# Navega de forma segura por la adopción de la IA con Symantec DLP

**Con la IA en la vía rápida, los desafíos de la gobernanza de datos se aceleran cada vez más.**

**La prevención de pérdida de datos (Data Loss Prevention, DLP) de Symantec puede ayudarte a manejar el cumplimiento y turboalimentar tus controles de protección de datos.**

## AI pública

El ChatGPT, por ejemplo, puede contener datos de cualquier persona

**¿Cómo puedo utilizar la IA de forma segura?**

**¿Qué aplicaciones de IA se están utilizando?**

**¿Es arriesgado usarlas?**

Symantec DLP analiza los riesgos de las aplicaciones de IA generativa a través del análisis de más de 300 atributos

**¿Quién está usando qué?**

Symantec DLP supervisa el uso de las aplicaciones de IA generativa en tiempo real, mostrando atributos como el usuario, la ubicación, la información del dispositivo y los datos compartidos.

**¿Qué datos están entrando (a través de los prompts) en los sistemas de IA?**

## IA empresarial

El Copilot para Office 365, por ejemplo, es un modelo de IA disponible públicamente que solo funciona con tus datos internos

**¿La IA necesita disponer de todos mis datos?**

**¿Qué datos internos deben excluirse de los análisis de IA?**

**¿Cómo encuentro y marco los datos de naturaleza confidencial (incluidos los archivados) para que la IA empresarial no acceda a ellos?**

Symantec DLP identifica los archivos que contienen datos de naturaleza confidencial e indica cómo clasificarlos para que la IA empresarial sepa a cuáles puede acceder y a cuáles no.

**¿Cómo hago que el proceso sea repetible y fácil de manejar para proteger los datos futuros de la misma manera?**

Mediante políticas precisas y unificadas, Symantec DLP garantiza que aplicas la misma protección a los datos de mañana que a los de hoy.

**¿Qué datos de mis sistemas están entrando (a través de los prompts) en la IA de acceso público?**

## Contenido generado por IA

**¿Cómo protejo lo que la IA crea?**

**¿Cómo escaneo y protejo los nuevos contenidos de IA? Necesito encontrar los datos de naturaleza confidencial inactivos o en uso.**

El usuario no siempre puede clasificar el contenido generado por IA. Symantec DLP automatiza de manera fiable las decisiones sobre clasificación de datos.

Arrow | Symantec by Broadcom | Carbon Black. by Broadcom

# COPILOT
## CON SYMANTEC DLP



## PROTEJA SUS DATOS CON SYMANTEC DLP ANTES DE HABILITAR COPILOT

Al igual que muchas herramientas de IA generativa, **Microsoft Copilot** abre la puerta a la productividad, pero también entraña ciertos riesgos. Está Integrado en toda la plataforma Microsoft 365 y puede acceder potencialmente a cualquier documento, presentación, correo electrónico, hoja de cálculo y más. Esto incluye sus datos más valiosos y confidenciales. **Para utilizar Copilot de forma segura y productiva,** necesita establecer sus límites desde el principio (con una gobernanza de datos adecuada).

### DESAFÍOS Y RIESGOS

**Las áreas clave que debe resolver antes de implementar Copilot.**

### ¿CÓMO VA A CREAR SU SISTEMA DLP?

Si ya está utilizando Symantec DLP: **buenas noticias**, es fácil ampliarlo para proporcionar gobernanza de datos para Copilot.

Si necesita construir su sistema desde cero, elija una **solución líder del mercado** que cubra todas las posibilidades. Symantec DLP es conocido por su detección precisa, integración completa con MSFT e implementación a escala, y puede ayudarle a encontrar, clasificar y etiquetar datos confidenciales con rapidez.

## 1. IDENTIFICACIÓN DE DATOS CONFIDENCIALES

Para proteger sus datos confidenciales, primero tiene que encontrarlos, inspeccionarlos en busca de contenido confidencial y etiquetarlos correctamente. La dificultad inherente es que necesita una estrategia sistemática y precisa. Una estrategia que funcione también con datos que no se hayan tocado desde hace tiempo, que refleje sus últimas políticas de seguridad y que sea repetible (porque, ¿de qué otra manera protegerá los nuevos datos que se generen?).

**Symantec DLP hace todo esto, y se integra con Microsoft Purview para garantizar que Copilot sepa con qué puede interactuar y qué no debe tocar.**

| | |
|---|---|
| **RIESGO** | **Si Copilot se confunde no reconocerá sus documentos confidenciales, con el consiguiente riesgo de fuga de datos.** |

## 2. ETIQUETADO DE NUEVOS CONTENIDOS

El contenido generado por Copilot **no hereda automáticamente las etiquetas de seguridad de sus archivos de origen.** Esto deja a los empleados la tarea de determinar si el nuevo contenido debe clasificarse como confidencial.

| | |
|---|---|
| **RIESGO** | **Los empleados podrán ver y compartir información confidencial de documentos mal etiquetados.** |

## 3. PERMISOS EXCESIVOS

**Copilot adopta los mismos derechos de acceso que sus usuarios**, pero los empleados a veces tienen más permisos de los que se supone que deberían tener. Esto permite a Copilot acceder a contenido confidencial y compartirlo con usuarios no autorizados.

| | |
|---|---|
| **RIESGO** | **El "exceso de autorización" aumenta el riesgo de acceso y exposición no autorizados a los datos.** |

## 4. INTEGRACIÓN CON MICROSOFT 365

Todo lo anterior se complica debido a la profunda integración de Copilot con la familia Microsoft 365. Ello añade **complejidad a la gobernanza de datos**, lo que dificulta mantener la visibilidad y limitar los niveles de acceso cuando los privilegios son mínimos.

| | |
|---|---|
| **RIESGO** | **Cuanto mayor es el alcance y la complejidad, mayor es el riesgo de exposición de los datos.** |

## SYMANTEC DLP – LA MEJOR FORMA DE HABILITAR COPILOT

**Symantec DLP** ofrece ventajas únicas a las organizaciones que implementan Copilot. La integración perfecta con Microsoft 365 facilita la aplicación de una gobernanza de datos homogénea en todo el ecosistema, protegiendo sus datos en todo lugar.

### LA SOLUCIÓN AUTOMATIZADA

**Inspecciona el contenido** para detectar datos confidenciales, incluidos archivos no etiquetados o clasificados erróneamente

**Corrige los datos clasificados erróneamente,** aplicando las etiquetas correctas basadas en las políticas de DLP

**Inspecciona, categoriza y etiqueta** todos los nuevos contenidos generados por Copilot

**Clasifica los archivos** y utiliza la tecnología de Microsoft para aplicar la etiqueta de confidencialidad, lo que garantiza que Copilot reconozca los datos confidenciales

**Aplica sus políticas DLP existentes** en todo Microsoft 365 para garantizar la uniformidad (incluidos los contenidos archivados y aún por generar)

## PROTECCIÓN DE DATOS SENCILLA Y UNIFICADA

El uso seguro de Copilot requiere una sólida gobernanza de los datos. Con Symantec DLP no tiene por qué ser complejo.

**Para ver cómo funciona en la práctica, contáctenos hoy mismo.**