OBSERVATORIO
DE CIBERSEGURIDAD
by SECCURACY

SHADOW IT & SHADOW AI

Análisis 2026

* Análisis estratégico basado en Microsoft, Netskope, IBM y Gartner

CRECIMIENTO DEL SHADOW IT GLOBAL

47% de usuarios de IA generativa acceden con cuentas personales

60% de organizaciones tuvieron incidentes por apps personales en la nube

20% de brechas vinculadas a Shadow AI (IBM 2025)

+USD 670.000 de sobrecosto promedio por brecha con Shadow AI

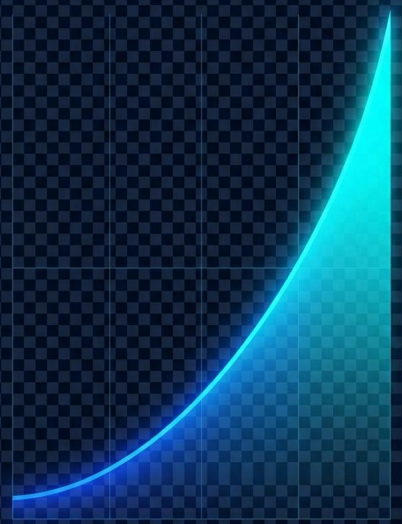
63% sin política de gobierno de IA al sufrir una brecha

69% sospecha o confirma uso de IA no autorizada (Gartner)

+40% de empresas sufrirán incidentes por Shadow AI para 2030

+1.550 apps de IA generativa rastreadas (versus 317 en 2024)

SECCURACY
Certeza en seguridad de la información



El crecimiento del Shadow IT no es coyuntural, sino estructural. La incorporación de herramientas de IA acelera exponencialmente la expansión de tecnología fuera del control organizacional.

Fuente: Netskope Cloud & Threat Report 2026; IBM Cost of a Data Breach Report 2025; Gartner, 2025.

TABLA DE EXPOSICIÓN POR TIPO DE TECNOLOGÍA

Tecnología no controlada	Nivel de exposición
SaaS / Aplicaciones cloud	Alto
Herramientas de IA generativa	Crítico
Almacenamiento personal	Alto
Automatizaciones (APIs / no-code)	Alto
Extensiones de navegador	Medio

Lectura Estratégica: El riesgo ya no se concentra en la infraestructura, sino en el uso distribuido de tecnología por parte del usuario. La superficie de ataque se vuelve dinámica, descentralizada e invisible para IT.

Fuente: Netskope Cloud & Threat Report 2026; Microsoft Defender for Cloud Apps; IBM Cost of a Data Breach Report 2025.

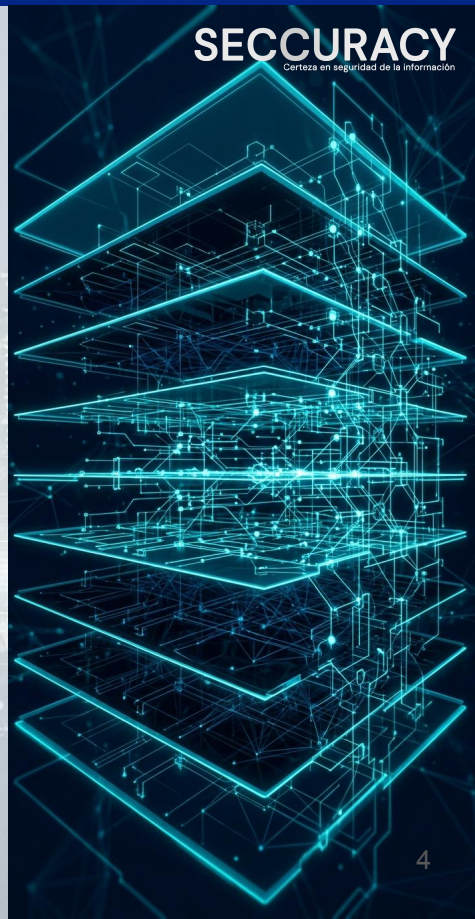
METODOLOGÍAS: EVOLUCIÓN DEL USO TECNOLÓGICO

Shadow IT tradicional: Uso de SaaS no autorizadas. Base sobre la que se apoyan el resto de las variantes.

Shadow SaaS: Proliferación de servicios cloud sin control corporativo. Dificulta la visibilidad y gobierno del inventario.

Shadow AI: Uso de IA sin gobierno del dato. Transferencia de información sensible a plataformas externas no validadas.

Shadow Integrations: Automatizaciones vía APIs sin validación de seguridad. Flujos de datos invisibles para IT.



Fuente: Elaboración propia basada en Microsoft, Netskope 2026.

NUEVAS FRONTERAS DEL RIESGO DIGITAL

- **Uso masivo de IA generativa con datos sensibles sin validación**
- **Integraciones invisibles vía APIs y plataformas no-code**
- **Uso de cuentas personales en entornos corporativos**
- **Transferencia de datos fuera del perímetro sin trazabilidad ni cifrado**
- **Falta de visibilidad sobre el ciclo de vida del dato en herramientas externas**

Conclusión del fenómeno: El Shadow IT ha evolucionado hacia un ecosistema paralelo donde el dato circula sin control, convirtiendo cada herramienta no gestionada en un vector potencial de exposición y fuga.

Fuente: IBM Cost of a Data Breach Report 2025; Netskope Cloud & Threat Report 2026; Gartner, 2025.

BUENAS PRÁCTICAS Y PREVENCIÓN

Estrategias de visibilidad, control y cultura organizacional

SECCURACY
Certeza en seguridad de la información

TECNOLOGÍA, PROCESOS Y CULTURA

SECCURACY

Tecnología	Procesos	Cultura Organizacional
CASB / SSPM para visibilidad cloud	Inventario actualizado de SaaS	Programas de concientización
SSO + MFA para control de acceso	Evaluación formal de proveedores	Awareness específico en IA
DLP (Data Loss Prevention)	Política de uso de IA generativa	Capacitación continua
Monitoreo continuo de tráfico cloud	Catálogo de herramientas aprobadas	Canales de reporte seguros

Fuente: Elaboración propia basada en Microsoft Defender for Cloud Apps; Netskope Cloud & Threat Report 2026.

¿CÓMO REACCIONAR ANTE UN INCIDENTE?

- Identificar y mapear las aplicaciones no autorizadas detectadas en la red.
- Bloquear accesos riesgosos mediante CASB y políticas de firewall.
- Revisar logs de tráfico cloud para determinar el alcance de la exposición.
- Contener posibles fugas de datos y evaluar el impacto.
- Ajustar y reforzar las políticas de uso tecnológico y controles de acceso.

Fuente: Microsoft Defender for Cloud Apps; IBM Cost of a Data Breach Report 2025.

TENDENCIAS CLAVE PARA 2026

✔ **Shadow AI como principal vector de riesgo**: La IA generativa sin gobierno del dato se consolida como la amenaza más crítica.

✔ **BYOAI generalizado:** Los usuarios incorporan sus propias herramientas de IA sin supervisión corporativa.

✔ **Automatización sin control:** Proliferación de flujos automatizados vía APIs y no-code fuera del perímetro gestionado.

✔ **Menor control de IT:** La descentralización tecnológica reduce la capacidad de mantener inventarios actualizados.

✔ **Mayor exposición del dato:** El volumen de información sensible fuera del perímetro controlado continuará en ascenso.

Fuente: Gartner, 2025; Netskope Cloud & Threat Report 2026; IBM Cost of a Data Breach Report 2025.

FUENTES PRINCIPALES

Fuente	Tipo
Microsoft Defender for Cloud Apps	Oficial tecnológico
Netskope Cloud & Threat Report 2026	Consultoría privada
IBM Cost of a Data Breach Report 2025	Consultoría privada
Gartner – GenAI Blind Spots (Dic. 2025)	Analista de mercado

Certeza en seguridad de la información.

OBSERVATORIO DE CIBERSEGURIDAD by SECCURACY

Informe desarrollado por SECCURACY

Marzo **2026**

www.seccuracy.com.ar