracciones del Reglamento General de Protección de Datos (RGPD) y la Ley de Privacidad del Consumidor de California (California Consumer Privacy Act, CCPA).
- Mejore la concienciación en seguridad en toda la organización.

Este conjunto de soluciones forma parte de la plataforma Human-Centric Security, que mitiga las cuatro principales áreas de riesgo asociado a las personas.




Las pérdidas de datos sensibles pueden ser especialmente perjudiciales y dañinas para su empresa. Según el informe *Data Loss Landscape* en 2024 de Proofpoint, el 85 % de las empresas entrevistadas admitieron haber sufrido al menos un incidente de pérdida de datos. Para el 50 % de ellos, el incidente provocó trastornos en su negocio. Los usuarios negligentes fueron la causa más común de las pérdidas de datos.

La prevención de la pérdida de datos (DLP) por correo electrónico es un componente esencial de la estrategia global de seguridad de datos de su organización. Protege los datos confidenciales de una exposición no deseada por correo electrónico. Un programa eficaz de DLP por correo electrónico combina el análisis de contenidos, las alertas en tiempo real, la aplicación de políticas y la formación de los usuarios. Previene la pérdida de datos y garantiza el cumplimiento de los requisitos legales y normativos.

Las soluciones tradicionales de DLP por correo electrónico pueden crear una base sólida aplicando reglas y políticas definidas a riesgos conocidos. Sin embargo, puede mejorar en gran medida su estrategia de protección de datos de correo electrónico si confía tanto en un producto de DLP de correo electrónico tradicional como en Proofpoint Adaptive Email DLP. Esta solución combinada ofrece un enfoque más dinámico y centrado en las personas para evitar la pérdida de datos por correo electrónico.

Estas son las ventajas de incorporar Proofpoint Adaptive Email DLP a su solución:

## Protección más completa

- **Las soluciones tradicionales de DLP por correo electrónico** se centran en el contenido. Proporcionan protección basada en reglas contra riesgos conocidos, como el envío de datos confidenciales por correo electrónico. Son especialmente eficaces para proteger datos, estructurados conocidos y bien definidos, incluidos datos de información personal identificable (identificación personal, números de tarjetas de crédito), etc.
- **Proofpoint Adaptive Email DLP** se centra en el contexto. Amplía la cobertura proporcionada por las soluciones DLP por correo electrónico tradicionales, por lo que también estará protegido frente a amenazas desconocidas y en constante evolución. Proofpoint Adaptive Email DLP utiliza IA basada en el comportamiento para detectar comportamientos inusuales de los usuarios. Esto podría implicar que un usuario envíe datos confidenciales al destinatario equivocado o un correo electrónico a una cuenta no autorizada, o que comparta archivos de forma inusual.

## Detección adaptable

Proofpoint Adaptive Email DLP utiliza IA basada en el comportamiento para detectar actividad de correo electrónico que difiere del comportamiento normal del usuario. Nuestra IA no se limita a buscar modelos de datos específicos.

# 1/3 usuarios

envió uno o varios mensajes al destinatario equivocado.

Fuente: Informe Data Loss Landscape 2024 de Proofpoint

# 84 %

de los correos electrónicos enviados al destinatario equivocado el año pasado contenían archivos adjuntos.

Fuente: Informe Data Loss Landscape 2024 de Proofpoint

# 50 %

de las fugas debidas a un error en 2023 fueron el resultado de correos electrónicos enviados a un destinatario equivocado.

Fuente: Verizon *2024 Data Breach Investigations* Report (Informe sobre las investigaciones de fugas de datos 2024)

# 160 000

Proofpoint Adaptive Email DLP evitó que más de 160 000 mensajes de correo electrónico se enviaran al destinatario equivocado en 2024.

Fuente: Proofpoint

Analiza un contexto más amplio, que incluye :

- Las personas a las que los usuarios están acostumbrados a enviar mensajes de correo electrónico.
- Los tipos de archivos adjuntos que suelen compartir los usuarios.
- La forma en que los usuarios están acostumbrados a gestionar los datos sensibles.

Proofpoint Adaptive Email DLP se adapta al comportamiento de sus empleados y a las tendencias del correo electrónico. Permite detectar posibles pérdidas de datos, incluso cuando no están claramente definidos. Imaginemos, por ejemplo, que un empleado que no está acostumbrado a enviar datos financieros de repente intenta enviar un archivo adjunto que contiene dicha información a un contacto externo no autorizado. Proofpoint Adaptive Email DLP detectará la cuenta de correo electrónico no autorizada y el archivo adjunto sensible, y lo señalará.

## Impida el envío de mensajes de correo electrónico al destinatario equivocado

Esta situación se produce cuando un usuario envía de manera accidental un mensaje a la persona equivocada. Los mensajes de correo electrónico enviados a un destinatario equivocado son una fuente habitual de riesgo para los datos. Según datos de Proofpoint, el 33% de los empleados envía uno o dos correos electrónicos a la persona equivocada cada año. También es el incidente de pérdida de datos más denunciado ante la ICO (Information Commissioner's Office) en el Reino Unido[1]. Además, Verizon descubrió que el 50 % de las fugas provocadas por errores en 2023 fueron el resultado de correos electrónicos enviados a un destinatario equivocado[2].

Enviar mensajes de correo electrónico a la persona equivocada es un problema difícil de resolver con los productos tradicionales de DLP por correo electrónico. En cambio, Proofpoint Adaptive Email DLP utiliza la inspección profunda de contenido y el análisis de comportamiento de Proofpoint Nexus® Relationship Graph (RG) para identificar los mensajes de correo electrónico enviados al destinatario incorrecto antes de que lleguen a enviarse. Cuando un usuario intenta enviar un correo electrónico a la persona equivocada, Proofpoint Adaptive Email DLP detecta el error y genera una advertencia. Según datos de Proofpoint, Proofpoint Adaptive Email DLP evitó que más de 160 000 mensajes de correo electrónico se enviaran al destinatario equivocado en 2024.

## Evite que se adjunten archivos incorrectos

Esta situación se produce cuando se envía un mensaje de correo electrónico a la persona correcta, pero al que se adjunta un archivo equivocado. Cuando la IA basada en el comportamiento detecta un archivo adjunto que parece inusual para un destinatario, advierte al usuario en tiempo real. El usuario puede corregir el problema antes de que se produzca el incidente.

1. ICO (Information Commissioner's Office), "Common data protection mistakes (and how to fix them)" (Errores comunes en la protección de datos y cómo corregirlos), febrero de 2025.
2. Verizon. *2024 Data Breach Investigations Report* (Informe sobre investigaciones de fugas de datos de 2023), 2024.

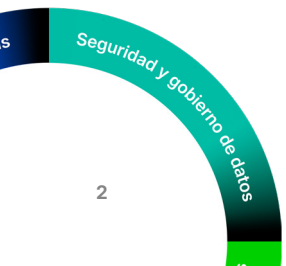



**Figura 1.** El panel de Proofpoint Adaptive Email DLP proporciona a los equipos de seguridad de la información una visibilidad completa y una mayor confianza en la prevención de la pérdida de datos.

# 1 100 000

Proofpoint Adaptive Email DLP detectó más de 1 100 000 mensajes de correo electrónico que filtraban datos en 2024.

Fuente: Proofpoint

## Bloquee las costosas filtraciones por correo electrónico

La filtración de datos confidenciales por correo electrónico es costosa de subsanar para las organizaciones. Según el Ponemon Institute, un equipo de seguridad necesita entre 48 y 72 horas para identificar y corregir un incidente de filtración de datos[3]. Proofpoint Adaptive Email DLP alivia esta creciente carga para su equipo. Analiza y clasifica automáticamente sus datos sensibles, e identifica cuentas de correo electrónico personales o no autorizadas pertenecientes a sus usuarios. Si un usuario intenta enviar datos confidenciales a sí mismo o a otros, Proofpoint Adaptive Email DLP bloquea o rastrea sus acciones, en función de su configuración. Según datos de Proofpoint, Proofpoint Adaptive Email DLP detectó más de 1 100 000 mensajes de correo electrónico que filtraban datos en 2024.

3. Ponemon Institute. "Email Data Loss Prevention: The Rising Need for Behavioral Intelligence" (Prevención de la pérdida de datos por correo electrónico: la creciente necesidad de inteligencia de amenazas basada en el comportamiento), mayo de 2022.


**Figura 2.** Proofpoint Adaptive Email DLP advierte a los usuarios en tiempo real sobre los mensajes de correo electrónico enviados a cuentas no autorizadas y los mensajes dirigidos a los destinatarios equivocados.

## Formación de usuarios en tiempo real

La formación de los usuarios en tiempo real ayuda a evitar errores e incumplimientos de las políticas. Además de la formación de concienciación sobre ciberseguridad, Proofpoint Adaptive Email DLP forma a los usuarios en los riesgos asociados al correo electrónico en tiempo real. Así, los usuarios pueden corregir sus propios errores sin ayuda de un administrador.

## La unión hace la fuerza

Las repercusiones de perder datos sensibles pueden ser extremadamente graves. Estos incidentes pueden costar a su empresa multas normativas, daños a su reputación y pérdidas de negocio. También pueden aumentar sus costes de mano de obra debido a las investigaciones y los informes reglamentarios y de cumplimiento.

Al integrar tanto un producto de DLP de correo electrónico tradicional como Proofpoint Adaptive Email DLP, su organización puede implementar un enfoque moderno multicapa para la seguridad de los datos de correo electrónico. Esta solución combina una sólida protección contra los riesgos conocidos con la detección inteligente y dinámica de amenazas de pérdida de datos desconocidas centradas en las personas. Como resultado, disfrutará de una mayor protección de los datos, un mejor cumplimiento por parte de los usuarios, una reducción de los costes operativos y un mayor nivel de seguridad general de los datos de correo electrónico.

proofpoint.

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Organizaciones líderes de todos los tamaños, entre las que se encuentran el 85 % de las empresas Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en las personas y su cumplimiento normativo, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en www.proofpoint.com/es.

Conecte con Proofpoint: LinkedIn



**DESCUBRA LA PLATAFORMA DE PROOFPOINT →**