Microsoft

La confianza como pilar de la Inteligencia Artificial. Y la Transformación de frontera

Santiago Cavanna
CISO Advisor – Microsoft MCSA
scavanna@microsoft.com

Microsoft

FRONTIER TRANSFORMATION

Intelligence + Trust: El fundamento de la empresa del futuro

Microsoft · Abril 2026 · Confidencial — Solo uso interno

ZONA 1

LA CAPA DE INTELIGENCIA

Poner la "I" de vuelta en la IA

La inteligencia no es el modelo. Es lo que la organización ya sabe: sus datos, sus flujos, sus relaciones. Los modelos cambian cada mes. Tu inteligencia debe perdurar.

Work IQ
Cómo trabaja cada persona: colaboración, patrones, producción

Fabric IQ
Razonamiento sobre datos de la organización con gobierno incorporado

Foundry IQ
Servidor de aplicaciones de AI: escala, seguridad, confiabilidad

> "Los modelos cambiarán. Tu inteligencia debe perdurar."
> — Microsoft Frontier Transformation Pitch, Marzo 2026

ZONA 2

ECUACIÓN CENTRAL

INTELLIGENCE + ⟷ + TRUST = FRONTIER FIRM

"Una Frontier Firm no solo agrega herramientas de AI. Conecta inteligencia que entiende cómo funciona el negocio, y la gobierna para que escale con confianza."

1.300 M agentes de AI proyectados para 2028
IDC / Microsoft, 2026

29% de los agentes en organizaciones operan sin aprobación de TI o Seguridad

ZONA 3

CAPA DE CONFIANZA / TRUST

OBSERVABILIDAD

"Lo que no se ve, no se puede gobernar"

Las organizaciones no saben cuántos agentes corren, qué hacen, ni a qué datos acceden. Agent 365 provee una vista unificada de todos los agentes —incluyendo terceros (Adobe, ServiceNow, Workday, Databricks)— con dashboards de telemetría, mapas de conectividad y métricas de impacto de negocio.

> "Sin inventario, no hay gobierno. Sin gobierno, no hay confianza."
> — Vasu Jakkal, CVP Microsoft Security

GOBIERNO

"Políticas de ciclo de vida para entidades no-humanas"

Los marcos de gobierno tradicionales no fueron diseñados para agentes. Microsoft propone tratarlos como empleados: identidad propia, acceso de mínimo privilegio, políticas de ciclo de vida y auditoría completa. Agent 365 permite incorporar, controlar, expirar y bloquear agentes desde un admin center centralizado.

✓ El agente PUEDE	✗ El agente NO DEBE
Acceder a datos autorizados	Escalar privilegios
Ejecutar en su scope	Acceder a recursos externos no declarados
Auditar cada acción	Operar sin propietario asignado

AI EU AI Act · GDPR Art. 5(2) · DORA

ZERO TRUST PARA AI

"Extender el paradigma Zero Trust a identidades no-humanas"

Cada agente recibe un Entra Agent ID con gestión de ciclo de vida, acceso condicional y filtrado de red. Microsoft Defender extiende la protección de amenazas al ecosistema de agentes. El Agent Governance Toolkit mapai directamente a los Top 10 riesgos OWASP para sistemas agénticos.

⚠ Prompt Injection · ⚠ Goal Hijacking · ⚠ Identity Abuse · ⚠ Data Poisoning · ⚠ Rogue Agents

> "Es extender Zero Trust al Zero Trust para AI. Igual que con personas: verificar identidad, mínimo privilegio, asumir compromiso."
> — Vasu Jakkal, CVP Microsoft Security, 2026

ZONA 4

[Microsoft Agent 365] [Microsoft Entra Agent ID] [Microsoft Defender XDR] [Microsoft Purview] [Copilot Studio] [Microsoft Sentinel]

Fuentes: Microsoft FY26 Pitch Deck, Vasu Jakkal Microsoft Security, IDC 2026, McKinsey AI Trust Survey 2026

LA IA Y LOS AGENTES INTRODUCEN NUEVOS DESAFÍOS DE SEGURIDAD EN ORGANIZACIONES DE TODOS LOS TAMAÑOS.

Proliferación de agentes y acceso a recursos

82%

de líderes esperan usar agentes en los próximos 12-18 meses para satisfacer la demanda de capacidad laboral[3]

Compartición excesiva de datos y fugas

80%

de líderes citaron la fuga de datos sensibles como su principal preocupación[1]

Shadow AI, nuevas amenazas de IA y vulnerabilidades

88%

de organizaciones están preocupadas por los ataques de inyección de prompt indirecta[2]

Cumplimiento normativo

55%

de líderes carecen de comprensión sobre cómo se regula y se regulará la IA y están buscando orientación[1]

1. First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400.
2. How to Secure Custom-Built AI Agents, Gartner, 17 March 2025, Dionisio Zumerle, Jeremy D'Hoinne.
3. Microsoft Work Trend Index Survey 2025

Lo que toda organización necesita para confiar en los agentes

Monitoreo y gestión de agentes

Guardrails para agentes y usuarios

Protección integral para agentes

CONFIANZA A LA ESCALA DE LA IA

La confianza es un **acelerador**

La confianza permite **elegir modelos**

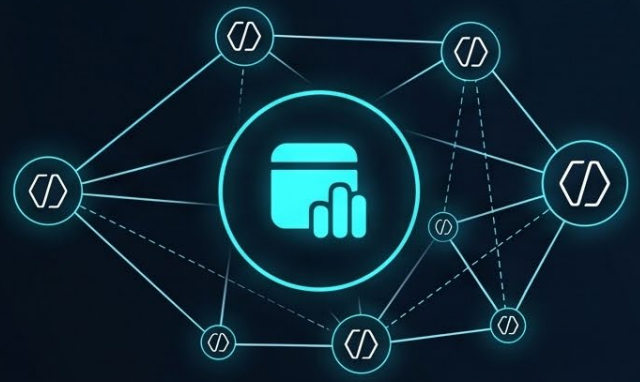
La confianza se **aplica, no se asume**

Microsoft

MICROSOFT AGENT 365

El plano de control para agentes

OBSERVAR



Monitorear y gestionar agentes en tiempo real

GOBERNAR

Establecer barreras de seguridad para agentes y usuarios

ASEGURAR

Proteger agentes de manera integral

Monitorear y gestionar agentes en tiempo real

Establecer barreras de seguridad para agentes y usuarios

Proteger agentes de manera integral

[Microsoft Agent 365] [Microsoft Entra Agent ID] [Microsoft Defender XDR] [Microsoft Purview] [Copilot Studio] [Microsoft Sentinel]

Microsoft

GESTIONAR LA SEGURIDAD EN EL PLANO DE CONTROL DE FOUNDRY

Protección de datos y cumplimiento

Protección de datos
Purview fortalece las protecciones de datos confidenciales en todas las interacciones de agentes de IA.

Visibilidad de auditoría
La actividad del agente fluye a Purview para una visibilidad de auditoría completa.

Protección basada en etiquetas
Las etiquetas de confidencialidad y las políticas de protección de Purview son respetadas por Azure AI Search, por lo que los agentes y las aplicaciones de IA acceden solo a los datos que los usuarios están autorizados a usar.

Microsoft Purview

Postura de seguridad y amenazas emergentes

Información de postura
Defender proporciona recomendaciones para la postura de seguridad del agente.

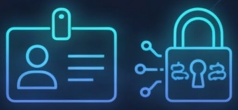
Alertas de riesgo
Alerta a los desarrolladores sobre amenazas y vulnerabilidades.

Rutas de ataque
Defender muestra posibles rutas de ataque en los entornos de agentes.

Inteligencia de amenazas
Defender añade detecciones para técnicas de ataque nuevas y emergentes.

Microsoft Defender

Identidad segura y acceso



Gestionar agentes de IA a escala
Asigna identidades únicas a nuevos agentes de IA para que las organizaciones puedan aplicar controles consistentes de identidad y acceso desde el primer día.

Gobernar identidades de agentes
Mantiene su flota de agentes bajo control con gestión de ciclo de vida y barreras de seguridad, incluyendo patrocinadores y paquetes de acceso de mínimo privilegio.

Proteger el acceso del agente o recursos
Reduce el riesgo de brecha aplicando políticas de Acceso Condicional para agentes y bloqueando el acceso de agentes riesgosos a los recursos.

Microsoft Entra Agent ID

ZONA 1

[Microsoft Agent 385] [Microsoft Entra Agent ID] [Microsoft Defender XDR] [Microsoft Purview] [Copilot Studio] [Microsoft Sentinel]

Eouerao Micnesoft TH/S Piich Tleeli, Nacu (Aiinl
Microsoft Security, IDC 2008, Maltlskey AI Thist Survey, 2020

ASEGURAR Y GOBERNAR LA IA CON MICROSOFT

COMENZAR SEGURO → MANTENERSE SEGURO

CAPACIDADES DE SEGURIDAD Y GOBIERNO

PROTEGER SECRETOS Y CÓDIGO
GitHub Advanced Security

GESTIONAR ACCESO DE AGENTES, EXPANSIÓN Y GUARDARRAÍLES
Plano de control de Foundry y Entra Agent ID

PREVENIR RIESGOS + VULNERABILIDADES
Agente de Red Teaming de AI, evaluaciones de Foundry y gestión de postura de Defender

DEFENDER CONTRA AMENAZAS
Inteligencia de amenazas de Microsoft Defender, Escudos de Prompt de Foundry

PREVENIR FUGAS DE DATOS Y HABILITAR CUMPLIMIENTO
Microsoft Purview

MICROSOFT ENTRA | **MICROSOFT DEFENDER** | **MICROSOFT PURVIEW**

COMPROMISOS FUNDACIONALES

SEGURO POR DISEÑO, SEGURO POR DEFECTO, OPERACIONES SEGURAS
Iniciativa de Futuro Seguro

LOS DATOS SON PRIVADOS EN EL TRABAJO, EN CASA Y EN MOVIMIENTO
Principios de privacidad

EQUIDAD, FIABILIDAD Y SEGURIDAD, PRIVACIDAD Y SEGURIDAD, INCLUSIÓN, TRANSPARENCIA, RENDICIÓN DE CUENTAS
Principios de AI

Seguridad integrada para agentes de IA: Desde el código hasta el tiempo de ejecución

Comience seguro y permanezca seguro con Microsoft