Servicio especializado de revisión de madurez

AI-Ready Data Security Assessment

Evaluación estratégica de protección de datos en la era de la inteligencia artificial

Microsoft Purview

2026

Contexto Estratégico

El nuevo riesgo: la intersección entre datos e IA

Adopción de IA empresarial

72%

de las organizaciones ya utilizan herramientas de IA generativa en operaciones diarias

Datos expuestos

+340%

incremento en exposición de información sensible vía colaboración digital

Vectores de riesgo emergentes

- **Copilot & Agentes IA**
  Acceso amplificado a datos sensibles a través de permisos heredados
- **Shadow AI**
  Uso no autorizado de herramientas externas sin visibilidad ni control
- **Oversharing**
  Datos sensibles sobreexpuestos en repositorios colaborativos

> La IA no crea nuevos datos sensibles, pero expone los que ya existen de formas que los controles tradicionales no anticiparon.

Análisis de Brechas

Por qué los modelos de seguridad tradicionales no son suficientes

Limitaciones críticas

Permisos heredados

Los controles tradicionales no evalúan el riesgo de acceso amplificado por IA

Ceguera ante Shadow AI

Sin visibilidad sobre qué datos se comparten en prompts de herramientas externas

DLP insuficiente

Las políticas actuales no protegen datos en contextos de IA generativa

El paradigma ha cambiado

Antes	Ahora
Proteger datos en reposo y tránsito	Proteger datos en uso por IA y agentes

Shadow AI
Sin visibilidad

Oversharing
Datos expuestos

Copilot Risk
Acceso amplificado

Insight ejecutivo: Las organizaciones necesitan un modelo de seguridad que evolucione de "proteger el perímetro" a "proteger los datos en cualquier contexto de uso, incluyendo IA."

Metodología

Framework de Evaluación

Cinco fases para asegurar datos en la era de la IA

01 Discover

Inventario completo de datos sensibles, ubicaciones y flujos de información

Data landscape mapping

02 Classify

Categorización de información según sensibilidad, regulación y criticidad

Sensitivity labeling

03 Protect

Implementación de controles DLP, encriptación y políticas de acceso

Policy enforcement

04 Govern

Gobierno de datos, gestión de ciclo de vida y cumplimiento regulatorio

Compliance framework

05 AI Secure

Evaluación específica de riesgos de IA, Copilot readiness y controles para prompts

AI-specific controls

Cobertura integral
Todos los vectores de riesgo

Enfoque ejecutivo
Riesgo de negocio primero

Actionable insights
Roadmap priorizado

Servicio

Alcance del Assessment

Evaluación integral de seguridad de datos y exposición a IA

Microsoft Purview

- DLP policies coverage & effectiveness
- Sensitivity labels adoption & usage
- Sensitive Info Types configuration
- Data Loss Prevention gaps

Riesgos de IA

- Copilot readiness assessment
- AI-specific exposure vectors
- Prompt data leakage risks
- Microsoft Graph permissions

Permisos & Exposición

- Oversharing analysis (SharePoint, Teams)
- Permission inheritance & exposure paths
- External sharing risk assessment
- Guest access & collaboration risks

Shadow AI

- Unauthorized AI tool usage detection
- Data sharing in external AI prompts
- Browser-based AI app controls
- User behavior & compliance gaps

Proceso

Metodología de Ejecución

Cinco fases para entregar insights accionables

01 Preparación

Scope definition, stakeholder mapping, data collection requirements

Semana 1

02 Workshops

Discovery sessions with security, compliance, and business teams

Semana 2

03 Revisión Técnica

Deep-dive analysis of Purview configuration, policies, and data exposure

Semana 3

04 Risk Mapping

Prioritized risk matrix, business impact assessment, quick wins identification

Semana 4

05 Executive Readout

Strategic presentation with scores, roadmap, and actionable recommendations

Semana 5

Duración total
5 semanas

Entregables
6 documentos

Stakeholders
CISO, CIO, Legal

Ejemplo practico

Perfil del Cliente Evaluado

Grupo Retail NovaMarket - Análisis de riesgo en entorno financiero

NovaMarket

Grupo Retail

Usuarios totales	25,000
Licenciamiento	M365 E5
Área foco	Finanzas

Riesgo Principal Identificado

Exposición de **información financiera sensible** y **datos personales de clientes** a través de:

Colaboración digital

SharePoint, Teams, OneDrive con permisos abiertos

Herramientas de IA

Copilot, agentes y shadow AI sin controles

Usuarios Finanzas

1,200

Área de alto riesgo con acceso a información financiera sensible y datos personales de clientes

Datos financieros

Estados, pagos, nómina

PII de clientes

Identidad, contacto, histórico

Cumplimiento

PCI-DSS, GDPR, SOX

Resultados Ejecutivos

Score de Madurez + AI Exposure

Evaluación cuantitativa del estado actual de seguridad de datos

OPTI
tecnologías que dan valor

Data Security Maturity

Madurez de controles de protección de datos

1.9 /4

● Riesgo Alto

Controles de DLP limitados, etiquetas sin adopción efectiva, y falta de gobierno de permisos

AI Exposure Score

Exposición a riesgos de inteligencia artificial

1.2 /4

● Alto Riesgo

Permisos abiertos explotables por Copilot, shadow AI activo, y falta de controles para prompts

Nivel 1	Nivel 2	Nivel 3	Nivel 4
Inicial	Parcial	Definido	Optimizado

Análisis de Riesgos

Top Riesgos Ejecutivos

Siete vulnerabilidades críticas identificadas en NovaMarket

OPTI
tecnologías que dan valor

01 DLP Limitado a Exchange — Alto

Las políticas DLP solo protegen correo electrónico, dejando expuestos SharePoint, Teams y OneDrive

02 Etiquetas sin Adopción — Alto

Las sensitivity labels existen pero tienen <15% de adopción por usuarios de finanzas

03 Datos Sensibles Sobreexpuestos — Crítico

Información financiera en SharePoint con permisos de "cualquiera con el enlace"

04 Permisos Abiertos → Copilot — Crítico

Copilot puede acceder a datos que usuarios ni siquiera saben que tienen disponibles

05 Uso Activo de Shadow AI — Alto

32% de usuarios de finanzas utilizan ChatGPT y herramientas similares sin controles

06 Sin Controles para Prompts de IA — Alto

No hay prevención de que usuarios peguen datos sensibles en herramientas de IA externas

07 Apps con Permisos Excesivos — Medio

Aplicaciones de terceros con acceso amplio a Microsoft Graph y datos de usuarios

⚠ **Impacto combinado:** Estos riesgos crean un escenario donde la información financiera y PII están expuestos a filtraciones accidentales y maliciosas.

Análisis Profundo

Oversharing + Copilot Risk

Cómo los permisos heredados amplifican la exposición de datos

OPTI
tecnologías que dan valor

Métricas de Oversharing

Archivos con "cualquiera con enlace"	2,847
Contienen datos sensibles	34%
Accesibles externamente	892

Repositorios críticos

Finanzas/Estados	968 archivos
RRHH/Nómina	523 archivos
Legal/Contratos	412 archivos

El efecto Copilot

Cuando un usuario consulta Copilot, la IA accede a **todos los documentos** que el usuario tiene permiso de ver, incluso si:

- No saben que tienen acceso a esos documentos
- Los permisos fueron heredados de equipos anteriores
- Los archivos contienen datos de otros departamentos

1,247	4,521	$2.4M
Usuarios con acceso amplificado	Documentos potencialmente expuestos	Estimado de impacto por brecha

Insight ejecutivo: Copilot no viola permisos, pero expone la mala gestión de permisos heredados que las organizaciones han acumulado durante años.

Análisis Profundo

Shadow AI: El Riesgo Invisible

Uso no autorizado de herramientas de IA y exposición de datos

OPTI
tecnologías que dan valor

Uso detectado de Shadow AI

32%
de usuarios en Finanzas

384
usuarios activos detectados

ChatGPT (web)	287 usuarios
Claude / Bard	156 usuarios
GitHub Copilot	89 usuarios
Midjourney / DALL-E	67 usuarios

Tendencia de uso

Crecimiento mensual **+18%**

Vectores de riesgo

Copy-paste de datos sensibles
Usuarios pegan información financiera, PII y datos confidenciales en prompts

Carga de documentos
Archivos de Excel, PDFs y reportes subidos para análisis por IA

Falta de visibilidad
No se sabe qué datos salieron ni quién los compartió

> **El problema:** Los usuarios no actúan con malicia, buscan productividad. Pero cada prompt puede exponer datos regulados y confidenciales.

Acciones Inmediatas

Quick Wins: 0-30 Días

Seis acciones de alto impacto y bajo esfuerzo para reducir riesgo inmediatamente

OPTI
tecnologías que dan valor

01

Expandir DLP

Extender políticas DLP a SharePoint, OneDrive y Teams, no solo Exchange

Impacto inmediato

02

Reducir Oversharing

Eliminar enlaces "cualquiera" en repositorios críticos de finanzas y RRHH

Impacto inmediato

03

Controlar Shadow AI

Implementar bloqueo de herramientas de IA no autorizadas vía Microsoft Defender

Impacto inmediato

04

SITs Personalizados

Crear Sensitive Info Types para datos específicos del negocio (SKU, ID internos)

Mejora detección

05

Simplificar Etiquetas

Reducir de 12 a 4 etiquetas clave y crear guía de uso para usuarios

Mejora adopción

06

Gobierno de Permisos

Establecer proceso de revisión trimestral de permisos en sitios críticos

Prevención

Resultado esperado: Implementación de estos quick wins puede reducir la exposición de datos en un 60-70% dentro del primer mes.

Plan Estratégico

Roadmap de Implementación

Tres horizontes para alcanzar madurez de seguridad de datos

OPTI
tecnologías que dan valor

Horizonte 1
0-30 días

Quick Wins

- Expandir DLP a SPO/Teams/OD
- Reducir oversharing crítico
- Implementar controles Shadow AI
- Crear SITs personalizados
- Simplificar etiquetas
- Gobierno de permisos

Meta: Reducir riesgo 60-70%

Horizonte 2
31-90 días

Automatización

- Implementar auto-labeling
- Desplegar Endpoint DLP
- Controles para aplicaciones de IA
- Tuning de políticas DLP
- Train users on labels
- Copilot readiness assessment

Meta: Madurez nivel 3

Horizonte 3
3-6 meses

Optimización

- Implementar DSPM
- Desplegar Insider Risk Management
- Gobierno de datos integral
- Modelo operativo definido
- Habilitación segura de Copilot
- Métricas y KPIs de seguridad

Meta: Madurez nivel 4

Quick wins · Automatización · Optimización

Timeline total estimado
6 meses

Valor de Negocio

Beneficios para el Negocio

Impacto cuantificable de la implementación del programa de seguridad de datos

OPTI
tecnologías que dan valor

Reducción de Riesgo

Reducción de exposición Datos sensibles expuestos	-70%
Prevención de brechas Incidentes de data loss	-85%
Compliance posture Cumplimiento regulatorio	+60%

ROI Financiero

$2.4M Costo evitado por brecha	$850K Multas regulatorias evitadas
40% Reducción tiempo incidentes	3.2x ROI en 12 meses

Habilitación de IA

- Copilot seguro y compliant desde el día 1
- Confianza para adoptar agentes de IA
- Visibilidad y control sobre uso de IA

Eficiencia Operativa

Automatización de clasificación	80% auto
Reducción falsos positivos	-65%
Tiempo de respuesta a incidentes	-40%

Resultado estratégico: Transformar la seguridad de datos de un centro de costos a un habilitador de negocio que permite adoptar IA con confianza.

Iniciemos tu
AI-Ready Assessment

OPTI
tecnologías que dan valor

SEC
SERVICIOS DE CIBERSEGURIDAD

Evaluamos tu exposición de datos frente a la IA, identificamos riesgos críticos y te entregamos un roadmap priorizado para proteger tu información.

Kickoff
2 semanas después de aprobación

Duración
5 semanas de assessment

Entregables
Scores, matriz de riesgos, roadmap

Convertimos la tecnología en un activo estratégico para su negocio.