DE PREGUNTAS AISLADAS A UN SISTEMA PERMANENTE DE GOBIERNO CIBERNÉTICO

Transformamos las inquietudes del Directorio en una capacidad continua de decisión, priorización y rendición de cuentas.

PROPÓSITO

Establecer un sistema permanente para gobernar el riesgo cibernético y proteger la continuidad y el valor del negocio.

1 SITUACIÓN ACTUAL | Preguntas reactivas y reportes fragmentados

PREGUNTAS REACTIVAS
El Directorio recibe respuestas puntuales sin contexto ni trazabilidad.

INFORMACIÓN FRAGMENTADA
Datos dispersos entre áreas, sin estándares ni consistencia.

DECISIONES DESALINEADAS
Falta de conexión entre riesgo, inversión y prioridades del negocio.

RIESGO NO CUANTIFICADO
No se comprende el impacto real ni la exposición aceptada por la organización.

SIN EVIDENCIA SOSTENIBLE
Dificultad para demostrar mejora, decisiones y rendición de cuentas.

2 NUESTRA INTERVENCIÓN | Advisory, Co-Gobierno y Alineamiento

TRADUCIMOS EXPECTATIVAS DEL DIRECTORIO
Convertimos el lenguaje del negocio en prioridades de riesgo y capacidades.

ESTRUCTURAMOS LA ESTRATEGIA
Alineamos ciberseguridad con los objetivos del negocio y la transformación digital.

PRIORIZAMOS INVERSIONES
Enfocamos recursos en lo que reduce efectivamente el riesgo y genera valor.

SISTEMA PERMANENTE DE DECISIÓN
Evidencia • Contexto
Decisiones • Seguimiento
Mejora Continua

ORGANIZAMOS CAPACIDADES
Diseñamos el modelo operativo, roles, procesos y tecnologías necesarias.

CONSTRUIMOS MÉTRICAS Y GOBIERNO
Definimos indicadores clave, tableros y mecanismos de control y trazabilidad.

FACILITAMOS EL VÍNCULO CON EL NEGOCIO
Conectamos ciberseguridad con operaciones, tecnología, finanzas, legal y compliance.

3 RESULTADO | Un sistema que responde cuatro preguntas fundamentales

1 ¿CUÁL ES NUESTRO NIVEL REAL DE RIESGO?
Comprendemos nuestra exposición, impactos y riesgo residual.

2 ¿ESTAMOS MEJORANDO?
Demostramos evolución de capacidades y reducción de riesgo.

3 ¿ESTAMOS INVIRTIENDO CORRECTAMENTE?
Nuestras inversiones están alineadas al riesgo y generan resultados medibles.

4 ¿ESTAMOS PREPARADOS PARA UNA INTERRUPCIÓN SIGNIFICATIVA?
Probamos nuestra resiliencia y capacidad de recuperación.

NO ES UN ASSESSMENT. NO ES UNA ARQUITECTURA AISLADA.
ES UN SISTEMA PERMANENTE DE DECISIÓN, EVIDENCIA Y MEJORA CONTINUA.

DIRECTORIO
Supervisa, decide y rinde cuentas.

CISO
Lidera, responde y ejecuta.

ASESOR EXTERNO
Facilita, desafía, estructura y conecta.

NEGOCIO
Ejecuta, comparte responsabilidad y genera valor.

@SCavanna - Microsoft MCSA - Security

Microsoft

DIRECTORIO, CISO Y ASESOR:
UN MODELO DE RESPONSABILIDAD SIN SUSTITUCIÓN DE ROLES

El valor del advisory está en conectar expectativas, decisiones, ejecución y evidencia manteniendo responsabilidades claramente diferenciadas.

PRINCIPIO CLAVE

- El Directorio supervisa.
- El CISO lidera.
- El asesor estructura y desafía.
- El negocio comparte responsabilidad.
- La evidencia conecta a todos.

1. DIRECTORIO

SUPERVISA Y DEFINE EXPECTATIVAS

- Define apetito y tolerancia al riesgo.
- Aprueba estrategia, inversiones y riesgos aceptados.
- Supervisa desempeño y rendición de cuentas.
- Recibe evidencia y toma decisiones.

ENTREGA

- Expectativas estratégicas
- Aprobaciones
- Decisiones y riesgos aceptados
- Solicitudes de evidencia

2. CISO

LIDERA, INTERPRETA Y RESPONDE

- Interpreta expectativas del Directorio.
- Define estrategia y prioridades.
- Dirige la ejecución y coordina al equipo.
- Gestiona riesgos, excepciones e incidentes.
- Rinde cuentas con evidencia objetiva.

ENTREGA

- Estrategia y planes
- Prioridades e inversiones
- Indicadores y métricas
- Reportes y recomendaciones

3. ASESOR EXTERNO

FACILITA, DESAFÍA, ESTRUCTURA Y CONECTA

- Traduce expectativas del Directorio.
- Desafía supuestos y expone riesgos no visibles.
- Estructura el modelo de gobierno y los foros.
- Diseña métricas y tableros.
- Mantiene trazabilidad y memoria del programa.

ENTREGA

- Marcos, modelos y mejores prácticas
- Agendas y materiales ejecutivos
- Tableros y métricas
- Seguimiento de compromisos

SISTEMA DE EVIDENCIA COMPARTIDA

Única fuente de verdad para decisiones y rendición de cuentas.

4. ÁREAS DEL NEGOCIO Y OPERACIONES (IT / OT)

EJECUTAN Y APORTAN CONTEXTO

- Ejecutan controles y planes en su ámbito.
- Gestionan riesgos propios y dependencias.
- Reportan eventos, indicadores y cambios.
- Participan en decisiones y simulaciones.

ENTREGA

- Información operacional y de riesgo
- Indicadores y cumplimiento
- Recursos y capacidades
- Acciones y compromisos

5. FUNCIONES DE APOYO Y CONTROL

ASESORAN, VALIDAN Y GARANTIZAN CUMPLIMIENTO

- Auditoría: evaluación independiente.
- Riesgo: integra riesgos empresariales.
- Legal/Compliance: requisitos y obligaciones.
- RRHH: cultura, talento y conducta.
- Finanzas: presupuesto y valor.

ENTREGA

- Evaluaciones y observaciones
- Requisitos regulatorios y legales
- Marcos de control y políticas
- Información para decisiones

CÓMO FLUYE LA INFORMACIÓN Y LA DECISIÓN

1. **EXPECTATIVAS** — El Directorio define expectativas y apetito de riesgo.
2. **ANÁLISIS Y CONTEXTO** — El CISO y el equipo analizan, priorizan y proponen.
3. **DESAFÍO Y ASESORÍA** — El asesor desafía, enriquece opciones y estructura la conversación.
4. **DECISIÓN** — El Directorio decide, aprueba o define acciones y riesgos aceptados.
5. **EJECUCIÓN** — Las áreas ejecutan y avanzan en los compromisos.
6. **EVIDENCIA Y REPORTE** — Se genera evidencia, se mide y se reporta el desempeño.
7. **APRENDIZAJE Y MEJORA** — Se incorporan lecciones, se ajustan prioridades y se reinicia el ciclo.

LO QUE ESTE MODELO GARANTIZA

- Rendición de cuentas clara y trazable
- Decisiones informadas y oportunas
- Alineamiento entre riesgo, negocio y tecnología
- Inversiones priorizadas y defendibles
- Mayor resiliencia y continuidad

LAS 15 CONVERSACIONES
QUE SOSTIENEN EL MANDATO DEL CISO INDUSTRIAL

Tres pilares. Quince conversaciones. Una conversación permanente con el Directorio.

- Responder de forma consistente
- Medir, comparar y evidenciar
- Tomar mejores decisiones
- Trazabilidad entre riesgo, decisión y acción

1 ESTRATEGIA
¿PROTEGEMOS EL VALOR?

La estrategia define cómo la ciberseguridad contribuye a la continuidad, la competitividad y la creación de valor.

1 ¿ESTAMOS SEGUROS?

Nivel de exposición, confianza, riesgo residual y tolerancia al riesgo.

- Probabilidad de interrupción
- Exposición actual
- Riesgo aceptado

2 ¿CÓMO ESTAMOS FRENTE A NUESTROS COMPETIDORES?

Benchmarking sectorial en inversión, madurez y capacidades diferenciales.

- Posición relativa
- Brechas clave
- Ventajas competitivas

3 ¿QUÉ ESTÁ OCURRIENDO EN NUESTRA INDUSTRIA?

Incidentes relevantes, tendencias de ataque e impacto económico.

- Casos públicos
- Tendencias
- Lecciones aprendidas

4 ¿ESTAMOS INVIRTIENDO ADECUADAMENTE?

Análisis de inversiones en tecnología, personas, procesos y terceros.

- Reducción de riesgo
- Retorno esperado
- Prioridades futuras

5 ¿HABILITA LA CIBERSEGURIDAD LA TRANSFORMACIÓN?

Alineamiento con innovación, automatización, IA y convergencia IT/OT.

- Industria 4.0 / IA
- Operaciones autónomas
- Convergencia IT/OT

2 GOBIERNO
¿CONTROLAMOS EL RIESGO QUE ASUMIMOS?

El gobierno asegura trazabilidad, control, responsabilidades y cumplimiento de lo que la organización decide aceptar.

6 ¿QUÉ RIESGOS ESTAMOS ACEPTANDO?

Definición del apetito de riesgo y gestión de excepciones.

- Vulnerabilidades
- Deuda técnica
- Excepciones
- Riesgo residual

7 ¿CÓMO MEDIMOS NUESTRA MADUREZ?

Evolución según marcos de referencia y modelos de madurez.

- NIST CSF
- Zero Trust
- IEC 62443 / CIS Controls
- Madurez y brechas

8 ¿CÓMO INTERACTÚA CIBERSEGURIDAD CON LA ORGANIZACIÓN?

Relación con áreas clave del negocio y funciones de control.

- Auditoría y Control Interno
- Operaciones y Tecnología
- RR. HH., Legal, Compliance

9 ¿ESTAMOS CUMPLIENDO REQUISITOS REGULATORIOS?

Cumplimiento de regulaciones nacionales, corporativas y sectoriales.

- Regulaciones nacionales
- Requisitos corporativos
- Infraestructura crítica
- Auditorías externas

10 ¿QUIÉN TOMA DECISIONES DURANTE UNA CRISIS?

Gobierno de incidentes y escalamiento durante situaciones críticas.

- Escalamiento
- Crisis Management
- Comité Ejecutivo
- Directorio

3 GESTIÓN
¿PODEMOS EJECUTAR Y RECUPERARNOS?

La gestión transforma estrategia y gobierno en capacidades operativas medibles y resiliencia real.

11 ¿QUÉ TIPOS DE INCIDENTES PODRÍAN AFECTARNOS?

Identificación de escenarios y vectores de ataque relevantes.

- Ransomware
- OT / ICS
- Supply Chain
- Insider Threat
- Identidad comprometida
- Exfiltración de datos

12 ¿PODEMOS DETECTAR Y RESPONDER OPORTUNAMENTE?

Capacidades de monitorización, detección, investigación y respuesta.

- Monitorización
- Detección
- Investigación
- Respuesta
- Recuperación

13 ¿NUESTROS PLANES FUNCIONAN?

Validación práctica de planes y capacidades ante escenarios reales.

- Simulaciones
- Tabletop Exercises
- Purple Team
- Crisis Drills

14 ¿CUÁL ES EL RIESGO INTRODUCIDO POR TERCEROS?

Gestión de proveedores y servicios críticos tercerizados.

- Proveedores tecnologicos
- Integradores
- MSSP / MSSOC
- Partnres estratégicos

15 ¿CÓMO ASEGURAMOS RESILIENCIA OPERACIONAL?

Continuidad, recuperación y dependencias críticas bajo control.

- Continuidad operacional
- Recuperación ante desastres
- Sitios remotos
- Ambientes OT heredados
- Dependencias críticas

UNA CONVERSACIÓN PERMANENTE

Estas 15 conversaciones se revisan cíclicamente con el Directorio, se actualizan con evidencia y se convierten en decisiones que protegen el negocio y generan confianza.

Conversamos → Evaluamos → Decidimos → Ejecutamos → Evidenciamos

- Riesgo comprendido y controlado
- Decisiones basadas en evidencia
- Inversiones alineadas al valor y al riesgo
- Mejora continua y adaptación
- Resiliencia para proteger el negocio

DE LA PREGUNTA DEL DIRECTORIO A LA EVIDENCIA

CAPACIDADES MICROSOFT COMO PLATAFORMA HABILITADORA

La tecnología entrega señales. El modelo de gobierno las convierte en decisiones y resultados.

PRINCIPIO CLAVE

- El Directorio supervisa.
- El CISO lidera.
- El asesor estructura y desafía.
- El negocio comparte responsabilidad.
- La evidencia conecta a todos.

1 PREGUNTA

El Directorio y el negocio plantean sus inquietudes estratégicas.

2 SEÑALES

Las capacidades Microsoft generan datos, eventos y telemetría.

3 CONTEXTO

Analizamos, correlacionamos y priorizamos según riesgo, impacto y objetivos del negocio.

4 DECISIÓN

Se definen acciones, inversiones, controles y excepciones aceptadas.

5 ACCIÓN

Ejecutamos iniciativas, mejoras y controles alineados a la estrategia.

6 EVIDENCIA

Medimos resultados para demostrar mejora, resiliencia y valor generado.

PREGUNTAS ESTRATÉGICAS DEL DIRECTORIO (4 RESULTADOS CLAVE)

¿CUÁL ES NUESTRO NIVEL REAL DE RIESGO?

Comprendemos exposición, impactos y riesgo residual.

¿ESTAMOS MEJORANDO?

Demostramos evolución de capacidades y reducción de riesgo.

¿ESTAMOS INVIRTIENDO CORRECTAMENTE?

Nuestras inversiones están alineadas al riesgo y generan resultados medibles.

¿ESTAMOS PREPARADOS PARA UNA INTERRUPCIÓN SIGNIFICATIVA?

Probamos nuestra resiliencia y capacidad de recuperación.

9 DOMINIOS HABILITADORES MICROSOFT

1 IDENTIDAD Y ZERO TRUST

- Microsoft Entra ID
- Entra Conditional Access
- Entra ID Governance
- Entra Verified ID
- Privileged Identity Management

Responde a:
- Riesgo
- Gobierno
- Cumplimiento
- Madurez

2 PROTECCIÓN Y RESPUESTA

- Microsoft Defender XDR
- Defender for Endpoint
- Defender for Identity
- Defender for Cloud Apps
- Defender for Office 365
- Microsoft Sentinel

Responde a:
- Incidentes
- Detección
- Respuesta
- Resiliencia

3 GESTIÓN DE VULNERABILIDADES Y POSTURA

- Defender Vulnerability Management
- Defender for Cloud
- CSPM
- Exposure Management

Responde a:
- Riesgo asumido
- Madurez
- Benchmarking
- Priorización

4 PROTECCIÓN DE DATOS Y GOBIERNO

- Microsoft Purview
- DLP
- Information Protection
- Insider Risk Management
- Data Lifecycle Management

Responde a:
- Gobierno
- Compliance
- Riesgo

5 OBSERVABILIDAD Y OPERACIONES

- Azure Monitor
- Log Analytics
- Application Insights
- Azure Arc
- Microsoft Sentinel

Responde a:
- Monitoreo
- Continuidad
- Gestión

6 GESTIÓN DE ACTIVOS Y ENDPOINTS

- Microsoft Intune
- Configuration Manager
- Azure Arc

Responde a:
- Vulnerabilidades
- Configuración
- Riesgo operativo

7 CONTINUIDAD OPERACIONAL

- Azure Backup
- Azure Site Recovery
- Azure Storage

Responde a:
- Recuperación
- Continuidad
- Resiliencia

8 DEVSECOPS

- GitHub Enterprise
- GitHub Advanced Security
- Azure DevOps

Responde a:
- Riesgo de aplicaciones
- Seguridad del software
- Vulnerabilidades

9 INTELIGENCIA ARTIFICIAL Y AGENTES

- Microsoft 365 Copilot
- Security Copilot
- Copilot Studio
- Azure AI Foundry
- Azure AI Search

Responde a:
- Gobierno
- Automatización
- Toma de decisiones
- Soporte ejecutivo

FUENTES DE EVIDENCIA

- Telemetría continua
- Eventos e incidentes
- Vulnerabilidades y exposición
- Cumplimiento y auditorías
- Pruebas y simulaciones
- Recuperación y continuidad
- Decisiones y excepciones

RESULTADOS PARA EL NEGOCIO

Riesgo comprendido y cuantificado
Visibilidad real de exposición e impacto.

Prioridades claras y defendibles
Inversiones alineadas al riesgo y al valor.

Mejora continua demostrable
Evolución de capacidades y madurez medible.

Decisiones informadas y trazables
Gobierno robusto con evidencia objetiva.

Resiliencia probada y recuperable
Capacidad de responder y recuperarse ante interrupciones críticas.

MICROSOFT COMO PLATAFORMA HABILITADORA, NO COMO FIN.
El valor surge cuando cada capacidad se conecta con riesgo, decisión y evidencia.

Microsoft

- Enfocado en resultados de negocio
- Basado en gobierno, riesgo y datos
- Apalancado en el ecosistema Microsoft
- Conversación permanente con el Directorio
- Decisiones que generan valor y resiliencia

SERIE DE 3 INFOGRAFÍAS

1 2 3

MAPA DE MADUREZ DEL GOBIERNO DE IA EN MICROSOFT

Del Asistente Personal al Ecosistema de Agentes Empresariales

Evolución escalonada de capacidades, controles e integraciones para gobernar la IA con confianza.

NIVEL (Madurez)	PLATAFORMA (Superficie Principal)	¿QUÉ RESPONDE? (Pregunta de Gobierno)	CAPACIDADES CLAVE (Ejemplos Destacados)	INTEGRACIONES CLAVE (Verticales de Seguridad)
1	**COPILOT CHAT** (Incluido sin costo con M365 E3/E5/Business)	¿Cómo habilitar IA empresarial básica con protección corporativa mínima?	• Activación/desactivación por tenant en M365 Admin Center • Grounding limitado (web + archivo abierto) • Enterprise Data Protection (EDP): sin uso de datos para entrenamiento • Analytics básicos de uso • Control de endpoints con Intune / Edge	**Entra ID** Autenticación corporativa (EDP) **Purview** DLP bloquea búsquedas web por SIT; Audit **Sentinel** Logs vía Unified Audit Log **Intune / Defender** Deshabilitar Copilot Chat en endpoints gestionados
2	**MICROSOFT 365 COPILOT** ($30/usuario/mes, add-on sobre E3/E5)	¿Cómo controlar y proteger el acceso de la IA a los datos corporativos?	• Copilot Control System (User access, Data access, Copilot actions, Other) • DLP en runtime: prompts + archivos etiquetados • DSPM for AI: detección de oversharing y acciones remediales • SharePoint Advanced Management (SAM) • Respeta permisos existentes en Microsoft Graph • Analytics avanzado (Copilot Dashboard, Viva Insights)	**Entra ID** Permisos Graph del usuario; CA, MFA, grupos **Purview** DLP, Labels, DSPM for AI, eDiscovery, Retention, Insider Risk, Comm. Comp. **Sentinel** Conector de datos Copilot (Preview) **Defender** Defender for Cloud Apps: patrones de acceso inusuales
3	**COPILOT STUDIO** (Plataforma low-code en Power Platform)	¿Cómo gobernar la creación de agentes por citizen developers y áreas de negocio?	• Estrategia de entornos zonificada (Default, Dev, Test/UAT, Prod) • DLP multinivel: Tenant → Environment → Agent • Control de conectores, canales y fuentes de conocimiento • Autenticación Entra ID obligatoria por defecto • ALM: pipeline Dev → Test → Prod (gated) • Zero-rated usage en M365 Copilot / Teams / SP • No se puede deshabilitar totalmente la creación de agentes (mitigación: DLP + control de entornos)	**Entra ID** Makers/usuarios autenticados; grupos para entornos y asignación de licencias **Purview** DLP, Labels, Insider Risk, Comm. Comp., eDiscovery, Audit de interacciones **Sentinel** Logs de auditoría Purview integrables vía UAL **Defender** Postura vía Defender for Cloud (si conecta a recursos Azure)
4	**AZURE AI FOUNDRY** (PaaS en Azure para agentes enterprise)	¿Cómo gobernar agentes críticos, complejos o regulados?	• RBAC multicapa (5 roles) • Evaluaciones pre-producción en 5 dimensiones • Prompt Shields (ataques a prompts y documentos) • AI Red Teaming Agent • Network isolation: private endpoints, control de trafico • Guardrail policies y evaluación continua • AI Reports exportables (PDF / SPDX) • 3 dashboards: ejecutivo, seguridad, operativo	**Entra (Agent ID)** Identidad propia por agente; CA, Identity Protection, lifecycle, sponsor/owner **Purview** Integración nativa (toggle) DLP, DSPM, auditoría **Defender** Postura AI, descubre workloads, analiza rutas de ataque **Sentinel** Logs de Foundry → Log Analytics → Sentinel; playbooks IA **Intune** Aplica si corre en Windows 365 for Agents
5	**AGENT 365** (Control Plane unificado $15/usuario/mes standalone o incluido en M365 E7 a $99/usuario/mes)	¿Qué agentes existen, quién los usa y cómo aplicar gobierno uniforme sobre todos ellos?	**OBSERVE** Registro unificado, Agent Map, Analytics, Activity View (30 días) **GOVERN** Onboarding controlado, Lifecycle, Policy Templates, Integrations, Audit & Compliance **SECURE** Access Control, Data Security, Threat Protection, Shadow AI detection, Registry Sync (AWS, Google Cloud), BYO MCP (Preview)	**Entra** Entra Agent ID, CA, Identity Protection, lifecycle workflows **Purview** Audit, DLP, eDiscoveey y compliance de agentes cross-plataforma **Defender** Detección de amenazas en runtime, postura, bloqueo de agentes **Intune** Shadow AI detection en endpoints Windows **Sentinel** Centraliza señales de todas las plataformas para SOC y gobierno

PRINCIPIO RECTOR

La mejor forma de gestionar agentes es extender la infraestructura que ya se usa para gestionar usuarios.

M365 Admin Center (Hub) + Entra (Identidades y Acceso) + Purview (Datos y Cumplimiento) + Defender (Postura y Amenazas) + Sentinel (SIEM/SOAR para IA)

SERIE DE 3 INFOGRAFÍAS

1 — 2 — 3

Pieza 2 de 3

MATRIZ DE INTEGRACIÓN
VERTICALES DE SEGURIDAD × NIVELES DE IA

Cómo cada vertical de Microsoft protege y gobierna los niveles de IA

Cada plataforma de IA se fortalece cuando las verticales trabajan juntas.

VERTICALES DE SEGURIDAD (¿Qué hacen?)	NIVELES DE IA / PLATAFORMAS				
	COPILOT CHAT (Incluido sin costo con M365 E3/E5/ Business)	**MICROSOFT 365 COPILOT** ($30/usuario/mes, add-on sobre E3/E5)	**COPILOT STUDIO** (Plataforma low-code en Power Platform)	**AZURE AI FOUNDRY** (PaaS en Azure para agentes enterprise)	**AGENT 365** (orquestador) (Control Plane unificado)
MICROSOFT ENTRA Identidad y acceso ¿Quién es el agente y qué puede hacer?	• Autenticación corporativa obligatoria (EDP aplica al iniciar sesión)	• Corre en nombre del usuario • Permisos de Microsoft Graph definen el alcance de datos • CA, MFA y grupos Entra para licencias	• Autenticación Entra ID obligatoria para makers y usuarios • Grupos Entra controlan acceso a entornos y licencias • Agent ID se provisiona automáticamente	• Entra Agent ID para cada agente publicado • CA, Identity Protection, access packages • Sponsor / Owner • Lifecycle workflows	• Extiende Entra Agent ID a toda la flota • Registro unificado de identidades de agentes • CA + Identity Protection aplicados a agentes
MICROSOFT PURVIEW Protección de datos y cumplimiento ¿Qué datos puede ver o exponer el agente?	• DLP bloquea búsquedas web por SITs en el prompt • Audit básico de interacciones	• DLP en runtime (prompts + archivos etiquetados) • Sensitivity Labels (E3 manual; E5 auto-labeling) • DSPM for AI • eDiscovery, Retention • Insider Risk (E5) • Comm. Compliance (E5) • Retención: "Teams chats & Copilot interactions"	• DLP, Etiquetado, Insider Risk, Comm. Compliance soportados para interacciones de agentes • eDiscovery y Audit vía parent app	• Integración nativa vía toggle en Control Plane • DLP, DSPM y Audit extendidos a agentes Foundry sin código adicional	• Conecta logs de auditoría, DLP y compliance de agentes cross-plataforma • Policy templates de Purview aplicables al onboarding de agentes
MICROSOFT DEFENDER Postura y detección de amenazas ¿Cuál es la postura de seguridad del agente?	— (No aplica directamente)	• Defender for Cloud Apps (E5): patrones de acceso inusuales	• Postura vía Defender for Cloud si agentes conectan a recursos en Azure	• Defender for Cloud: descubre agentes, postura AI, rutas de ataque, análisis de exposición	• Detección de amenazas en runtime de agentes • Gestión de postura y vulnerabilidades • Bloqueo de agentes comprometidos
MICROSOFT INTUNE Endpoints y Shadow AI ¿Hay IA no autorizada en los dispositivos?	• Control de activación de Copilot Chat en dispositivos gestionados	—	—	• Aplica si agentes corren en Windows 365 for Agents (Cloud PCs gestionados)	• Shadow AI detection: descubre agentes locales no autorizados en Windows (OpenClaw → GitHub Copilot CLI, Claude Code) • Bloqueo vía políticas de Intune
MICROSOFT SENTINEL SIEM / SOAR para IA ¿Qué incidente existe y cómo responder?	• Logs vía Purview Unified Audit Log (UAL)	• Conector de datos Copilot (Preview) • Ingesta de telemetría en Sentinel para monitoreo SOC	• Logs de auditoría Purview integrables vía UAL	• Logs de Foundry a Log Analytics → Sentinel • Playbooks de respuesta a incidentes IA	• Centraliza señales de todas las plataformas (Agent 365 + Entra + Purview + Defender) • SOC y gobierno con la misma imagen operativa

FÓRMULA DE COORDINACIÓN UNIFICADA

Cada componente responde a una pregunta de gobierno diferente

Agent 365 — ¿Qué agentes existen, dónde están, quién los usa, qué herramientas/datos consumen, cuáles son shadow agents?

→ **Entra Agent ID** — ¿Qué identidad tiene el agente, a qué puede acceder, bajo qué condiciones, quién es su sponsor, cuándo expira?

→ **Purview** — ¿Qué datos puede ver el agente, qué no debe exponer, qué interacciones auditar, qué evidencia conservar?

→ **Defender + Sentinel** — ¿Qué incidente existe, qué señales convergen, qué playbooks disparar, qué hunting hacer?

→ **RESULTADO:** Confianza, control y visibilidad unificados para todo el ciclo de vida de los agentes de IA.

LEYENDA DE CAPACIDADES

- Identidad y Acceso
- Protección de Datos y Cumplimiento
- Postura y Detección de Amenazas
- Endpoints y Shadow AI
- SIEM / SOAR para IA

NIVELES DE MADUREZ

(De básico a avanzado)

1. Asistente Personal → 2. Asistente Empresarial → 3. Creación de Agentes → 4. Agentes Enterprise → 5. Control Unificado

PRINCIPIO RECTOR

La mejor forma de gestionar agentes es extender la infraestructura que ya se usa para gestionar usuarios: M365 Admin Center como hub, Entra para identidades, Purview para datos y compliance, Defender para postura y amenazas, Sentinel para operación SOC.

SERIE DE 3 INFOGRAFÍAS

1 — 2 — 3

PIEZA 3 DE 3

MODELO OPERATIVO UNIFICADO

Agent 365 + Entra + Purview + Defender + Sentinel

Un plano de control integrado para gobernar toda la flota de agentes de IA

ECOSISTEMA DE PLATAFORMAS DE IA (Flota de Agentes)

Copilot Chat	Microsoft 365 Copilot	Copilot Studio	Azure AI Foundry	Agent 365
IA básica con riesgo acotado	IA en el trabajo con Microsoft Graph	Creación de agentes low-code	Agentes enterprise críticos y regulados	Control plane unificado
FOUNDATION	GOVERNED	EXTENDED	ENTERPRISE	UNIFIED CONTROL PLANE

Principio rector

La mejor forma de gestionar agentes es extender la infraestructura que ya se usa para gestionar usuarios.

- M365 Admin Center como hub
- Defender para postura y amenazas
- Entra para identidades y acceso
- Purview para datos y cumplimiento
- Sentinel para operación SOC

MICROSOFT ENTRA
Identidad y Acceso

- Entra Agent ID: identidad propia por agente
- Conditional Access, MFA e Identity Protection
- Access Packages, Sponsor/Owner
- Lifecycle workflows: creación, actualización y expiración de agentes

PREGUNTA QUE RESPONDE:
¿Qué identidad tiene el agente, a qué puede acceder, bajo qué condiciones y quién es su sponsor?

MICROSOFT INTUNE
Endpoints y Shadow AI

- Control de activación de Copilot Chat en dispositivos
- Descubrimiento de Shadow AI en Windows (OpenClaw → GitHub Copilot CLI, Claude Code)
- Bloqueo y control de uso de IA no autorizada
- Aplica si agentes corren en Windows 365 for Agents

PREGUNTA QUE RESPONDE:
¿Qué IA no autorizada existe en los endpoints y cómo controlarla?

REGISTRO ÚNICO DE AGENTES
Fuente única de verdad

AGENT 365
PLANO DE CONTROL UNIFICADO

OBSERVE
Registro unificado • Agent Map
Analytics • Activity View (30 días)
Shadow AI detection

GOVERN
Lifecycle Management • Policy Templates
Integration Management • Audit & Logging
Data Compliance

SECURE
Access Control • DLP en runtime
Threat Protection • Insider Risk
Bloqueo de agentes

CICLO DE VIDA DE AGENTES
Onboarding → Operación → Revisión → Expiración

MICROSOFT PURVIEW
Datos y Cumplimiento

- DLP en runtime: prompts, respuestas y archivos
- Sensitivity Labels y auto-labeling
- DSPM for AI: detección de oversharing y remediación
- eDiscovery, Retention, Audit, Insider Risk
- Communication Compliance (E5)

PREGUNTA QUE RESPONDE:
¿Qué datos puede ver el agente, qué no debe exponer y qué evidencia conservar?

MICROSOFT DEFENDER
Postura y Amenazas

- AI Security Posture Management: descubre agentes y evalúa postura
- Análisis de rutas de ataque y exposición
- Detección de amenazas en runtime de agentes
- Bloqueo de agentes maliciosos y comprometidos

PREGUNTA QUE RESPONDE:
¿Cuál es la postura de seguridad del agente y qué amenazas existen?

MICROSOFT SENTINEL
SIEM / SOAR para IA

- Ingesta de señales: Agent 365 + Entra + Purview + Defender + Foundry
- Correlación de eventos e incidentes en tiempo real
- Playbooks de respuesta a incidentes de IA

En Agent 365 (Grap lectura) de amenazas

PREGUNTA QUE RESPONDE:
¿Qué incidente existe, qué señales convergen y qué acciones (playbooks) ejecutar?

VALOR DEL MODELO UNIFICADO

- Visibilidad completa de todos los agentes (autorizados y shadow)
- Gobierno consistente con políticas centralizadas
- Reducción de riesgos por datos, identidad y amenazas
- Operación SOC efectiva con contexto completo
- Cumplimiento y auditoría simplificados

FÓRMULA DE COORDINACIÓN UNIFICADA

Cada componente responde a una pregunta de gobierno diferente

Agent 365	+ Entra Agent ID	+ Purview	+ Defender + Sentinel	= Gobierno Efectivo de Agentes de IA
¿Qué agentes existen, dónde están, quién los usa, qué herramientas/datos consumen y cuáles son shadow agents?	¿Qué identidad tiene el agente, a qué puede acceder, bajo qué condiciones, quién es su sponsor y cuándo expira?	¿Qué datos puede ver el agente, qué no debe exponer, qué interacciones auditar y qué evidencia conservar?	¿Qué incidente existe, qué señales convergen, qué playbooks disparar y qué hunting hacer?	

ROLES CLAVE EN EL GOBIERNO DE AGENTES

AI ADMIN	AI READER	SECURITY REVIEWER	SPONSOR / OWNER
Gestión completa del ciclo de vida, políticas, integraciones y seguridad	Lectura y auditoría de inventario, actividad y cumplimiento	Revisión de seguridad, evaluaciones y cumplimiento	Responsable del agente, aceptación de riesgos y decisiones de ciclo de vida
En Agent 365 (Control total)	En Agent 365 (Solo lectura)	En Azure AI Foundry y Agent 365	En Entra ID y Agent 365

PROFUNDIDAD FUNODIONAL DE AGENT 365 SEGÚN LICENCIA SUBYACENTE

Licencia base	Entra	Defender	Purview	Observabilidad A365
Office E3	Sin CA, IDP, ID Gov para agentes	Sin Threat Hunting	Sin protección de grounding data (sin labeling)	Completamente funcional
M365 E3	Sin CA, IDP, ID Gov para agentes	Sin Threat Hunting	Grounding data protegido con labels manuales	Completamente funcional
M365 E5	Sin IDP para agentes	Sin Threat Hunting	Grounding data protegido con labels manuales	Completamente funcional
M365 E5 + Security	Completamente funcional	Completamente funcional	Completamente funcional	Completamente funcional

LICENCIAMIENTO DESTACADO

Microsoft 365 E7 (Frontier Suite)
$99 USD /usuario/mes
Incluye M365 E5 + Copilot + Entra Suite + Agent 365
Funcionalidad completa en todas las verticales

Agent 365 (Standalone SKU)
$15 /usuario/mes
Disponible como SKU independiente

BUENAS PRÁCTICAS CLAVE

- ✓ Registrar todos los agentes en Agent 365
- ✓ Asignar owner/sponsor y revisar periódicamente
- ✓ Aplicar mínimo privilegio a identidades de agentes
- ✓ Clasificar y proteger datos con Purview
- ✓ Monitorear postura y amenazas con Defender
- ✓ Correlacionar y responder con Sentinel
- ✓ Detectar y bloquear Shadow AI con Intune

EL NUEVO ROL DEL CISO INDUSTRIAL

Cerrar la brecha entre el Directorio y la ciberseguridad

La mayoría de los CISO de industrias críticas no fracasan por problemas tecnológicos. Fracasan porque existe una **brecha** entre lo que el Directorio pregunta y la forma en que el **área de ciberseguridad responde**.

EL DIRECTORIO PIENSA EN

- Riesgo
- Continuidad operacional
- Impacto financiero
- Responsabilidad fiduciaria
- Reputación
- Cumplimiento regulatorio

LA BRECHA

- Lenguajes diferentes
- Prioridades desalineadas
- Decisiones sin contexto suficiente
- Pérdida de confianza

SEGURIDAD SUELE RESPONDER CON

- Vulnerabilidades
- Herramientas
- Incidentes
- Arquitecturas
- Controles

CISO ESTRATÉGICO

Convierte la ciberseguridad en una conversación de negocio basada en **riesgo, evidencia y valor.**

- Traducir expectativas
- Organizar estrategia
- Priorizar inversiones
- Construir indicadores
- Generar consensos
- Negociar presupuesto
- Comunicar riesgos
- Construir confianza

RESULTADO ESPERADO

- Confianza institucional
- Decisiones basadas en riesgo
- Alineación con el negocio
- Mejor comunicación ejecutiva

Este workbook **no es** una guía tecnológica.
Es una guía de liderazgo, gobierno, gestión y transformación.

→ PARA INDUSTRIAS CRÍTICAS

- MINERÍA
- ENERGÍA
- OIL & GAS
- INFRAESTRUCTURA CRÍTICA

PROPÓSITO DEL PROGRAMA

Acompañar al CISO durante 12 meses para responder con evidencia las preguntas que el Directorio exige.

SIGUIENTE:
LOS TRES PILARES DEL MODELO

@SCavanna - Microsoft MCSA - Security

LOS TRES PILARES DEL MODELO

Tres dimensiones para una conversación ejecutiva completa

Toda la conversación entre Directorio y CISO puede organizarse en **tres dimensiones complementarias e interdependientes**.

1 ESTRATEGIA

¿Estamos protegiendo adecuadamente el negocio?

ENFOQUE

- Riesgo
- Posicionamiento
- Prioridades
- Inversiones

2 GOBIERNO

¿Tenemos control sobre los riesgos que asumimos?

ENFOQUE

- Accountability
- Cumplimiento
- Madurez
- Respon-abilidades

3 GESTIÓN

¿Somos capaces de ejecutar lo que prometemos?

ENFOQUE

- Capacidades operativas
- Detección y respuesta
- Validación y ejercicios
- Continuidad operacional

CIBERSEGURIDAD ESTRATÉGICA

Confianza • Resiliencia • Valor

Proteger el negocio hoy y habilitar el futuro

DISEÑADO PARA DECISIONES, NO PARA HERRAMIENTAS

Cada pilar aporta una perspectiva esencial para tomar mejores decisiones, asignar recursos con criterio y demostrar gestión responsable.

El equilibrio entre los tres pilares genera valor sostenible y confianza institucional.

¿QUÉ LOGRAMOS CON ESTE MODELO?

ALINEACIÓN EJECUTIVA
Hablar el mismo idioma que el Directorio.

DECISIONES INFORMADAS
Basadas en riesgo, evidencia y contexto.

GESTIÓN RESPONSABLE
Gobernar, ejecutar y demostrar resultados.

CONFIANZA INSTITUCIONAL
Credibilidad, transparencia y resiliencia.

Este modelo no es lineal: los tres pilares se refuerzan constantemente.
El éxito del CISO depende del equilibrio dinámico entre ellos.

ANTERIOR:
1/9 EL NUEVO ROL DEL CISO INDUSTRIAL

SIGUIENTE:
3/9 LAS 5 PREGUNTAS DE ESTRATEGIA

Este modelo será la guía para responder las 15 preguntas clave del Directorio a lo largo de los próximos 12 meses.

LAS 5 PREGUNTAS DE ESTRATEGIA

Riesgo, contexto, inversión y transformación

El Directorio no busca certeza absoluta.
Busca entender el riesgo, priorizar y tomar mejores decisiones.

1 ¿CUÁL ES NUESTRO NIVEL REAL DE RIESGO?

Comprender nuestra exposición actual, sus tendencias y el riesgo residual.

EVIDENCIA CLAVE

- Nivel de riesgo actual
- Tendencia y evolución
- Riesgo residual
- Riesgo aceptado
- Nivel de exposición

EJERCICIO

Identificar 5 escenarios que podrían detener la operación.

Estimar probabilidad relativa e impacto económico.

2 ¿CÓMO ESTAMOS RESPECTO DEL SECTOR?

El Directorio necesita contexto para tomar decisiones informadas.

EVIDENCIA CLAVE

- Madurez relativa
- Inversión en ciberseguridad
- Capacidades clave
- Incidentes relevantes

EJERCICIO

Construir benchmark sectorial de madurez, inversión, capacidades e incidentes.

3 ¿QUÉ ESTÁ OCURRIENDO EN LA INDUSTRIA?

Los casos y tendencias de la industria nos enseñan y preparan.

EVIDENCIA CLAVE

- Ataques relevantes
- Tendencias emergentes
- Casos públicos
- Lecciones aprendidas

EJERCICIO

Preparar actualización trimestral con Top 10 incidentes globales, impacto económico y lecciones aplicables.

4 ¿ESTAMOS INVERTIENDO CORRECTAMENTE?

Toda inversión debe vincularse con la reducción, transferencia o evitación del riesgo.

EVIDENCIA CLAVE

- Riesgo mitigado
- Riesgo transferido
- Riesgo evitado

EJERCICIO

Mapear:
Presupuesto →
Capacidad →
Riesgo reducido.

5 ¿LA CIBERSEGURIDAD HABILITA LA TRANSFORMACIÓN?

Seguridad como habilitador, no como freno, de la innovación y el crecimiento.

IA | Automatización | IoT / OT | Digital Twins | Robótica

EVIDENCIA CLAVE

- Proyectos estratégicos
- Dependencias tecnológicas
- Riesgos que podrían bloquearlos
- Controles habilitadores

EJERCICIO

Listar proyectos estratégicos del negocio y responder:
¿Cómo los habilita ciberseguridad?
¿Cómo podría bloquearlos?

PRINCIPIOS PARA RESPONDER ESTAS PREGUNTAS

- Lenguaje de negocio
- Decisiones basadas en evidencia
- Enfocado en lo que realmente importa
- Riesgo aceptado explícito
- Comunicación clara, frecuente y oportuna

Responder estas 5 preguntas estratégicas consolida la base para gobernar y ejecutar con éxito.

ANTERIOR:
2/9 LOS TRES PILARES DEL MODELO

SIGUIENTE:
4/9 LAS 5 PREGUNTAS DE GOBIERNO

LAS 5 PREGUNTAS DE GOBIERNO

Decisiones explícitas, responsabilidades y evidencia

El Gobierno convierte el riesgo en decisiones claras, define responsabilidades y asegura que podamos demostrar cumplimiento y preparación ante una crisis.

6 ¿QUÉ RIESGOS ESTAMOS ACEPTANDO?

Todas las organizaciones aceptan riesgos. El problema es cuando nadie los conoce ni los gestiona.

ARTEFACTO / EVIDENCIA

Registro Ejecutivo de Riesgos

- Descripción del riesgo
- Impacto potencial
- Probabilidad
- Responsable del riesgo
- Estrategia de mitigación
- Estado actual

EJERCICIO EJECUTIVO

Construir y mantener un registro actualizado de riesgos críticos para el negocio.

7 ¿CÓMO MEDIMOS NUESTRA MADUREZ?

La madurez no puede medirse por percepción, sino con marcos reconocidos y un plan de mejora.

ARTEFACTO / EVIDENCIA

Perfil de Madurez y Plan de Transición (24M)

- Estado actual (as-is)
- Estado objetivo (to-be)
- Brechas prioritarias
- Roadmap de transición 24 meses

MARCOS DE REFERENCIA

- NIST CSF 2.0
- Zero Trust
- CIS Controls
- IEC 62443

EJERCICIO EJECUTIVO

Definir estado actual, estado objetivo y plan de transición a 24 meses con hitos y métricas.

8 ¿CÓMO INTERACTÚA CIBERSEGURIDAD CON LA ORGANIZACIÓN?

La seguridad no actúa sola. Debe integrar procesos y responsabilidades clave.

ARTEFACTO / EVIDENCIA

Mapa RACI Interorganizacional

Tecnología | Operaciones | RRHH | Legal | Auditoría | Control Interno

EJERCICIO EJECUTIVO

Construir y validar un mapa RACI que aclare roles, decisiones y rendición de cuentas.

9 ¿CUMPLIMOS LOS REQUISITOS REGULATORIOS?

La verdadera pregunta no es si cumplimos, sino si podemos demostrarlo en cualquier auditoría.

ARTEFACTO / EVIDENCIA

Mapa de Cumplimiento Regulatorio

- Obligaciones regulatorias aplicables
- Evidencias requeridas
- Controles y procesos asociados
- Estado de cumplimiento
- Procesos de auditoría y revisión

EJERCICIO EJECUTIVO

Identificar obligaciones, evidencias y procesos para demostrar cumplimiento ante auditores y reguladores.

10 ¿QUIÉN DECIDE DURANTE UNA CRISIS?

En una crisis el tiempo desaparece, la presión aumenta y las responsabilidades se confunden. La decisión debe estar definida antes de que ocurra.

ARTEFACTO / EVIDENCIA

Marco de Decisión en Crisis

- Comité de crisis y suplencias
- Escalamiento y notificación
- Matriz de decisión por escenarios
- Procedimientos ejecutivos y playbooks
- Comunicación ejecutiva y regulatoria

EJERCICIO EJECUTIVO

Definir comité, niveles de escalamiento, matriz de decisión y procedimientos listos para activar.

ACCOUNTABILITY: EL EJE QUE SOSTIENE EL GOBIERNO

Roles claros | Decisiones documentadas | Evidencias verificables | Revisión periódica | Transparencia y trazabilidad | Rendición de cuentas

SIN ACCOUNTABILITY, los riesgos quedan sin dueño y las decisiones sin respaldo.

El Gobierno no busca eliminar el riesgo.
Busca tomar decisiones informadas, gestionar lo aceptado y demostrar control con evidendia.

ANTERIOR: 3/9 LAS 5 PREGUNTAS DE ESTRATEGIA

EN ESTA SERIE VEREMOS

Estrategia 1–5 — Gobierno 6–10 — Gestión 11–15 — Evidencia Sist. Artefactos — Tecnologías Microsoft — Roadmap 12 Meses — Confianza Resultado

SIGUIENTE: 5/9 LAS 5 PREGUNTAS DE GESTIÓN

LAS 5 PREGUNTAS DE GESTIÓN

Capacidad operacional demostrada, no solo declarada

El Directorio quiere saber si somos capaces de ejecutar y mantener la operación ante amenazas, fallas o interrupciones significativas.

11 ¿QUÉ INCIDENTES PODRÍAN AFECTARNOS?

Pensar en escenarios, no en herramientes. Entender amenazas que pueden interrumpir el negocio.

EVIDENCIA CLAVE

- Catálogo corporativo de escenarios
- Impacto potencial por escenario
- Probabilidad relativa
- Dependencias críticas
- Controles existentes

EJERCICIO EJECUTIVO

Construir y revisar el catálogo de escenarios críticos con impacto operacional y financiero.

12 ¿PODEMOS DETECTAR Y RESPONDER OPORTUNAMENTE?

La velocidad determina el impacto.

EVIDENCIA CLAVE

- MTTD – Tiempo medio de detección
- MTTR – Tiempo medio de respuesta
- MTTC – Tiempo medio de recuperación
- Tendencia y objetivos aprobados
- Brechas y acciones priorizadas

EJERCICIO EJECUTIVO

Definir línea base actual, objetivos realistas y plan de mejora con hitos trimestrales.

13 ¿NUESTROS PLANES FUNCIONAN?

La única forma de validar un plan es poniéndolo a prueba.

EVIDENCIA CLAVE

- Plan anual de ejercicios aprobado
- Tabletop (directivos y críticos)
- Purple Team
- Red Team
- Lecciones aprendidas y mejoras

EJERCICIO EJECUTIVO

Ejecutar el plan anual de ejercicios y cerrar acciones correctivas con responsables.

14 ¿QUÉ RIESGO INTRODUCEN TERCEROS?

La superficie de ataque se extiende más allá de la organización.

EVIDENCIA CLAVE

- Inventario de terceros críticos
- Clasificación de criticidad
- Evaluación de riesgo y controles
- Monitoreo y desempeño
- Planes de respuesta conjunta

EJERCICIO EJECUTIVO

Clasificar terceros críticos y validar controles, contratos y planes de contingencia.

15 ¿PODEMOS MANTENER LA CONTINUIDAD OPERACIONAL?

No se trata de backups.
El Directorio pregunta cuánto tiempo podemos operar bajo condiciones adversas.

EVIDENCIA CLAVE

- RTO – Tiempo objetivo de recuperación
- RPO – Punto objetivo de recuperación
- Capacidades de recuperación
- Dependencias críticas del negocio
- Resultados de pruebas de recuperación

EJERCICIO EJECUTIVO

Validar RTO, RPO y capacidades de recuperación mediante pruebas periódicas.

PRINCIPIOS DE GESTIÓN OPERACIONAL

Visibilidad continua | Detección temprana | Respuesta coordinada | Recuperación rápida | Continuidad del negocio | Mejora continua

RESULTADO ESPERADO

Demostrar al Directorio que tenemos la capacidad de prepararnos, responder y mantener el negocio en funcionamiento.

ANTERIOR:
4/9 LAS 5 PREGUNTAS DE GOBIERNO

Estas cinco preguntas convierten la estrategia y el gobierno en capacidad real de ejecución.

SIGUIENTE:
6/9 DEL CUESTIONAMIENTO A LA EVIDENCIA

DEL CUESTIONAMIENTO A LA EVIDENCIA

La conversación ejecutiva debe terminar en decisiones trazables

Las 15 preguntas del Directorio solo generan valor cuando se convierten en evidencia verificable, responsabilidades claras y decisiones informadas.

PROPÓSITO

Conectar preguntas → artefactos → decisiones para gobernar el riesgo con evidencia.

		PREGUNTA DEL DIRECTORIO	ARTEFACTO / EVIDENCIA CLAVE	RESPONSABLE PRINCIPAL	CADENCIA SUGERIDA	DECISIÓN REQUERIDA
ESTRATEGIA ¿Estamos protegiendo adecuadamente el negocio?	1	¿Cuál es nuestro nivel real de riesgo?	Mapa de escenarios y exposición actual	CISO / Gerencia de Riesgos	Trimestral o ante cambios relevantes	Aceptar, mitigar, transferir o evitar riesgos críticos
	2	¿Cómo estamos respecto del sector?	Benchmark sectorial de madurez, inversión, capacidades e incidentes	CISO / Planeamiento Estratégico	Anual	Definir brechas prioritarias e inversiones
	3	¿Qué está ocurriendo en la industria?	Informe de inteligencia de amenazas y lecciones aprendidas	CISO / Inteligencia de Amenazas	Trimestral	Actualizar prioridades y controles según tendencias
	4	¿Estamos invirtiendo correctamente?	Mapa Presupuesto → Capacidad → Riesgo Reducido	CISO / Finanzas	Semestral	Aprobar, ajustar o redireccionar inversiones
	5	¿La ciberseguridad habilita la transformación?	Evaluación de proyectos estratégicos habilitados por seguridad	CISO / Líderes de Negocio	Por proyecto / revisión trimestral	Autorizar avance, condicionar o mitigar riesgos de bloqueo
GOBIERNO ¿Tenemos control sobre los riesgos que estamos asumiendo?	6	¿Qué riesgos estamos aceptando?	Registro Ejecutivo de Riesgos	Dueños de Riesgo / CISO	Trimestral	Aceptar con control, mitigar más o escalar al Directorio
	7	¿Cómo medimos nuestra madurez?	Perfil de Madurez (actual vs objetivo) Plan 24 meses	CISO / Arquitectura Empresarial	Semestral	Priorizar iniciativas para cerrar brechas críticas
	8	¿Cómo interactúa ciberseguridad con la organización?	Mapa RACI interorganizacional	CISO / Recursos Humanos	Anual o ante cambios organizacionales	Aprobar roles, responsabilidades y rendición de cuentas
	9	¿Cumplimos los requisitos regulatorios?	Mapa de Cumplimiento: obligaciones, evidencias y auditorías	CISO / Legal & Cumplimiento	Trimestral / según regulación	Demostrar cumplimiento ante auditores
	10	¿Quién decide durante una crisis?	Marco de Decisión en Crisis: comité, escalamiento, matriz y procedimientos	Comité de Crisis / CISO	Revisión semestral y antes de ejercicio	Autorizar y activar decisiones bajo presión
GESTIÓN ¿Somos capaces de ejecutar lo que prometemos?	11	¿Qué incidentes podrían afectarnos?	Catálogo corporativo de escenarios	CISO / Seguridad Operacional	Anual y ante cambios relevantes	Definir preparación por escenario prioritario
	12	¿Podemos detectar y responder a tiempo?	KPIs: MTTD, MTTR, MTTC Línea base y objetivos	SOC / CISO	Mensual (reporte)	Mejorar capacidades y procesos para cumplir objetivos
	13	¿Nuestros planes funcionan?	Plan anual de ejercicios: Tabletop, Simulación, Purple Team, Red Team	CISO / Continuidad del Negocio	Anual	Cerrar hallazgos y aprobar mejoras de planes
	14	¿Qué riesgo introducen terceros?	Registro y clasificación de terceros críticos	CISO / Compras / Legal	Semestral	Aprobar, condicionar o restringir terceros críticos
	15	¿Podemos mantener la continuidad operacional?	Plan de Continuidad: RTO, RPO, dependencias y capacidades de recuperación	Continuidad del Negocio / Operaciones	Semestral y después de cada prueba	Validar resiliencia y autorizar operación bajo condiciones adversas

REGRA DE ORO: Sin evidencia no hay confianza. Sin decisión no hay reducción de riesgo.

ANTERIOR: 4/9 LAS 5 PREGUNTAS DE GOBIERNO

ESTA SERIE CONSTRUVE CAPACIDAD EJECUTIVA

Estrategia · Gobierno · Gestión · Evidencia · Tecnologías · Roadmap · Confianza

SIGUIENTE: 6/9 DEL CUESTIONAMIENTO A LA EVIDENCIA

DEL CUESTIONAMIENTO A LA EVIDENCIA

La conversación ejecutiva debe terminar en decisiones trazables

Las 15 preguntas del Directorio solo generan valor cuando se convierten en evidencia verificable, responsabilidades claras y decisiones informadas.

PROPÓSITO

Conectar preguntas → artefactos → decisiones para gobernar el riesgo con evidencia.

		PREGUNTA DEL DIRECTORIO	ARTEFACTO / EVIDENCIA CLAVE	RESPONSABLE PRINCIPAL	CADENCIA SUGERIDA	DECISIÓN REQUERIDA
ESTRATEGIA ¿Estamos protegiendo adecuadamente el negocio?	1	¿Cuál es nuestro nivel real de riesgo?	Mapa de escenarios y exposición actual	CISO / Gerencia de Riesgos	Trimestral o ante cambios relevantes	Aceptar, mitigar, transferir o evitar riesgos críticos
	2	¿Cómo estamos respecto del sector?	Benchmark sectorial de madurez, inversión, capacidades e incidentes	CISO / Planeamiento Estratégico	Anual	Definir brechas prioritarias e inversiones
	3	¿Qué está ocurriendo en la industria?	Informe de inteligencia de amenazas y lecciones aprendidas	CISO / Inteligencia de Amenazas	Trimestral	Actualizar prioridades y controles según tendencias
	4	¿Estamos invirtiendo correctamente?	Mapa Presupuesto → Capacidad → Riesgo Reducido	CISO / Finanzas	Semestral	Aprobar, ajustar o redireccionar inversiones
	5	¿La ciberseguridad habilita la transformación?	Evaluación de proyectos estratégicos habilitados por seguridad	CISO / Líderes de Negocio	Por proyecto / revisión trimestral	Autorizar avance, condicionar o mitigar riesgos de bloqueo
GOBIERNO ¿Tenemos control sobre los riesgos que estamos asumiendo?	6	¿Qué riesgos estamos aceptando?	Registro Ejecutivo de Riesgos	Dueños de Riesgo / CISO	Trimestral	Aceptar con control, mitigar más o escalar al Directorio
	7	¿Cómo medimos nuestra madurez?	Perfil de Madurez (actual vs objetivo) Plan 24 meses	CISO / Arquitectura Empresarial	Semestral	Priorizar iniciativas para cerrar brechas críticas
	8	¿Cómo interactúa ciberseguridad con la organización?	Mapa RACI interorganizacional	CISO / Recursos Humanos	Anual o ante cambios organizacionales	Aprobar roles, responsabilidades y rendición de cuentas
	9	¿Cumplimos los requisitos regulatorios?	Mapa de Cumplimiento: obligaciones, evidencias y auditorías	CISO / Legal & Cumplimiento	Trimestral / según regulación	Demostrar cumplimiento ante auditores
	10	¿Quién decide durante una crisis?	Marco de Decisión en Crisis: comité, escalamiento, matriz y procedimientos	Comité de Crisis / CISO	Revisión semestral y antes de ejercicio	Autorizar y activar decisiones bajo presión
GESTIÓN ¿Somos capaces de ejecutar lo que prometemos?	11	¿Qué incidentes podrían afectarnos?	Catálogo corporativo de escenarios	CISO / Seguridad Operacional	Anual y ante cambios relevantes	Definir preparación por escenario prioritario
	12	¿Podemos detectar y responder a tiempo?	KPIs: MTTD, MTTR, MTTC Línea base y objetivos	SOC / CISO	Mensual (reporte)	Mejorar capacidades y procesos para cumplir objetivos
	13	¿Nuestros planes funcionan?	Plan anual de ejercicios: Tabletop, Simulación, Purple Team, Red Team	CISO / Continuidad del Negocio	Anual	Cerrar hallazgos y aprobar mejoras de planes
	14	¿Qué riesgo introducen terceros?	Registro y clasificación de terceros críticos	CISO / Compras / Legal	Semestral	Aprobar, condicionar o restringir terceros críticos
	15	¿Podemos mantener la continuidad operacional?	Plan de Continuidad: RTO, RPO, dependencias y capacidades de recuperación	Continuidad del Negocio / Operaciones	Semestral y después de cada prueba	Validar resiliencia y autorizar operación bajo condiciones adversas

REGRA DE ORO: Sin evidencia no hay confianza. Sin decisión no hay reducción de riesgo.

ANTERIOR: 4/9 LAS 5 PREGUNTAS DE GOBIERNO

ESTA SERIE CONSTRUVE CAPACIDAD EJECUTIVA

Estrategia · Gobierno · Gestión · Evidencia · Tecnologías · Roadmap · Confianza

SIGUIENTE: 6/9 DEL CUESTIONAMIENTO A LA EVIDENCIA

ROADMAP DE ACOMPAÑAMIENTO DE 12 MESES

De la comprensión a la demostración de valor ante el Directorio.

Un programa estructurado en cuatro trimestres para transformar la estrategia, el gobierno y la gestión en resultados medibles y evidencia confiable.

Q1 COMPRENDER — MESES 1–3

OBJETIVO

Establecer una línea base clara del riesgo, capacidades y contexto del negocio.

ENFOQUE

- Evaluación inicial y diagnóstico
- Identificación de riesgos críticos
- Inventario de capacidades actuales
- Mapeo de stakeholders
- Alineación con expectativas del Directorio

ENTREGABLES CLAVE

- Baseline de ciberseguridad
- Registro Ejecutivo de Riesgos
- Mapa de Stakeholders y comunicaciones
- Reporte de brechas y oportunidades
- Prioridades preliminares de negocio y seguridad

Q2 ORGANIZAR — MESES 4–6

OBJETIVO

Definir la estrategia, el modelo de gobierno y el plan de transformación.

ENFOQUE

- Definición de estrategia y posicionamiento de riesgo
- Diseño del modelo de gobierno y accountability
- Marco de métricas e indicadores
- Roadmap de iniciativas a 24 meses
- Aprobación de prioridades e inversiones

ENTREGABLES CLAVE

- Plan Director de Ciberseguridad
- Modelo de Gobierno y RACI
- Framework de Métricas y KPIs Ejecutivos
- Roadmap de Transformación 24 meses
- Plan de Inversiones y Caso de Negocio

Q3 EJECUTAR — MESES 7–9

OBJETIVO

Ejecutar las iniciativas priorizadas, gestionar progreso y riesgos.

ENFOQUE

- Implementación de iniciativas estratégicas
- Gestión de programas y proyectos
- Integración tecnológica y operativa
- Gestión de riesgos y dependencias
- Comunicación y gestión del cambio

ENTREGABLES CLAVE

- Dashboard Estratégico
- Dashboard de Gobierno
- Dashboard Operacional
- Reporte de Avance de Programas
- Control de Riesgos y Acciones Correctivas

Q4 DEMOSTRAR — MESES 10–12

OBJETIVO

Demostrar resultados, madurez alcanzada y preparación ante el Directorio.

ENFOQUE

- Medición de resultados y KPIs
- Ejercicios de crisis y resiliencia
- Revisión ejecutiva con el Directorio
- Evaluación de madurez
- Definición del plan del siguiente ciclo

ENTREGABLES CLAVE

- Informe Anual al Directorio
- Evaluación de Madurez y Tendencia
- Riesgo Residual y Exposición
- Lecciones Aprendidas
- Plan del Siguiente Ciclo (12–24 meses)

HABILITADORES TRANSVERSALES DURANTE TODO EL PROGRAMA

- Comunicación con el Directorio
- Alineación con negocio y operaciones
- Gestión de Riesgos continua
- Métricas e Indicadores en tiempo real
- Gestión del Cambio y Cultura
- Seguridad por Diseño (Zero Trust)

Este roadmap cubre 12 meses de acompañamiento. La transición completa hacia el estado objetivo de madurez puede extenderse hasta 24 meses.

ÉXITO DEL PROGRAMA

Decisiones informadas, riesgos bajo control, operación resiliente y confianza institucional.

RESULTADO ESPERADO

- Menor Exposición al Riesgo
- Mejor Toma de Decisiones
- Inversión Eficiente
- Operación Resiliente
- Confianza del Directorio

ANTERIOR: 7/9 CAPACIDADES MICROSOFT AL SERVICIO DE DECISIONES

SIGUIENTE: 9/9 EL SCORECARD DE CONFIANZA

WORKBOOK EJECUTIVO PARA EL CISO INDUSTRIAL

LAS 4 PREGUNTAS QUE DEFINEN AL CISO ESTRATÉGICO

LO QUE REALMENTE NECESITA COMPRENDER EL DIRECTORIO

El éxito del CISO industrial no se mide por la ausencia de incidentes, sino por su capacidad para **entender, explicar** y **gestionar** el riesgo con **evidencia**.

1 ¿CUÁL ES NUESTRO NIVEL REAL DE RIESGO?

Entender la exposición real del negocio hoy.

- Escenarios críticos
- Exposición actual
- Tendencias y amenazas
- Riesgo residual
- Dependencias críticas

EVIDENCIA CLAVE

- Mapa de riesgos y exposición
- Catálogo de escenarios
- Riesgo residual aceptado
- Métricas de riesgo

2 ¿ESTAMOS MEJORANDO?

Demostrar progreso y reducción del riesgo.

- Madurez actual vs. objetivo
- Tendencia de métricas
- Mejoras implementadas
- Lecciones aprendidas
- Brechas prioritarias

EVIDENCIA CLAVE

- Dashboard de madurez
- Indicadores de tendencia
- Planes de mejora
- Resultados de ejercicios

3 ¿ESTAMOS INVIRTIENDO CORRECTAMENTE?

Vincular inversión, capacidades y reducción del riesgo.

- Presupuesto vs. plan
- Capacidades financiadas
- Riesgo mitigado/transferido/evitado
- Prioridades vs. valor
- Decisiones pendientes

EVIDENCIA CLAVE

- Mapa inversión → riesgo
- Evaluación de valor
- Capacidades habilitadas
- Backlog de decisiones

4 ¿ESTAMOS PREPARADOS PARA UNA INTERRUPCIÓN SIGNIFICATIVA?

Demostrar resiliencia y capacidad de mantener operaciones críticas.

- Planes de continuidad
- RTO, RPO y capacidades
- Resultados de ejercicios
- Recuperación y pruebas
- Dependencias y terceros críticos

EVIDENCIA CLAVE

- Planes y runbooks
- Resultados de pruebas
- Tiempo de recuperación
- Mapa de dependencias

LA BASE QUE SOSTIENE LAS 4 RESPUESTAS

EVIDENCIA
Información confiable, trazable y actualizada que permite tomar decisiones con certeza.

GOBIERNO
Decisiones claras, roles definidos, accountability y cumplimiento demostrable.

GESTIÓN
Capacidad operacional, procesos efectivos y ejecución disciplinada de los planes.

LO QUE EL DIRECTORIO ESPERA DEL CISO

- Visión clara del riesgo del negocio
- Comunicación simple, relevante y frecuente
- Decisiones basadas en evidencia y contexto
- Gestión responsable y priorización disciplinada
- Preparación y resiliencia ante interrupciones significativas
- Mejora continua y creación de valor

LA MISIÓN DEL CISO INDUSTRIAL MODERNO ES ADMINISTRAR CONFIANZA.
No se trata de eliminar el riesgo, sino de gestionarlo con inteligencia, disciplina y transparencia para proteger el negocio y generar valor sostenible.

ANTERIOR:
8/9 ROADMAP DE ACOMPAÑAMIENTO DE 12 MESES

EN ESTA SERIE HEMOS CONSTRUIDO:

- 1-2 Modelo y Pilares
- 3-5 15 Preguntas Ejecutivas
- 6 Del cuestionamiento a la evidencia
- 7 Capacidades Microsoft
- 8 Roadmap de 12 meses
- 9 Scorecard de confianza

FIN DE LA SERIE
ESTÁS LISTO PARA LA CONVERSACIÓN CON EL DIRECTORIO

@SCavanna - Microsoft MCSA - Security

PLAN DE INFOGRAFÍAS DE ALTO IMPACTO: MICROSOFT AGENT 365

AUDIENCIA: Arquitectos de Soluciones y CISOs | ALCANCE: Agent 365 de extremo a extremo | FORMATO: Editorial-Visual

RUTA CRÍTICA: GOBERNANZA & SEGURIDAD →

01. LA EMPRESA AGENCIAL: POR QUÉ SE NECESITA UN PLANO DE CONTROL

Contasto de proiiferación de agentes IA, singinierão de chation AI y necesidad estratégiaa de Agent 365 como respuesta unificada.

02. ARQUITECTURA UNIFICADA DE AGENT 365

Estructura de le plataforma! Centro de administración IS265, Entra, Befunder, Perviam o Intuno como componentes integrados del control plane.

03. OBSERVABILIDAD: VISIBILIDAD TOTAL DE LA FLOTA DE AGENTES

Telemotría en tiempo real, panciea de métrivas, OpeeTelemotry y detección temprana de anomallas.

04. GOBERNANZA PROACTIVA A ESCALA EMPRESARIAL

Directivas contralizadas, mínimo pricilegia, cnimuotización de controlas de cisio de viiia y praporación para auditeria.

05. SEGURIDAD INTEGRAL Y PROTECCIÓN EN TIEMPO REAL

Defenaa en profundidad para paentes: identidad, OFB, deteeción de amenazaa con Defunden dentrolas de red y sistemiente.

06. IDENTIDAD DE AGENTE: MICROSOFT ENTRA AGENT ID

Fundamento de identiiiad corporativa para agentes, medidas delegado ve autónomo, acesua condicional y petreainadores.

12. PROTECCIÓN DE DATOS, RESIDENCIA Y RETENCIÓN

Geografía de ahoaconamiente, citrado, retención de 30 días, compromisos de eusipitninste (DPA, SOK, IOR) y fimileo de datos de la UE.

11. CUMPLIMIENTO NORMATIVO Y AUDITORÍA CON MICROSOFT PURVIEW

DLF. pógentes de sansibilidad, RXPM para IA, auditoría inrastaida, oftioyovory y administración de rrasgos infornos aplicados a agentes.

AGENT 365: ARQUITECTURA Y PLANO DE CONTROL UNIFICADO

06. REGISTRO CENTRALIZADO DE AGENTES

Inventario unificado multi-pletetoriuo: liiicea, aaciones administrativas y visibilidad de agentes gestionados y no gestionados.

07. CICLO DE VIDA DEL AGENTE: DE LA CREACIÓN AL RETIRO

Incorporación controlada, operación soucreleada, resatpnación de oropiedad y baja planificado.

ECOSISTEMA EXTENDIDO →

13. INTEGRACIONES NATIVAS: AGENTES DEL ECOSISTEMA MICROSOFT

Coutiat Studio, Foundra, Agent Ruibler y planjclas MCP, ſsteegración antomatico con registro, syiociorcia e Identidad Entre.

14. AGENTES EXTERNOS, TERCEROS Y ECOSISTEMA DE SOCIOS

Sineronización del regintre con AMS Gedroeb y Scogfe Cloud. SDX para agentes personcircanos, scales de leacsmiento (Sonsuerk, Zendock, Koro, etc.).

15. HERRAMIENTAS DE DESARROLLO: SDK, CLI Y WORK IQ MCP

SDKs multiplateforma, CLI de Agent 365, exbliogo de herramientas MCP y fiuia de certificación para markoiptese.

16. SHADOW AI: DETECCIÓN Y BLOQUEO DE AGENTES NO GESTIONADOS

Deseubrindento de agentes loceles sia bitona/ffefander, blogoeo de OpenCiou, aigoso de ronta de explosióa y coatlolos basados en paliticos.

17. MEDICIÓN DE VALOR E IMPACTO EMPRESARIAL

Mátriesa de productividad. DCI de agentes, vivoulación de ascioioso con resultados de negocio y anátiris de tendencias de adopción.

18. ESTRATEGIA DE ADOPCIÓN: DE LA VISIBILIDAD AL CONTROL TOTAL

Modulo de adopción por faces (inventario --- identidad -- control oseasado), mejeres prácticas y ovolución hacia la emprasa agencial madura.

FASE DE ADOPCIÓN & VALOR

@SCavanna

LA EMPRESA AGENCIAL:
POR QUÉ SE NECESITA UN PLANO DE CONTROL

Serie: Plan de Infografías de Alto Impacto | Bloque 1 de 18

SOPORTE

DISPONIBILIDAD: Mayo 2026 (Comercial)

PRINCIPIO: Observabilidad es el punto de partida

ALCANCE: Multiplataforma (Microsoft & Socios)

@SCavanna

02. ARQUITECTURA UNIFICADA DE AGENT 365: PLANO DE CONTROL

DIAGRAMA DE ARQUITECTURA EN CAPAS | INTEGRACIÓN CON LA PILA DE SEGURIDAD Y ADMINISTRACIÓN DE MICROSOFT

CENTRO DE ADMINISTRACIÓN DE MICROSOFT 365 (M365 ADMIN CENTER)

PUNTO DE ENTRADA Y EXPERIENCIA UNIFICADA

Ventanilla única de administración. Resumen, uso, adopción y gobernanza de agentes.

MICROSOFT ENTRA (IDENTIDAD Y ACCESO)

IDENTIDAD DEL AGENTE

Control de acceso, autenticación, identidad de agente (Agent ID).

MICROSOFT PURVIEW (CUMPLIMIENTO Y DATOS)

AUDITORÍA Y PROTECCIÓN

Protección de datos, cumplimiento normativo, auditoría extendida.

AGENT 365: PLANO DE CONTROL UNIFICADO PARA AGENTES

MICROSOFT DEFENDER (SEGURIDAD Y AMENAZAS)

DETECCIÓN EN TIEMPO REAL

Detección de amenazas, insights de postura de seguridad.

MICROSOFT INTUNE (ENDPOINTS Y DISPOSITIVOS)

GOBIERNO LOCAL

Gestión de endpoints, descubrimiento y control de agentes locales en Windows.

REGISTRO DE AGENTES: FUENTE ÚNICA DE VERDAD

INVENTARIO COMPLETO

Metadatos de agentes gestionados, shadow AI, registrados manualmente. Alimenta toda la pila de seguridad.

COMPONENTES FUNCIONALES PRINCIPALES

- **REGISTRO** — Vista completa
- **CONTROL DE ACCESO** — Incorporar y limitar
- **VISUALIZACIÓN** — Explorar conexiones
- **INTEROPERABILIDAD** — Work IQ, Apps, Datos
- **SEGURIDAD** — Proteger frente amenazas

NIVEL 3: SOPORTE Y DESPLIEGUE

REQUISITOS DE LICENCIAMIENTO

Licencia por usuario (M365 E7 o Agent 365). Agentes no requieren licencia.

PRERREQUISITOS RECOMENDADOS

Entra P1/P2, Entra Suite, Purview DLP para capacidades completas.

MODELO DE DESPLIEGUE

Servicio SaaS integrado en M365. Sin infraestructura adicional. Integración automática con Copilot Studio, Foundry.

@SCavanna

OBSERVABILIDAD: VISIBILIDAD TOTAL DE LA FLOTA DE AGENTES (03/18)

ARQUETIPO: Analítico / Jerárquico | **DASHBOARD DE MÉTRICAS:** Telemetría en tiempo real para insights procesables, rendimiento y gobernanza.

NIVEL 1: CORE · VISIÓN ESTRATÉGICA

AGENTES PLATAFORMA
(Foundry, Copilot Studio, Agent Builder)
- Compatibilidad integrada

FLUJO DE DATOS 1.7 GB/s
FLUJO DE DATOS 5.1 GB/s
1.4 GB/s
FLUJO DE DATOS 1.2 GB/s
1.2 GB/s
FLUJO DE DATOS 1.2 GB/s
1.6 GB/s

AGENT 365: PANEL DE CONTROL DE OBSERVABILIDAD UNIFICADO
Recopilación de telemetría en tiempo real de todos los agentes.
Transforma datos en insights procesables para supervisión de TI y seguridad.

FLUJO DE DATOS 1.8 GB/s
FLUJO DE DATOS 1.2 GB/s
1.2 GB/s
FLUJO DE DATOS 1.5 GB/s
1.4 GB/s
FLUJO DE DATOS 1.5 GB/s
1.9 GB/s

AGENTES PERSONALIZADOS / TERCEROS
- Integración explícita SDK

Estratégico: Transparencia completa y responsabilidad del ciclo de vida.

NIVEL 2: CONCEPTOS CLAVE · TELEMETRÍA Y ANÁLISIS CONVERGENTE

1. TELEMETRÍA BASADA EN OPENTELEMETRY

Ejecuciones
Uso de Herramientas
Llamadas de Modelo
Latencia
Errores

OpenTelemetry

AGENT 365: REPOSITORIO ESTÁNDAR ABIERTO
Instrumentación estándar abierta para capturar lo ocurrido durante una acción o sesión del agente.
SDKs con auto-instrumentación (Python, Node.js, .NET).

Ámbitos: InvokeAgentScope, ExecuteToolScope, InferenceScope, OutputScope

2. PANEL CENTRALIZADO DE MÉTRICAS

TENDENCIA DE USO (30 DÍAS)
ERRORES POR AGENTE

Insights procesables: Supervisión de rendimiento y salud general de la flota.
Dashboard de observabilidad en M365 Admin Center para administradores de TI. Instantánea de actividad, identificación de riesgos y brechas de gobernanza. Aprobación de solicitudes pendientes y administración de agentes sin propietarios.

3. INTEGRACIÓN CON SEGURIDAD Y CUMPLIMIENTO

ALIMENTACIÓN DEFENDER: ANÁLISIS DE SEGURIDAD Y DETECCIÓN DE AMENAZAS

ALIMENTACIÓN PURVIEW: SUPERVISIÓN DE CUMPLIMIENTO Y AUDITORÍA
Uso de datos pertinentes de actividad para escenarios de investigación y auditoría. Telemetría como insumo primario para detección y cumplimiento.

4. MÉTRICAS DE IMPACTO EMPRESARIAL

RETORNO DE INVERSIÓN (ROI)
Ahorro de tiempo
Calidad interacción
Menor costo por notificación
Procesamiento más rápido
ACTIVIDAD DEL AGENTE

De la telemetría al valor: Medición del impacto y ROI en tiempo real.
Observabilidad proporciona información útil sobre productividad. Vinculación de acciones específicas a resultados empresariales medibles con inteligencia de procesos (ej. Celonis).

NIVEL 3: SOPORTE Y CONEXIONES · FLUJO Y CONTROL

SOPORTE DE RECOPILACIÓN

INICIO DE RECOPILACIÓN
Prueba o Licencia + Términos de Uso. No se almacenan datos antes.

DATOS RECOPILADOS
Ejecuciones, Uso de herramiantas, Tiempo, Errores, Identificadores de inquilino, agente y usuario. Control de datos para terceros.

CONEXIONES EXTERNAS

- **BLOQUE 5: SEGURIDAD** (Detección de amenazas)
- **BLOQUE 11: CUMPLIMIENTO** (Auditoría)
- **BLOQUE 17: ROI** (Métricas de valor)
- **BLOQUE 15: SDK/CLI** (Instrumentación técnica)

@SCavanna

GOBERNANZA PROACTIVA A ESCALA EMPRESARIAL (04/18)

Directivas centralizadas, mínimo privilegio, automatización de controles de ciclo de vida y preparación para auditoría. | ARQUETIPO: Editorial / Modular (Bento Box)

NIVEL 1: CORE · MARCO DE GOBERNANZA EQUILIBRADO

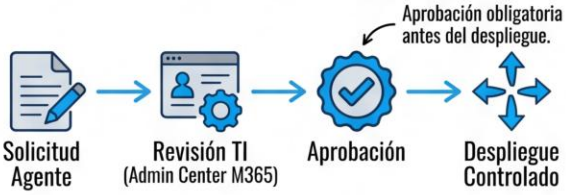
Agent 365 establece un marco que equilibra la libertad de innovación con la supervisión centralizada. Asegura que cada agente opere dentro de límites definidos desde el día uno.

La gobernanza implica directivas, configuración y acciones para controlar acceso, publicación y administración, garantizando seguridad y cumplimiento de datos.

NIVEL 2: CONCEPTOS CLAVE

1. INCORPORACIÓN CONTROLADA DESDE EL DÍA CERO

Onboarding intencional con supervisión de TI



Las organizaciones ponen agentes bajo control desde el primer día con flujo de aprobación de TI. Aplicación de plantillas de directiva para gobernanza y cumplimiento. Agentes con identidad propia requieren aprobación del administrador.

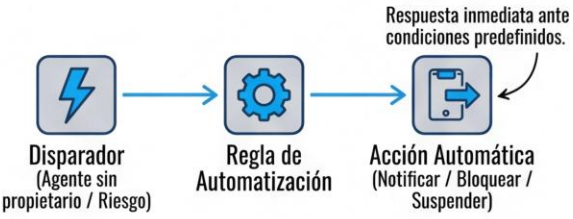
2. ACCESO CON MÍNIMO PRIVILEGIO

Least Privilege para agentes

Control de qué usuarios, datos y herramientas pueden usar los agentes. Límite de acceso solo a los recursos necesarios para prevenir exposición innecesaria por agentes sobrepermisados.

3. AUTOMATIZACIÓN DE CONTROLES DE CICLO DE VIDA

Reglas de administración basada en eventos



Administración de agentes basada en reglas para aplicar automáticamente directivas de ciclo de vida. Reduce carga manual de TI y asegura respuesta inmediata ante condiciones predefinidas.

4. PREPARACIÓN PARA AUDITORÍA

Audit readiness integrada

Visibilidad mejorada sobre uso y funcionamiento de agentes para seguridad, cumplimiento y fiabilidad. Controles permiten detectar, retener e investigar interacciones no éticas.

NIVEL 3: SOPORTE · DESAFÍOS Y CONEXIONES EXTERNAS

DESAFÍOS ORGANIZACIONALES

Aplicar directivas coherentes, equilibrar libertad de desarrolladores con supervisión, identificar y retirar agentes de bajo valor/riesgo. Agent 365 aborda esto con su enfoque integrado.

CONEXIONES EXTERNAS (Ecosistema)

@SCavanna

SEGURIDAD INTEGRAL Y PROTECCIÓN EN TIEMPO REAL (05/18)

Defensa en profundidad para agentes: identidad, DLP, detección de amenazas con Defender, controles de red y aislamiento. | ARQUETIPO: Técnico / Despiece

NIVEL 1: CORE · DEFENSA EN PROFUNDIDAD EXTENDIDA

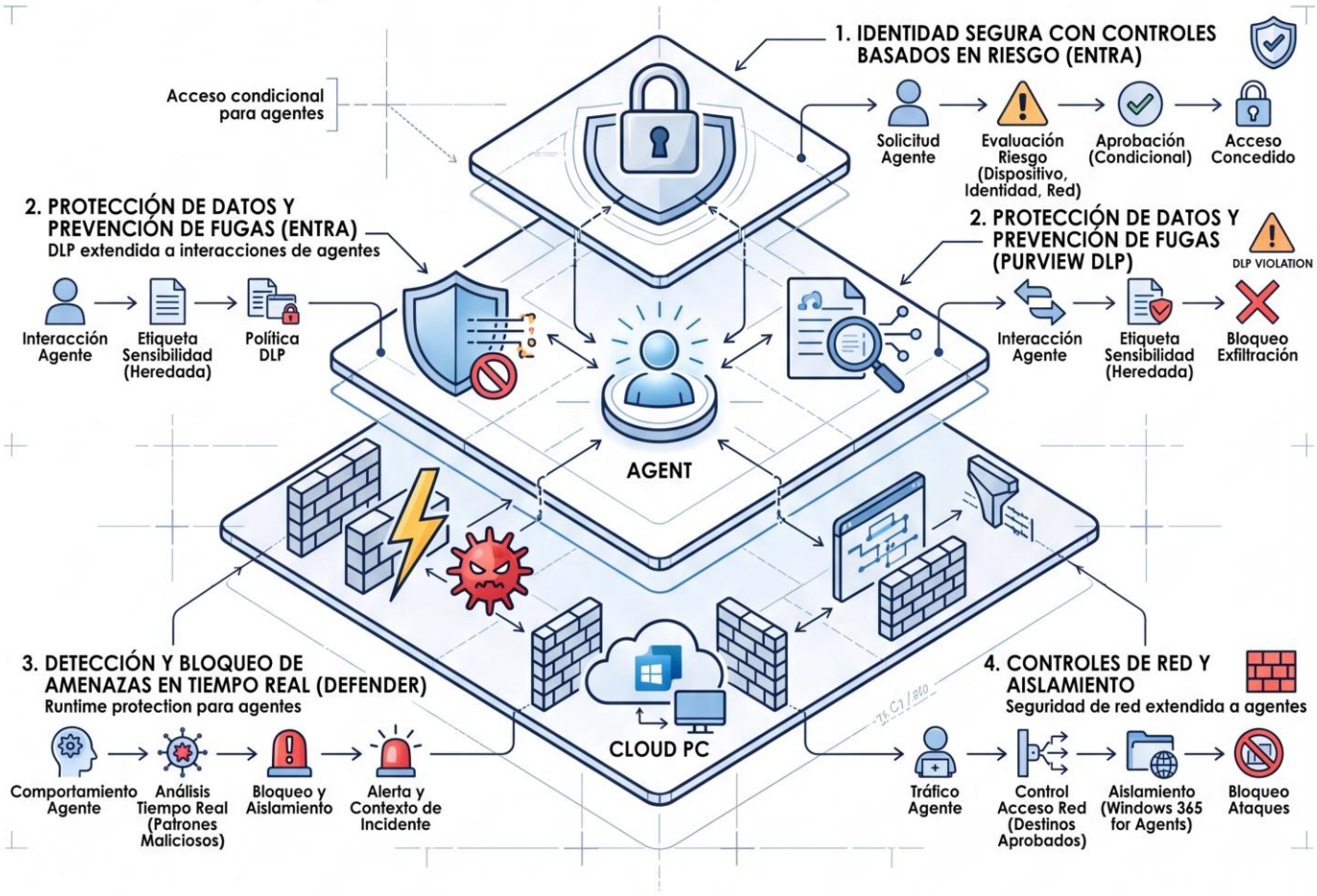
MICROSOFT ENTRA
Controles de acceso basados en riesgo, identidad segura.

MICROSOFT PURVIEW
Visibilidad profunda de riesgos de datos, DLP, etiquetas de sensibilidad.

MICROSOFT DEFENDER
Detección continua y bloqueo de amenazas en tiempo real.

Agent 365 extiende la defensa en profundidad de Microsoft al mundo de los agentes autónomos, garantizando que cada agente solo acceda a recursos autorizados, evite la pérdida de datos y esté protegido contra amenazas en constante evolución.

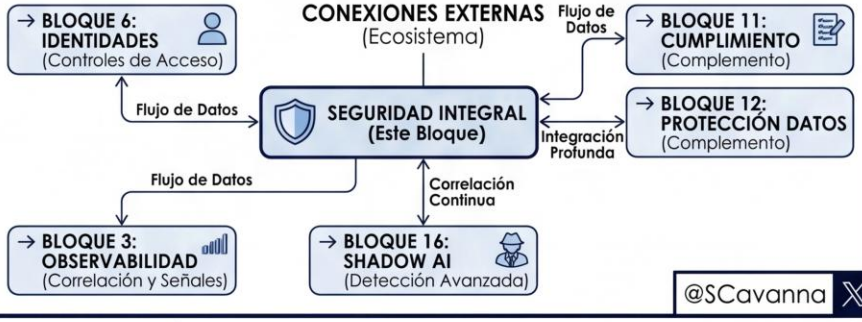
NIVEL 2: CONCEPTOS CLAVE (DIAGRAMA DE CAPAS DE SEGURIDAD)



NIVEL 3: SOPORTE · INTEGRACIÓN, OBSERVABILIDAD Y CONEXIONES EXTERNAS

INTEGRACIÓN CON OBSERVABILIDAD (BLOQUE 3)

La seguridad se integra con la observabilidad para correlacionar señales. Defender analiza telemetría para identificar anomalías y reducir la exposición. A partir de junio de 2026, Defender proporcionará mapeo de contexto de activos para cada agente (dispositivos, identidades, recursos) para evaluar el radio de explosión.



@SCavanna

IDENTIDAD DE AGENTE: MICROSOFT ENTRA AGENT ID (06/18)

Fundamento de identidad corporativa para agentes, modelos delegado vs autónomo, acceso condicional y patrocinadores. | ARQUETIPO: Sistémico / Relacional

NIVEL 1: CORE - IDENTIDAD CORPORATIVA CENTRALIZADA

MICROSOFT ENTRA AGENT ID

Cada agente de IA recibe una identidad corporativa formal a través de Microsoft Entra Agent ID, convirtiéndose en un "ciudadano de primera clase" dentro del directorio de la organización, sujeto a la las mismas políticas de acceso y ciclo de vida que los usuarios humanos.

Registro Unificado y Gestión Segura por Defecto

NIVEL 2: CONCEPTOS CLAVE

1 MODELOS DE IDENTIDAD: DELEGADO VS AUTÓNOMO

AGENTE DELEGADO (OBO)

Trabaja en nombre de usuarios.
Usa tokens OBO (On-Behalf-Of).
Permisos del patrocinador.

AGENTE AUTÓNOMO (Acceso Propio)

Opera con sus propias credenciales y permisos.
Entra Agent ID independiente.

Disponibilidad General.
Flujos de trabajo de equipo (Preview) en desarrollo.

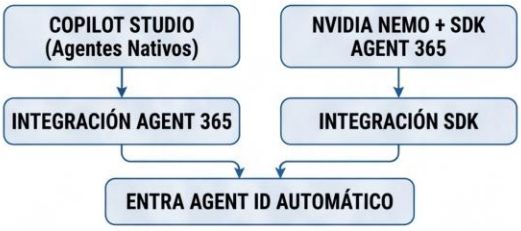
2 PATROCINIO Y ASIGNACIÓN DE PROPIETARIOS

Gestión segura incluye asignación de propietario/patrocinador para ciclo de vida (incorporación, monitoreo, retiro) y acceso condicional. Sin Agent ID, la gobernanza es limitada.

3 ACCESO CONDICIONAL EXTENDIDO A AGENTES

Políticas basadas en riesgo.
ID Protection monitorea comportamiento.
Microsoft Sentinel ingiere actividad para SOC.

4 APROVISIONAMIENTO AUTOMÁTICO



Agentes compilados e implementados se aprovisionan automáticamente con una identidad de agente Entra.
Registro y telemetría automáticos.

NIVEL 3: SOPORTE - DESAFÍOS Y CONEXIONES EXTERNAS

DESAFÍOS ORGANIZACIONALES & INSIGHTS

La identidad Entra es el FUNDAMENTO para Gobernanza (Bloque 4) y Seguridad (Bloque 5).

Desafío: Correlación de identificadores entre registros (Purview, Agent 365, Entra ID).
Equipos de producto trabajan en unificación.

Sin un Agent ID, el agente es invisible para auditoría y control.

CONEXIONES EXTERNAS (Ecosistema)

Prerrequisito para gobernanza y seguridad. Amplía capacidades con SDK y permite identidad en agentes externos.

CICLO DE VIDA DEL AGENTE: DE LA CREACIÓN AL RETIRO (07/18)

Incorporación controlada, operación supervisada, reasignación de propiedad y baja planificada. | ARQUETIPO: Secuencial / Narrativo (Roadmap)

NIVEL 1: CORE · MARCO DE GOBERNANZA DEL CICLO DE VIDA

learn.microsoft.com

Cada agente de IA sigue un ciclo de vida gestionado —desde la incorporación intencional hasta la baja planificada— bajo la supervisión de Agent 365, asegurando que ningún agente se crea, opera o elimina sin controles adecuados. Garantiza adopción coherente y segura desde la compilación hasta la retirada.

[microsoft-agent-365 | PDF]

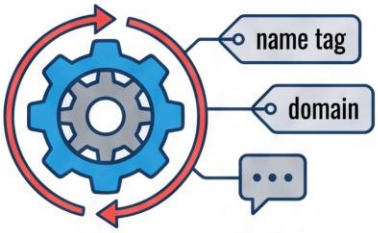
NIVEL 2: CONCEPTOS CLAVE

1. SOLICITUD Y APROBACIÓN CONTROLADA

[microsoft-agent-365 | PDF]

Flujo de incorporación intencional. Usuario solicita instancia, administrador aprueba en Centro de administración de M365, asigna licencias y directivas. Punto de control formal antes del despliegue.

2. APROVISIONAMIENTO Y CONFIGURACIÓN



Setup automatizado del agente. Configuración de icono, nombre, alias, dominio. Comunicación vía Teams y aparición en organigrama bajo supervisión del creador.

[microsoft-agent-365 | PDF]

3. OPERACIÓN SUPERVISADA Y MANTENIMIENTO

Monitoreo continuo durante la operación. Agent 365 monitorea actividad (Bloque 3), aplica directivas (Bloque 4) y detecta anomalías (Bloque 5). Administradores ejecutan acciones de gobernanza.

4. RETIRO CONTROLADO Y RETENCIÓN

[microsoft-agent-365 | PDF]

Bloqueo pausa el agente. Eliminación permanente no se puede deshacer. Recursos asociados permanecen 30 días post-eliminación para recuperación y auditoría.

NIVEL 3: SOPORTE · AGENTES HUÉRFANOS Y CONEXIONES EXTERNAS

AGENTES HUÉRFANOS

Detección proactiva de agentes sin propietario (usuario eliminado). Centro de administración permite identificar y reasignar/retirar. Plantillas definen funcionalidades y cumplimiento.

[microsoft-agent-365 | PDF]

CONEXIONES EXTERNAS (Ecosistema)

AGENTES HUÉRFANOS (Este Bloque)

→ **BLOQUE 4: GOBERNANZA** (Operacionaliza políticas)

→ **BLOQUE 10: ROLES** (Requiere roles para aprobación/retiro)

→ **BLOQUE 8: REGISTRO** (Se ejecuta desde el registro)

REGISTRO CENTRALIZADO DE AGENTES (08/18)

Inventario unificado multiplataforma: filtros, acciones administrativas y visibilidad de agentes gestionados y no gestionados. | ARQUETIPO: Analítico / Jerárquico

NIVEL 1: CORE · CENTRO DE ADMINISTRACIÓN UNIFICADO

SEGURIDAD Y GOBERNANZA

OBSERVABILIDAD TOTAL

El Registro de Agent 365 centraliza en un solo lugar la lista completa de todos los agentes de IA en la organización, proporcionando el inventario dinámico que habilita toda la gobernanza, seguridad y observabilidad de la plataforma.

Visibilidad centralizada de todos los agentes disponibles para la organización.
[microsoft-agent-365 | PDF]

NIVEL 2: CONCEPTOS CLAVE

1. TIPOS DE AGENTES CLASIFICADOS
(Taxonomía del inventario)

AGENTES DE MICROSOFT	AGENTES EXTERNOS DE ASOCIADOS	PUBLICADOS POR SU ORGANIZACIÓN (LOB)	COMPARTIDOS POR CREADOR
Creados y mantenidos por Microsoft.	Desarrolladores de confianza.	Agentes personalizados aprobados.	Creados por usuarios individuales.

[microsoft-agent-365 | PDF]

2. MÉTRICAS DEL REGISTRO
(Indicadores clave)

TOTAL DE AGENTES	AGENTES SIN PROPIETARIOS	AGENTES NO ADMINISTRADOS
1540	42	12
Disponibles en el inquilino.	Ya no tienen propietarios.	Sin protección de Agent 365.

[microsoft-agent-365 | PDF]

3. FILTROS AVANZADOS
(Navegación inteligente)

ESTADO · TIPO DE PUBLICADOR · CANAL · PLATAFORMA · ORIGEN DE DATOS

Filtrar por estado, tipo, canal (Copilot, Teams, Outlook, Apps M365, SharePoint), plataforma de creación y origen de conocimiento.

[microsoft-agent-365 | PDF]

4. ACCIONES ADMINISTRATIVAS
(Operaciones directas)

- REFRESH (Actualizar vista)
- EXPORT (Exportar a CSV)
- AGREGAR AGENTE (Cargar manifiesto .zip)
- ADMINISTRACIÓN DE ANCLADOS (Prioridad)
- PERSONALIZAR VISTA
- BÚSQUEDA

Operaciones directas sobre la lista y agentes individuales.

[microsoft-agent-365 | PDF]

NIVEL 3: SOPORTE · RESTRICCIONES Y CONEXIONES EXTERNAS

RESTRICCIONES Y USO

Filtros de uso y observabilidad limitados a inquilinos con <4.000 agentes.

Uso basado en actividad de informes de Agent 365.

[microsoft-agent-365 | PDF] [Microsoft...Field FAQ]

CONEXIONES EXTERNAS (Ecosistema)

BASE OPERATIVA: BLOQUES 3, 4, 5

→ ALIMENTA BLOQUE 9: MAPA DE AGENTES (Datos de inventario)

→ EJECUTA BLOQUE 7: CICLO DE VIDA

→ SINCRONIZA BLOQUE 14: AGENTES EXTERNOS

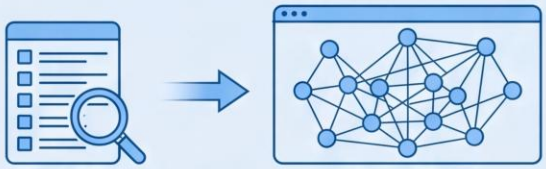
→ FUENTE ÚNICA DE VERDAD PARA: Entra (Identidad), Defender (Protección), Purview (Seguridad de datos).

@SCavanna

MAPA DE AGENTES E INTERCONEXIONES (09/18)

Visualización relacional tipo grafo: clústeres por plataforma, indicadores de riesgo y acciones directas desde la vista gráfica. || ARQUETIPO: Sistémico / *Relacional*

NIVEL 1: CORE · TRANSFORMACIÓN RELACIONAL



INVENTARIO TABULAR
(Plano)
Lista plana, dependencias invisibles.

MAPA VISUAL
(Sistémico)
Filtros · Exportación · Navegación

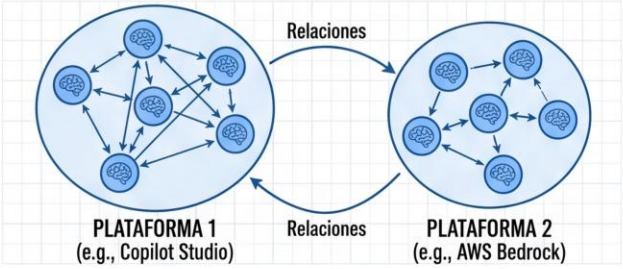
El Mapa de agentes transforma el inventario tabular en una visualización relacional que revela dependencias, concentraciones y patrones de riesgo invisibles en una lista plana. Ofrece una vista visual de las relaciones, dependencias e interacciones de los agentes con datos, herramientas y otros agentes. Incluye filtros por estado, publicador, canal, origen de datos y uso; permite exportación y controles de navegación.

Insight de Autor: Esta perspectiva sistémica es imposible de obtener desde una vista tabular. (Architects Daughter font)

NIVEL 2: CONCEPTOS CLAVE

1. AGRUPAMIENTO VISUAL POR CLÚSTERES

Cartografía del ecosistema agencial

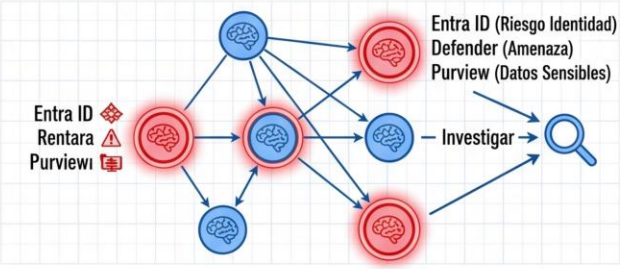


Los nodos se agrupan por plataforma de creación o categoría funcional, revelando la composición y distribución del ecosistema. Filtros disponibles: riesgo, propietario, uso. Acciones directas: asignar propietario, bloquear, instalar o anclar.

Filtros: Riesgo, Propietario, Uso · Acciones: Asignar, Bloquear, Instalar

2. INDICADORES DE RIESGO SUPERPUESTOS

Mapa de calor de riesgos agenciales



Agentes con riesgos de alta gravedad se resaltan visualmente mediante una columna de Riesgos que muestra información procedente de Entra, Defender y Purview, con acciones de mitigación como bloquear o investigar.

Priorizar Investigación · Mitigación Directa

3. PANEL DE DETALLES DEL AGENTE

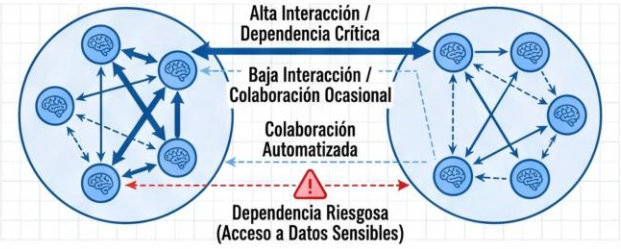
Ficha contextual del agente

Al seleccionar un agente, se despliega un panel flotante con pestañas para investigar, actuar y documentar sin cambiar de contexto. Muestra información completa sobre el agente seleccionado.

Investigar y Actuar en Contexto

4. EXPLORACIÓN DE CONEXIONES AGENT-TO-AGENT

Mapeo de interacciones entre agentes



Las conexiones bidireccionales entre agentes revelan patrones de colaboración automatizada o dependencias potencialmente riesgosas. Permite identificar dependencias complejas entre agentes.

Colaboración · Dependencias · Riesgos Inter-agente

NIVEL 3: SOPORTE · DESAFÍOS Y CONEXIONES EXTERNAS

DESAFÍOS ORGANIZACIONALES & LIMITACIONES

El mapa complementa al Registro (Bloque 8) aportando la dimensión relacional.
Para inquilinos grandes, los filtros de uso solo están disponibles con menos de 4.000 agentes.
Permite a líderes entender *cómo se relacionan* los agentes entre sí y con los activos de la organización, no solo *qué* agentes existen.

CONEXIONES EXTERNAS

(Ecosistema)

"@SCavanna"

ROLES, PERMISOS Y SEGREGACIÓN DE FUNCIONES (10/18)

Modelo RBAC de Agent 365: quién puede ver, quién puede actuar y cómo se aplica el principio de mínimo privilegio administrativo. | ARQUETIPO: Analítico / Jerárquico (Matriz)

NIVEL 1: CORE · MODELO RBAC GRANULAR Y SEGREGACIÓN DE FUNCIONES

Agent 365 implementa un modelo RBAC granular donde solo dos roles tienen autoridad para modificar y aprobar agentes, mientras que otros roles proporcionan visibilidad sin capacidad de acción, protegiendo contra la concentración de privilegios.

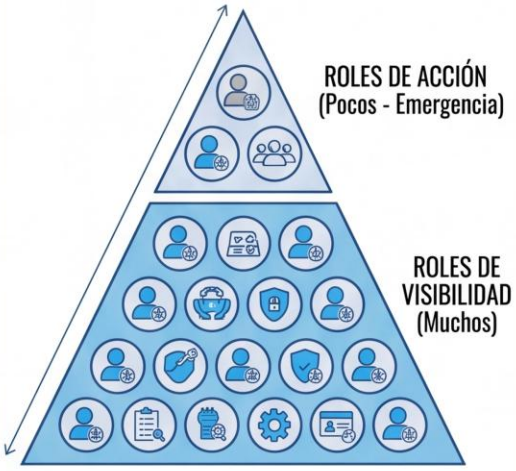
El acceso a la administración en Centro de administración de Microsoft 365 se controla mediante roles de Microsoft Entra. [learn.microsoft.com]

NIVEL 2: CONCEPTOS CLAVE · MATRIZ DE PERMISOS Y PRINCIPIO DE MÍNIMO PRIVILEGIO

ROL (Microsoft Entra)	CAPACIDAD 1: Visualizar Info Org	CAPACIDAD 2: Visualizar Registro Agente	CAPACIDAD 3: Instalar, Modificar, Aprobar y Administrar
ROLES CON AUTORIDAD DE GOBERNANZA COMPLETA			
Administrador global	✓	✓	✓
Administrador de IA	✓	✓	✓
Únicamente estos roles tienen capacidad para realizar acciones de gobernanza y visibilidad completa en todo el inquilino.			
ROLES CON VISIBILIDAD PERO SIN ACCIÓN			
Lector global	✓	✓	✗
Lector de inteligencia artificial	✓	✓	✗
Administrador de seguridad	✓	✓	✗
Lector de seguridad	✓	✓	✗
Operador de seguridad	✓	✓	✗
Lector de informes	✓	✓	✗
Admin. éxito exp. usuario	✓	✓	✗
ROLES DE ALCANCE LIMITADO			
Admin. específico producto (ej. Power Platform, Fabric)	✓	✗	✗
Admin. cuentas usuario	✓	✗	✗

Roles pueden visualizar información y Registro, pero NO pueden instalar, modificar, aprobar ni administrar configuraciones.

PRINCIPIO DE MÍNIMO PRIVILEGIO ADMINISTRATIVO



Se recomienda usar y asignar roles con los permisos más mínimos para realizar tareas. El administrador global debe limitarse a escenarios de emergencia.

NIVEL 3: SOPORTE · SEGREGACIÓN DE FUNCIONES Y CONEXIONES EXTERNAS

SEGREGACIÓN PARA CISOs

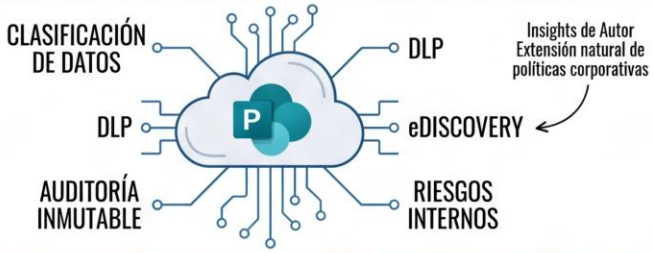
La segregación de funciones es fundamental para CISOs: permite que los equipos de seguridad tengan visibilidad completa sin riesgo de modificaciones accidentales, mientras que las acciones de alto impacto requieren roles específicos con mayor responsabilidad. Roles IRM en Purview son necesarios para alertas de Insider Risk Management. [PDF]

CONEXIONES EXTERNAS (Ecosistema)

CUMPLIMIENTO NORMATIVO Y AUDITORÍA CON MICROSOFT PURVIEW (11/18)

DLP, etiquetas de sensibilidad, DSPM para IA, auditoría inmutable, eDiscovery y administración de riesgos internos aplicados a agentes. | ARQUETIPO: Editorial / Modular (Bento Box)

NIVEL 1: CORE · MARCO DE CUMPLIMIENTO INTEGRAL PARA AGENTES



Microsoft Purview extiende a los agentes de IA todo su arsenal de cumplimiento corporativo —clasificación de datos, DLP, auditoría inmutable, eDiscovery y gestión de riesgos internos— asegurando que las interacciones agenciales son tan trazables y controlables como las de cualquier usuario humano.

Agent 365 extiende capacidades de Microsoft Purview para proporcionar seguridad de datos y cumplimiento de extremo a extremo para interacciones de agentes, abarcando escenarios agent-to-user, agent-to-agent y agent-to-tool.

NIVEL 2: CONCEPTOS CLAVE

1. DSPM PARA IA
(Gestión de Postura de Seguridad de Datos)

Gestión de postura de seguridad de datos para agentes.
Purview DSPM para IA identifica y mitiga riesgos de exposición en las interacciones de agentes. Permite revisar la actividad relacionada con contenido que contiene información confidencial a través del Explorador de actividades. La observabilidad de la inteligencia artificial proporciona una vista centralizada de la actividad del agente en toda la organización.

OBSERVABILIDAD IA → VISTA CENTRALIZADA → IDENTIFICACIÓN DE RIESGOS

2. DLP EXTENDIDO A AGENTES
(Prevención de Pérdida de Datos Agencial)

Prevención de pérdida de datos agencial.
Las políticas de Data Loss Prevention se aplican a las interacciones de los agentes, previniendo el uso inseguro de datos. Las etiquetas de sensibilidad son heredadas y aplicadas en interacciones de agentes. Esto incluye la integración con Power Platform DLP para gobernanza ampliada.

INTERACCIÓN AGENTE → DLP CHECK → BLOQUEO / CIFRADO

3. AUDITORÍA INMUTABLE
(Registros de Auditoría para Acciones de Agentes)

Registros de auditoría para todas las acciones de agentes
Los registros completos de auditoría cubren interacciones de agentes, eventos de ciclo de vida y uso de datos. Los eventos de IA son capturados en registros de auditoría, y los controles de seguridad detectan interacciones dañinas o no conformes. Purview Audit proporciona logging inmutable y búsquedo de actividad para identidades humanas y no humanas en el ecosistema Microsoft 365 y Azure.

EVENTO IA → REGISTRO AUDITORÍA → ALMACENAMIENTO INMUTABLE

4. GESTIÓN DE RIESGOS INTERNOS Y eDISCOVERY
(Investigación y Detección de Comportamiento Anómalo)

Investigación y detección de comportamiento anómalo
Purview extiende la administración de riesgos internos y eDiscovery a las interacciones de agentes, permitiendo detectar y prevenir comportamiento riesgoso o dañino con indicadores específicos para agentes, y aplicar políticas para bloquear acciones inseguras o acceso a datos. Las políticas de retención y ciclo de vida gestionan los datos generados por agentes conforme a los requisitos regulatorios.

ANÁLISIS DE COMPORTAMIENTO → DETECCIÓN ANOMALÍA → ACCIÓN CORRECTIVA

NIVEL 3: SOPORTE · DESAFÍOS Y CONEXIONES EXTERNAS

DESAFÍOS ORGANIZACIONALES

El cumplimiento agencial es especialmente relevante en sectores regulados (finanzas, salud, gobierno) donde las auditorías son frecuentes y los requisitos de trazabilidad son estrictos. La integración con Purview asegura que las organizaciones puedan realizar investigaciones forenses sobre la actividad de agentes con el mismo rigor que aplican a la actividad de empleados.

Agent 365 se basa en servicios auditados que cuentan con certificaciones SOC, ISO, FedRAMP, HIPAA y PCI DSS.

[learn.microsoft.com]

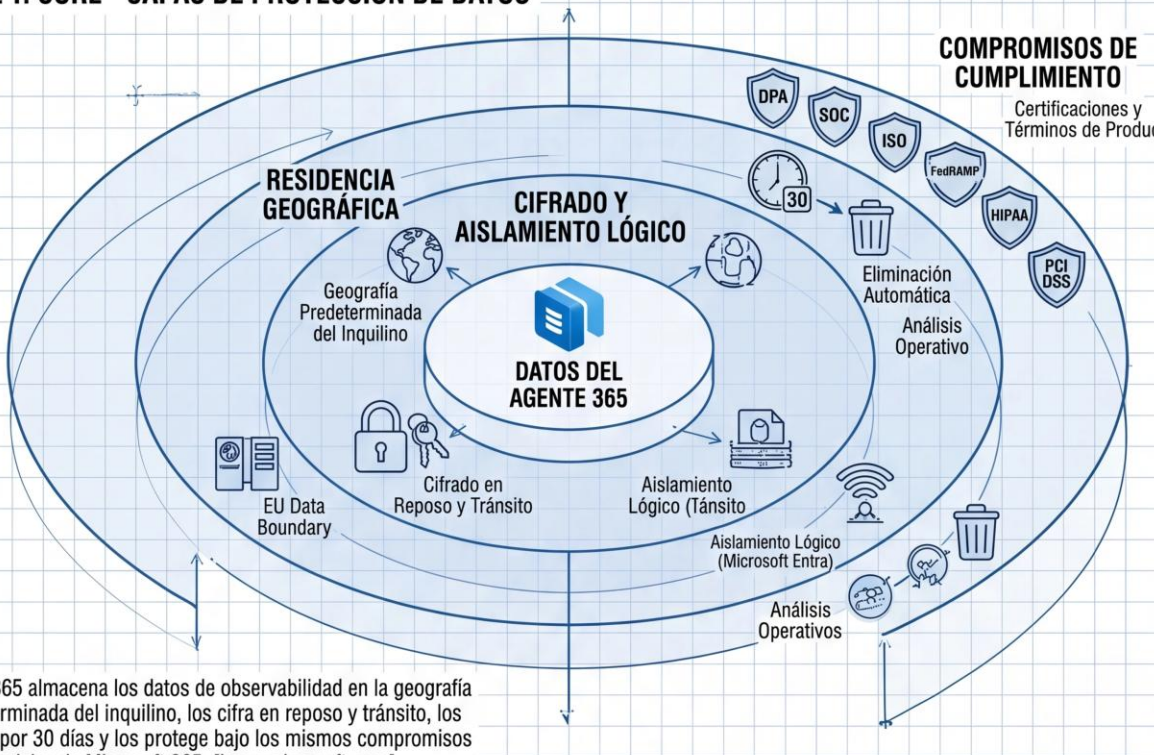
CONEXIONES EXTERNAS (Ecosistema)

@SCavanna

PROTECCIÓN DE DATOS, RESIDENCIA Y RETENCIÓN (12/18)

Geografía de almacenamiento, cifrado, retención de 30 días, compromisos de cumplimiento (DPA, SOC, ISO) y límites de datos de la UE. | **ARQUETIPO:** Técnico / Despiece (Exploded View)

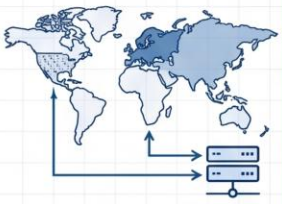
NIVEL 1: CORE - CAPAS DE PROTECCIÓN DE DATOS



Agent 365 almacena los datos de observabilidad en la geografía predeterminada del inquilino, los cifra en reposo y tránsito, los retiene por 30 días y los protege bajo los mismos compromisos empresariales de Microsoft 365. [learn.microsoft.com]

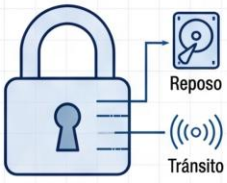
NIVEL 2: CONCEPTOS CLAVE

1. RESIDENCIA DE DATOS GEOGRÁFICA



Nombre: Almacenamiento en la geografía del inquilino.
Explicación: La selección del país/región al crear el inquilino define la geografía de almacenamiento. Ciertos datos pueden replicarse (UE para inquilinos UE, EE. UU. para otros). Respeta EU Data Boundary (EUDB). NO admite Advanced Data Residency (ADR). [learn.microsoft.com]

2. CIFRADO Y AISLAMIENTO LÓGICO



Nombre: Protección de datos en reposo y tránsito.
Explicación: Aislamiento lógico mediante Microsoft Entra. Cifrado estándar de Microsoft para datos en reposo y en tránsito. Sin acceso a terceros, anunciantes o servicios no-Microsoft. [learn.microsoft.com]

3. RETENCIÓN DE 30 DÍAS

Nombre: Ventana de retención de telemetría.
Explicación: Los datos de observabilidad se conservan durante 30 días y se eliminan automáticamente. Permite análisis recientes e investigaciones, minimizando acumulación histórica. [learn.microsoft.com]

4. COMPROMISOS DE CUMPLIMIENTO

Nombre: DPA, términos de producto y marcos de certificación.
Explicación: Procesa datos según DPA y Términos de Productos. Funciona sobre servicios Core Online sometidos a auditorías independientes. Microsoft trabaja en la clasificación de Core Online Service para Agent 365. [learn.microsoft.com]

NIVEL 3: SOPORTE - DESAFÍOS Y CONEXIONES EXTERNAS

DESAFÍOS ORGANIZACIONALES

Para agentes personalizados y de terceros, los clientes y desarrolladores deciden qué datos se incluyen mediante la configuración de cómo se instrumenta el agente. Esto otorga a los arquitectos control preciso sobre qué información se comparte con el servicio de observabilidad. La última actualización de esta documentación data del 30/04/2026. [learn.microsoft.com]

CONEXIONES EXTERNAS (Ecosistema)

→ **BLOQUE 11: CUMPLIMIENTO PURVIEW** (Complemento) → **PROTECCIÓN DE DATOS** (Este Bloque) → **BLOQUE 2: ARQUITECTURA** (Decisiones arquitectónicas)

→ **BLOQUE 14: AGENTES EXTERNOS** (Consideración de geografía de datos)

→ Fundamenta las garantías de privacidad para todo el sistema.

INTEGRACIONES NATIVAS: AGENTES DEL ECOSISTEMA MICROSOFT (13/18)

Copilot Studio, Foundry, Agent Builder y plantillas MCP: integración automática con registro, telemetría e identidad Entra. | ARQUETIPO: Secuencial / Narrativo

NIVEL 1: CORE · MARCO DE GOBERNANZA EQUILIBRADO

Los agentes construidos dentro del ecosistema Microsoft se integran automáticamente con Agent 365 —aparecen en el registro, envían telemetría y reciben identidad Entra— sin intervención adicional de desarrolladores o administradores.

NIVEL 2: CONCEPTOS CLAVE

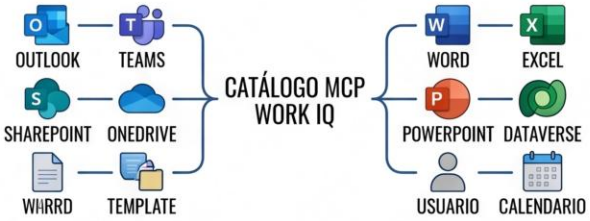
1. Integración automática con Copilot Studio

Zero-touch onboarding para agentes low-code

Agent 365 también ofrece a los desarrolladores SDK y marcos unificados que simplifican el desarrollo, la incorporación y la certificación de agentes integrados personalizados. Las herramientas de agente de Agent 365 exponen interfaces y SDK de MCP coherentes para Outlook, Teams y SharePoint e integraciones empresariales.

2. Herramientas MCP de Work IQ

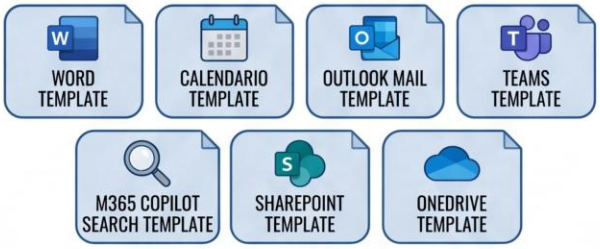
Catálogo de herramientas empresariales para agentes



El catálogo de herramientas de Agent 365 proporciona un amplio conjunto de Work IQ y otros servidores MCP que exponen herramientas seguras y auditables para flujos de trabajo empresariales comunes. Las herramientas de MCP de Work IQ incluyen Copilot, Calendario, Correo, SharePoint, OneDrive, Teams, Usuario, Word y Dataverse/Dynamics 365.

3. Plantillas de agentes predefinidas

Agentes de plantilla listos para desplegar



Los administradores del agente pueden acceder a varios agentes de plantilla diseñados para trabajar con aplicaciones y servicios populares, disponibles como servidores MCP en Microsoft Agent 365.

4. Agente de Desarrollo de Ventas como caso de uso

Ejemplo concreto de agente nativo

El agente de desarrollo de ventas automatiza la difusión de ventas y la administración de clientes potenciales en Microsoft Teams, ayudando a los equipos de ventas a escalar la prospección manteniendo comunicación personalizada.

NIVEL 3: SOPORTE · DESAFÍOS Y CONEXIONES EXTERNAS

DESAFÍOS ORGANIZACIONALES

La integración automática de plataformas Microsoft elimina la fricción de adopción: los agentes heredan seguridad y cumplimiento de nivel empresarial desde su creación. Esto contrasta con los agentes externos (Bloque 14) que requieren integración explícita vía SDK. Las plantillas de directivas predeterminadas incluyen configuraciones para auditoría, DSPM, cumplimiento, protección de identidad, visibilidad de red, ciclo de vida, acceso, permisos y protección en tiempo real.

CONEXIONES EXTERNAS (Ecosistema)

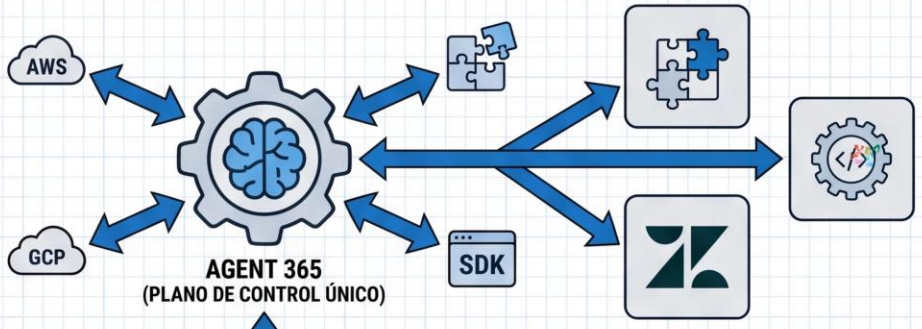
@SCavanna

AGENTES EXTERNOS, TERCEROS Y ECOSISTEMA DE SOCIOS (14/18)

Sincronización del registro con AWS Bedrock y Google Cloud, SDK para agentes personalizados y socios de lanzamiento como **Genspark, Zendesk y Kore.** | **ARQUETIPO:** Sistémico / Relacional

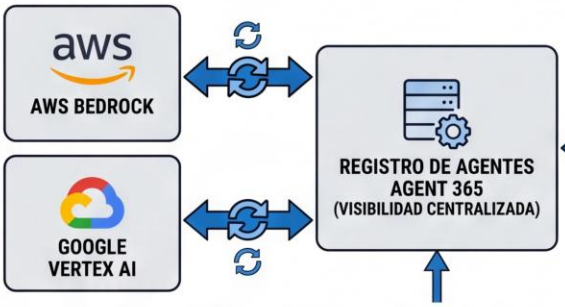
NIVEL 1: CORE · HUB CENTRAL DE GOBERNANZA EXTENDIDA

Agent 365 extiende su gobernanza más allá del ecosistema Microsoft, permitiendo sincronizar registros con AWS Bedrock y Google Cloud, incorporar agentes de socios SaaS preintegrados y conectar agentes personalizados mediante el SDK de Agent 365. Proporciona un único plano de control para llevarlos bajo una administración coherente.



NIVEL 2: CONCEPTOS CLAVE

1. SINCRONIZACIÓN DEL REGISTRO CON NUBES RIVALES



Visibilidad multi-cloud para descubrir, inventariar y gobernar agentes de plataformas externas en un solo lugar.

2. SOCIOS DEL ECOSISTEMA DE LANZAMIENTO

AGENTES LISTOS PARA IMPLEMENTAR

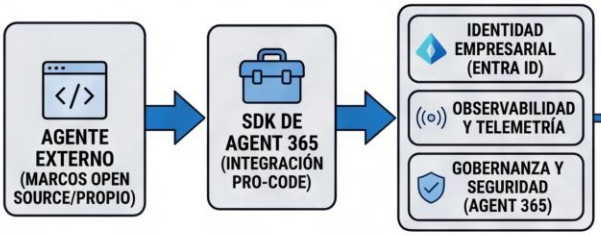
Adobe, box, Canva, celonis, cornerstone, EGNYTE, Figma, Lucid, miro, SOPHOS, Zensai, ZOHO

GENERADORES DE AGENTES (PROVISIÓN AUTOMÁTICA DE ENTRA ID)

coursera, kasisto, kore, Manus, n8n, NVIDIA, ROX, zendesk

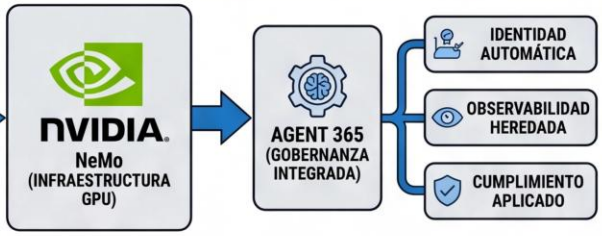
Integraciones preintegradas: despliegue directo o plataformas que crean agentes con identidad regulada.

3. SDK DE AGENT 365 PARA AGENTES PERSONALIZADOS



Permite que agentes existentes obtengan identidad, seguridad y acceso regulado a datos M365 mediante el SDK.

4. EJEMPLO: NVIDIA NEMO



Aprovisionamiento automático de Entra Agent ID para agentes creados en infraestructura acelerada por GPU sin trabajo adicional.

NIVEL 3: SOPORTE · CASOS DE USO Y CONEXIONES EXTERNAS

CASOS DE USO DESTACADOS

- Agentes de socios como Genspark, Zensai, Egnyte y Zendesk completamente habilitados para gestión sin intervención de TI.
- Generadores como Kasisto, Kore y n8n aprovisionan automáticamente Entra Agent ID regulado.

CONEXIONES EXTERNAS (Ecosistema)

HERRAMIENTAS DE DESARROLLO: SDK, CLI Y WORK IQ MCP (15/18)

SDKs multiplataforma, CLI de Agent 365, catálogo de herramientas MCP y flujo de certificación para marketplace. | ARQUETIPO: Técnico / Despiece (Exploded View)

NIVEL 1: CORE · TOOLKIT DE DESARROLLO COMPLETO

SDKs MULTIPLATAFORMA

AGENT 365 TOOLKIT

CLI DE AUTOMATIZACIÓN

WORK IQ MCP (CATÁLOGO)

Agent 365 proporciona a los desarrolladores un toolkit completo —SDKs multiplataforma, CLI de automatización y el catálogo de herramientas Work IQ MCP— para instrumentar agentes con identidad corporativa, telemetría y acceso regulado a datos de Microsoft 365. Simplifica el desarrollo, incorporación y certificación de agentes integrados personalizados.

AGENTES CON IDENTIDAD CORPORATIVA

Instrumentación, Telemetría, Acceso Regulado

NIVEL 2: CONCEPTOS CLAVE

1. SDKS MULTIPLATAFORMA

INSTRUMENTACIÓN MULTILENGUAJE

PYTHON (PyPi) → NODE.JS (npm) → .NET (NuGet)

AGENT 365 TELEMETRÍA (OpenTelemetry)

Soporte para auto-instrumentación (Copilot Studio, LangChain, OpenAI) y manual. Ámbitos definidos (InvokeAgentScope, ExecuteToolScope). Atributos obligatorios (gen_ai.agent.id, microsoft.tenant.id, user.email) para publicación.

2. CLI DE AGENT 365

AUTOMATIZACIÓN DEL CICLO DE VIDA

```
> a365 develop-mcp list-environments
...
...
...
...

> a365 develop-mcp publish
Publicando... [OK]
```

DETECTAR & CONECTAR → AUTENTICAR → PROBAR & VALIDAR → DESPLEGAR

Automatización desde terminal para detectar, conectar, autenticar servidores Work IQ MCP. Comandos para desarrollar, listar entornos, publicar y gestionar el ciclo de vida con trazabilidad integrada.

3. CATÁLOGO WORK IQ MCP

ACCESO REGULADO A DATOS M365

WORK IQ (Inteligencia Organizacional)

MAIL · CALENDAR · TEAMS · SHAREPOINT · ONEDRIVE · WORD · DATAVERSE

GOBERNANZA CENTRALIZADA & SEGURIDAD EMPRESARIAL
Consentimiento Explícito, Auditoría en Entra

Capa de inteligencia con contexto organizacional en tiempo real. Herramientas auditables con permisos visibles y auditables en Entra. Requiere consentimiento explícito por servidor MCP.

4. CERTIFICACIÓN Y PUBLICACIÓN

FLUJO DE MARKETPLACE

DESARROLLO (Configuración Blueprint, managedIdentityPrincipalId) → INSTRUMENTACIÓN (Validación Atributos Telemetría) → VALIDACIÓN (Automatizada & Manual, OpenAPI) → MARKETPLACE (Publicación) → CERTIFICACIÓN MCP (Cumplimiento Continuo, Monitoreo) → VALIDACIÓN (Validición Desarrollizado)

Proceso riguroso para servidores externos. Requiere OpenAPI, autenticación segura, y validación de atributos de telemetría específicos. Configuración definida en el Portal de Desarrolladores.

NIVEL 3: SOPORTE · DIAGNÓSTICO Y CONEXIONES EXTERNAS

DIAGNÓSTICO Y RESOLUCIÓN

Habilitar exportación con variable: `ENABLE_A365_OBSERVABILITY_EXPORTER`

Errores comunes: falta de exportador, problemas de token, atributos de identidad ausentes, errores HTTP (401/403/429/5xx).

Resolución: revisar configuración, permisos (Agent365.Observability.OtelWrite), licencias (M365 E7, Frontier). Guías y repositorios en GitHub.

CONEXIONES EXTERNAS (Ecosistema)

HERRAMIENTAS DE DESARROLLO (Este Bloque)

→ BLOQUE 14: INTEGRACIONES (Materialización técnica) → BLOQUE 6: IDENTIDADES (Asignación programática)

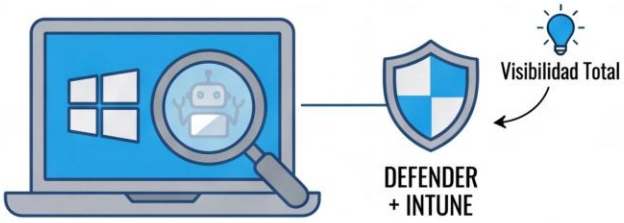
→ BLOQUE 3: TELEMETRÍA (Instrumentación) → BLOQUE 13: CAPACIDADES (Habilitación via MCP)

@SCavanna

SHADOW AI: DETECCIÓN Y BLOQUEO DE AGENTES NO GESTIONADOS (16/18)

Descubrimiento de agentes locales mediante Intune y Defender, bloqueo de OpenClaw, mapeo de radio de explosión y controles basados en políticas. | ARQUETIPO: Secuencial / Narrativo

NIVEL 1: CORE · DETECCIÓN Y REMEDIACIÓN DE SHADOW AI

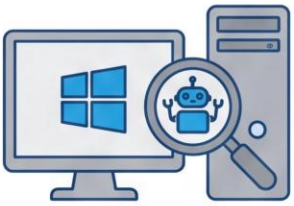


Agent 365 detecta agentes de IA no gestionados ("shadow AI") en dispositivos Windows corporativos mediante Defender e Intune, dando visibilidad sobre su existencia y herramientas para bloquearlos o incorporarlos bajo gobernanza.

NIVEL 2: CONCEPTOS CLAVE · ROADMAP DE DESCUBRIMIENTO Y REMEDIACIÓN

1. DETECCIÓN DE AGENTES LOCALES

Descubrimiento en endpoints Windows



Con Defender e Intune, se descubren y gestionan agentes de IA locales (OpenClaw, GitHub Copilot CLI, Claude Code). Muestra qué agentes y dispositivos los usan. Nueva página Shadow AI en Agent 365.

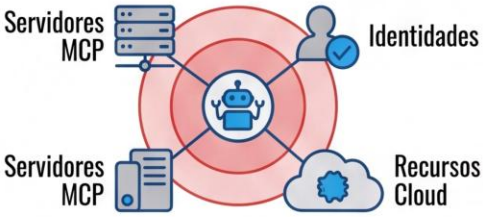
2. PANEL DE SHADOW AI EN ADMIN CENTER

Dashboard centralizado de IA en la sombra

Funcionalidad en vista previa a través del programa Frontier. Página 'Shadow AI' en el Centro de administración de Microsoft 365 como dashboard central para el proceso de descubrimiento.

3. MAPEO DE RADIO DE EXPLOSIÓN (BLAST RADIUS)

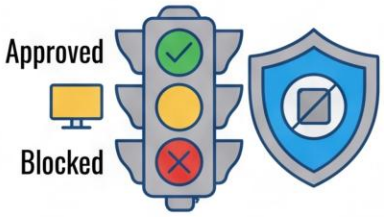
Contexto de activos para evaluar exposición



A partir de junio de 2026, Defender proporciona mapeo del contexto de activos para cada agente (dispositivos, servidores MCP, identidades, recursos cloud) para evaluar exposición y radio de explosión.

4. CONTROLES DE BLOQUEO BASADOS EN POLÍTICAS

Enforcement y remediación



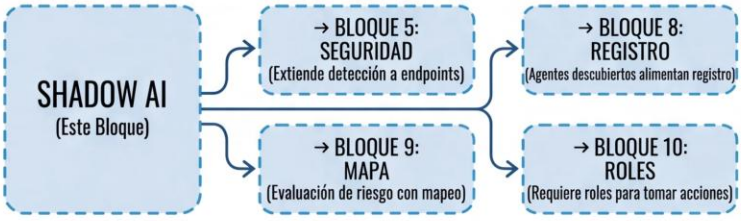
Las organizaciones aplican controles basados en políticas. Defender puede bloquear agentes de codificación en tiempo de ejecución por comportamiento malicioso y generar alertas. Disponibles en vista previa pública en junio de 2026.

NIVEL 3: SOPORTE · DESAFÍOS Y CONEXIONES EXTERNAS

DESAFÍOS ORGANIZACIONALES

La detección de shadow AI responde a una realidad urgente: los agentes han superado la infraestructura de gobernanza diseñada para gestionarlos. Las organizaciones ahora enfrentan un tipo fundamentalmente diferente de expansión: software autónomo que puede invocar herramientas, acceder a datos sensibles y tomar acciones por cuenta propia.

CONEXIONES EXTERNAS (Ecosistema)

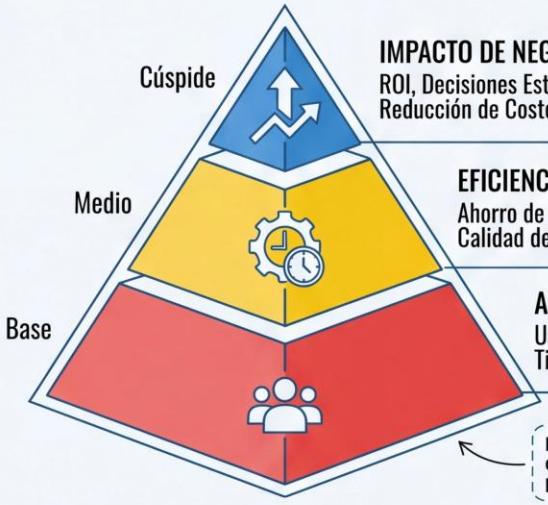


@SCavanna

MEDICIÓN DE VALOR E IMPACTO EMPRESARIAL (17/18)

Métricas de productividad, ROI de agentes, vinculación de acciones con resultados de negocio y análisis de tendencias de adopción.

NIVEL 1: CORE · PIRÁMIDE DE VALOR Y ROI



IMPACTO DE NEGOCIO
ROI, Decisiones Estratégicas, Reducción de Costos, Crecimiento.

EFICIENCIA OPERATIVA
Ahorro de Tiempo, Velocidad de Proceso, Calidad de Interacción, Reducción de Errores.

ADOPCIÓN Y USO
Usuarios Activos, Total de Agentes, Tiempo de Ejecución, Frecuencia de Interacción.

Agent 365 permite medir el impacto real de los agentes de IA en el negocio, vinculando su actividad con indicadores de productividad, ahorro de tiempo y calidad de interacción para justificar inversiones y orientar decisiones estratégicas.

Observabilidad Integrada

La observabilidad proporciona información útil sobre la productividad del agente, el ahorro de tiempo y la calidad de la interacción, permitiendo a los líderes medir el retorno de la inversión. [microsoft-agent-365 | PDF]

NIVEL 2: CONCEPTOS CLAVE

1. MÉTRICAS DE ADOPCIÓN Y USO

Indicadores base de la flota agencial
Instantánea de la actividad del agente en los últimos 30 días, seguimiento de tendencias, total de agentes, usuarios activos, tiempo de ejecución, sincronización de registro, análisis por creadores y plataformas, agentes en riesgo.

Usuarios Activos | Tiempo Ejecución | Total Agentes

[learn.microsoft.com] [micr...pdf | PDF]

2. VINCULACIÓN DE AGENTES CON RESULTADOS DE NEGOCIO

ACCIÓN DEL AGENTE → **MÉTRICAS OPERATIVAS** (Menor costo por notificación, Procesamiento rápido) → **INDICADORES DE NEGOCIO** (Ahorro de costos, Mejores resultados de clientes, ROI Real)

Agent-to-outcome mapping
Al combinar registros de gobernanza de Agent 365 con inteligencia de procesos (ej. Celonis), se vinculan acciones específicas a resultados empresariales medibles. El seguimiento del ROI en tiempo real permite consultar resultados medibles vinculados a agentes específicos. [microsoft-agent-365 | PDF]

3. IDENTIFICACIÓN DE OPORTUNIDADES DE OPTIMIZACIÓN

Next-best-agent opportunity
Los datos de procesos permiten buscar dónde agregar o ajustar un agente ofrece el máximo valor. Esto convierte la medición de valor en una herramienta prospectiva para la planificación estratégica de la flota agencial.
[microsoft-agent-365 | PDF]

4. SUPERVISIÓN ESPECÍFICA POR ROL

TI (Infraestructura)	CISO (Seguridad)	NEGOCIO (Líderes)	RIESGO (Gestión)
• Uptime • Uso de Recursos	• Alertas de Seguridad • Cumplimiento	• ROI • Crecimiento de Ingresos	• Nivel de Riesgo • Incidentes

Vistas diferenciadas para líderes
La supervisión específica del rol amplía esta visibilidad a los líderes empresarialos y de seguridad, asegurando que las partes interesadas tengan la información personalizada para administrar riesgo y medir el valor del agente.
[microsoft-agent-365 | PDF] [Agent 365...for Agents | PowerPoint]

NIVEL 3: SOPORTE · DESAFÍOS Y CONEXIONES EXTERNAS

DESAFÍOS DE JUSTIFICACIÓN

La medición de valor es clave para justificar la inversión en Agent 365 y el ecosistema de agentes. Sin métricas, las iniciativas de IA agencial corren el riesgo de percibirse como gastos sin retorno. Agent 365 cierra esta brecha al integrar la telemetría operativa con indicadores de negocio.

CONEXIONES EXTERNAS (Ecosistema)

→ **BLOQUE 3: OBSERVABILIDAD** (Fuente de Telemetría)
→ **BLOQUE 8: REGISTRO** (Fuente de Métricas de Adopción)
→ **BLOQUE 10: ROLES** (Fuente de Insights por Rol)

→ **MEDICIÓN DE VALOR** (Este Bloque) → **BLOQUE 18: ESTRATEGIA DE ADOPCIÓN** (Toma de Decisiones)

@SCavanna

ESTRATEGIA DE ADOPCIÓN: DE LA VISIBILIDAD AL CONTROL TOTAL (18/18)

Modelo de adopción por fases (inventario, identidad, control avanzado), mejores prácticas y evolución hacia la empresa agencial madura. | ARQUETIPO: Secuencial / Narrativo (S-Pattern)

NIVEL 1: CORE · MARCO DE GOBERNANZA EQUILIBRADO

La adopción de Agent 365 sigue un modelo de madurez progresiva —inventario, identidad, control avanzado— que permite a las organizaciones escalar la gobernanza de agentes de forma realista y con resultados tempranos en cada fase.

Progresa de forma incremental: visibilidad e inventario, luego asignan identidades y gestionan el acceso, y finalmente incorporan aislamiento, control avanzado y visibilidad profunda.

NIVEL 2: CONCEPTOS CLAVE

1. FASE "CRAWL": INVENTARIO Y VISIBILIDAD

Descubrir la flota de agentes.

Obtener visibilidad e inventario completo (nativos, multi-cloud, shadow en endpoints). Habilitar Agent 365 para poblar el Registro y sincronización manual.

Objetivo: ¿cuántos agentes, dónde están y quién los creó?

2. FASE "WALK": IDENTIDAD Y ACCESO

Asignar identidades y gobernar permisos.

Asignar Entra Agent ID y gestionar el acceso como primer paso en gestión del riesgo. Aplicar políticas de acceso condicional y configurar mínimo privilegio. Tratar agentes como entidades gobernadas formalmente.

3. FASE "RUN": CONTROL AVANZADO

Aislamiento, bloqueo en tiempo real y visibilidad profunda.

Capacidades avanzadas: aislamiento Windows 365, bloqueo en tiempo de ejecución con Defender, mapeo de radio de explosión, controles de red extendidos, sincronización con nubes rivales y detección de shadow AI.

4. PROGRAMA FRONTIER COMO ACELERADOR

Acceso anticipado a funcionalidades emergentes.

Participar en características experimentales de IA antes de su disponibilidad general. Requiere licencia Microsoft 365 Copilot o Agent 365 (E7). Habilitado por administrador global.

Complimiente y trasabilidad parantizados.

NIVEL 3: SOPORTE · DESAFÍOS Y CONEXIONES EXTERNAS

PLAZO ESTIMADO: 90 días (aprox.), depende de madurez de seguridad y shadow AI.

SOCIOS DE IMPLEMENTACIÓN: Accenture, KPMG, Capgemini, Protiviti, Slalom, etc. (Agent 365 Launch Partners) para evaluación, enforcement, y gestión.

EVOLUCIÓN CONTINUA: Herramientas deben evolucionar con los agentes. Implementar observabilidad temprano para evitar incidentes sin visibilidad.

CONEXIONES EXTERNAS (Integración del Ecosistema)

ESTRATEGIA DE ADOPCIÓN (Este Bloque)

- FASE 1: INVENTARIO → BLOQUE 3, 8, 9
- FASE 2: IDENTIDAD → BLOQUE 6, 7, 10
- FASE 3: CONTROL AVANZADO → BLOQUE 5, 11, 12, 16
- MEDICIÓN DE VALOR → BLOQUE 17

@SCavanna

1 EL NUEVO PERÍMETRO

Identidades no humanas en la era de la IA agéntica

Zero Trust amplía su alcance: de la identidad humana a todas las entidades que pueden **decidir y actuar** en nombre de la organización.

SERIE: ZERO TRUST EN LA ERA DE LA IA AGÉNTICA — 1 DE 5

2 LA EVOLUCIÓN DEL PERÍMETRO DE CONTROL

RED

El perímetro era la red corporativa.

IDENTIDAD HUMANA

El perímetro pasó a ser la identidad humana.

IDENTIDADES HUMANAS + NO HUMANAS

El perímetro hoy incluye todas las entidades que pueden tomar decisiones o ejecutar acciones organizacionales.

¿POR QUÉ CAMBIA EL PERÍMETRO?

- Agentes y workloads operan con permisos válidos y pueden acceder a sistemas críticos en contextos no previstos.
- La incorporación de agentes amplia la superficie y la complejidad de control.

3 ¿QUÉ HACE A UNA IA AGÉNTICA DIFERENTE DE UN LLM CONVERSACIONAL?

1. **OBJETIVO** — Recibe un objetivo o instrucción.
2. **PLANIFICA** — Descompone el objetivo en pasos.
3. **USA HERRAMIENTAS** — Accede a herramientas, APIs o sistemas.
4. **EJECUTA** — Realiza acciones en nombre de la organización.
5. **OBSERVA** — Obtiene resultados e información.
6. **ADAPTA / ITERA** — Ajusta su plan y repite hasta lograr el objetivo.

Un agente autónomo puede **planificar, usar herramientas, ejecutar e iterar** con mínima o nula intervención humana.

3 LOS TRES PRINCIPIOS DE ZERO TRUST PERMANECEN

VERIFICAR EXPLÍCITAMENTE
Evaluar continuamente la identidad, el contexto, el dispositivo, la postura y el comportamiento.

APLICAR MÍNIMO PRIVILEGIO
Restringir el acceso a datos, herramientas y acciones solo a lo necesario para el propósito.

ASUMIR COMPROMISO
Diseñar para resistir el uso indebido, la manipulación y el movimiento lateral.

Mismos principios. Nuevas entidades. Nuevos límites de confianza.

4 IDENTIDADES: DIFERENCIAS OPERATIVAS

IDENTIDAD HUMANA	IDENTIDAD NO HUMANA
Se autentica con credenciales (ej. MFA).	Se autentica con tokens, API keys o identidades administradas.
Acceso relacionado con rol organizacional.	Acceso asociado a propósito funcional o servicio.
Sesión con inicio y fin definidos.	Ejecución a velocidad de máquina y potencialmente continua.
Credenciales administradas por políticas corporativas.	Secretos o tokens con ciclo de vida propio (rotación, expiración).
Comportamiento humano, variable y observable.	Comportamiento automático; puede actuar sin intervención humana.

EJEMPLOS DE IDENTIDADES

- Agentes autónomos
- Bots y asistentes
- Microservicios
- Pipelines automatizados
- Workloads de IA

Todas deben ser identificadas, gobernadas y protegidas.

5 APLICACIÓN DE ZERO TRUST FOR AI (ZT4AI)

ZT4AI

Extiende Zero Trust al ciclo de vida completo de IA.

Desde los datos y el entrenamiento hasta el despliegue y el comportamiento del agente.

PUNTOS CLAVE DEL CICLO DE VIDA DE IA

1. **Datos** — Ingesta segura y gobierno de datos.
2. **Entrenamiento** — Entornos controlados, integridad del modelo.
3. **Despliegue** — Identidades, permisos y guardrails.
4. **Operación** — Monitoreo de comportamiento del agente.
5. **Mejora Continua** — Aprendizaje seguro, feedback y control adaptativo.

ZT4AI INCLUYE

- ✓ Identidades de agentes y workloads.
- ✓ Controles de acceso y permisos.
- ✓ Protección de datos y modelos.
- ✓ Seguridad de prompts y herramientas.
- ✓ Gobernanza y visibilidad.
- ✓ Detección y respuesta.

6 CAPACIDADES Y RECURSOS DE MICROSOFT PARA OPERACIONALIZAR ZT4AI

MICROSOFT ENTRA AGENT ID

Identidad, acceso, protección y gobernanza de identidades no humanas.

- Creación y administración de identidades de agentes.
- Controles de acceso con Microsoft Entra.
- Gobernanza de ciclo de vida y supervisión.

ZERO TRUST WORKSHOP

Marco guiado para diseñar e implementar controles de Zero Trust para IA.

- Escenarios y patrones de referencia.
- Mapeo de controles y capacidades.
- Priorización de acciones y roadmap.

ZERO TRUST ASSESSMENT

Evalúa tu postura de Zero Trust, incluyendo controles específicos para IA.*

- Evaluación automatizada de configuración.
- Hallazgos y recomendaciones priorizadas.
- Seguimiento de mejora continua.

*Pilar de IA en desarrollo según el documento fuente; Microsoft anunció posteriormente experiencia de evaluación enfocada en IA (ago 2026).

EN RESUMEN

Zero Trust no cambia. El mundo sí.

Las organizaciones actuales deben proteger a todas las entidades que pueden tomar decisiones o actuar en su nombre.

@SCavanna - Microsoft MCSA - Security

2 DE 5

IDENTIDADES NO HUMANAS

Nuevas entidades, nuevos desafíos

Los agentes y workloads actúan en nombre de la organización.
Zero Trust debe gobernar su identidad, acceso y comportamiento.

SERIE: ZERO TRUST EN LA ERA DE LA IA AGÉNTICA
2 DE 5

1 ¿QUÉ ES UNA IDENTIDAD NO HUMANA?

Son entidades digitales que pueden autenticarse, obtener permisos y ejecutar acciones en sistemas y datos de la organización sin intervención humana directa.

EJEMPLOS DE IDENTIDADES NO HUMANAS

- Agentes autónomos
- Bots y asistentes
- Microservicios y APIs
- Pipelines automatizados
- Workloads de IA
- Tokens, API keys e identidades administradas

REALIDAD CLAVE

"Cada nueva identidad no humana amplía la superficie de acceso y la complejidad de control."

2 ¿POR QUÉ IMPORTA AHORA?

PODER OPERATIVO
Pueden leer, modificar, crear o ejecutar acciones críticas como cualquier usuario privilegiado.

ESCALA Y VELOCIDAD
Pueden operar 24/7 y a velocidad de máquina en múltiples sistemas simultáneamente.

RIESGO NO MALICIOSO
El riesgo no proviene solo de malas intenciones, sino de contextos inadecuados o manipulados.

GOBERNANZA COMPLEJA
Las organizaciones deben administrar en paralelo identidades humanas y no humanas.

VISIBILIDAD LIMITADA
Muchos agentes operan sin visibilidad completa de su actividad.

IMPACTO PARA EL NEGOCIO

- Accesos excesivos o innecesarios
- Visibilidad limitada sobre actividades
- Mayor superficie de ataque
- Riesgos de cumplimiento y auditoría

3 IDENTIDAD HUMANA vs. IDENTIDAD NO HUMANA

IDENTIDAD HUMANA	ASPECTO	IDENTIDAD NO HUMANA
Usuario autenticado (ej. empleado)	NATURALEZA	Entidad digital sin presencia física (agente, servicio, workload)
Rol organizacional y pertenencia a grupos	PROPÓSITO	Propósito funcional o servicio específico
Sesiones interactivas de duración acotada	COMPORTAMIENTO	Ejecución automatizada, continua y a escala
Credenciales administradas por el usuario (MFA, reset)	CREDENCIALES	Tokens, secretos o identidades con ciclo de vida propio
Actividad observable como comportamiento humano	OBSERVABILIDAD	Actividad a velocidad de máquina; requiere telemetría y heurísticas
Acceso basado en necesidad del rol y tarea	ACCESO IDEAL	Acceso basado en mínimo privilegio, propósito y contexto

VERIFICACIÓN CONTINUA

Para ambas identidades

Verificar identidad y contexto → Evaluar comportamiento → Validar permisos y recursos → Reevaluar de forma continua

Zero Trust no distingue entre humanos y máquinas; verifica a todos.

4 APLICAR ZERO TRUST A IDENTIDADES NO HUMANAS

IDENTIFICAR Y REGISTRAR
- Inventariar todas las identidades no humanas.
- Definir propietario, propósito y sistemas que acceden.

GOBERNAR Y CONTROLAR
- Aplicar mínimo privilegio.
- Aprobaciones y excepciones justificadas.
- Rotación de secretos y lifecycle management.

DETECTAR Y RESPONDER
- Monitoreo de actividad.
- Detección de anomalías.
- Respuesta automática ante comportamientos sospechosos.

AUDITAR Y MEJORAR
- Revisar accesos y uso.
- Analizar riesgos y brechas.
- Ajustar controles de forma continua.

RESULTADO
Identidades no humanas seguras, gobernadas y alineadas al propósito organizacional.

5 CAPACIDADES Y RECURSOS DE MICROSOFT PARA ESTE DESAFÍO

MICROSOFT ENTRA AGENT ID
Administrar, proteger y gobernar identidades de agentes y workloads.
- Identidad única para agentes.
- Permisos granulares y ciclo de vida.
- Autenticación y autorización con Microsoft Entra.

ZERO TRUST WORKSHOP
Marco guiado para diseñar e implementar controles de Zero Trust para IA.
- Escenarios y patrones de referencia.
- Mapeo de controles y capacidades.
- Prioridad de acciones y roadmap.

ZERO TRUST ASSESSMENT
Evalúa tu postura Zero Trust, incluyendo controles específicos para IA.
- Evaluación automatizada de configuración.
- Hallazgos y recomendaciones priorizadas.
- Seguimiento de mejora continua.

EN RESUMEN

Nuevas identidades exigen nuevos controles.

Con Zero Trust, cada agente tiene el acceso justo, por el tiempo justo, para el propósito correcto.

EN LA SERIE:
1 El nuevo perímetro
2 Identidades no humanas
3 Ciclo de vida de IA con ZT
4 Controles clave para agentes
5 Arquitectura y herramientas

Próxima infografía: Ciclo de vida de IA protegido con Zero Trust

3 DE 5

CICLO DE VIDA DE IA CON ZERO TRUST

Seguridad continua de extremo a extremo

ZT4AI aplica Zero Trust en cada etapa del ciclo de vida de la IA, desde los datos hasta el comportamiento del agente en producción.

SERIE: ZERO TRUST EN LA ERA DE LA IA AGÉNTICA
3 DE 5

1 EL CICLO DE VIDA DE LA IA AGÉNTICA | 6 etapas, un mismo modelo de confianza

1. DATOS
Ingesta, limpieza y preparación de datos.

→

2. ENTRENAMIENTO
Entrenamiento y ajuste de modelos con datos gobernados.

→

3. DESPLIEGUE
Publicación segura de modelos y componentes.

→

4. OPERACIÓN
Ejecución del agente, uso de herramientas y recursos.

→

5. MONITOREO
Observabilidad de actividad, rendimiento y riesgos.

→

6. MEJORA CONTINUA
Retroalimentación, ajustes y nuevas capacidades.

VERIFICAR EXPLÍCITAMENTE • APLICAR MÍNIMO PRIVILEGIO • ASUMIR COMPROMISO

REALIDAD DEL CICLO

"El riesgo no aparece solo al final del ciclo. Zero Trust debe estar presente en cada decisión y cada acción."

2 AMENAZAS Y RIESGOS POR ETAPA (EJEMPLOS)

DATOS
- Datos envenenados
- Fugas en origen
- Accesos indebidos

ENTRENAMIENTO
- Poisoning de datos
- Robo de modelos
- Dependencias vulnerables

DESPLIEGUE
- Configuraciones expuestas
- Componentes no aprobados
- Secretos filtrados

OPERACIÓN
- Prompt injection
- Abuso de herramientas
- Escalada de privilegios
- Acciones indebidas

MONITOREO
- Actividad anómala no detectada
- Falta de trazabilidad
- Fatiga de alertas

MEJORA CONTINUA
- Retroalimentación envenenada
- Deriva del modelo
- Cambios sin control

ENFOQUE

Anticipar, detectar y responder en cada etapa del ciclo. No confiar por defecto en nada ni en nadie.

3 CONTROLES ZERO TRUST POR ETAPA

DATOS
- Clasificación y etiquetado
- Cifrado en tránsito y en reposo
- DLP para datos sensibles
- Control de acceso basado en contexto

ENTRENAMIENTO
- Orígenes de datos confiables
- Entornos aislados
- Gestión de secretos
- Validación de integridad

DESPLIEGUE
- Infraestructura como código
- Imágenes firmadas y escaneadas
- Control de cambios y aprobaciones

OPERACIÓN
- Identidades de agentes con mínimo privilegio
- Autorización por herramienta y acción
- Limitación y control de sesiones

MONITOREO
- Telemetría completa
- Detección de anomalías
- Alertas con contexto
- Respuesta automatizada

MEJORA CONTINUA
- Validación de datos de feedback
- Pruebas continuas
- Evaluación de deriva
- Gestión de versiones y rollbacks

PRINCIPIOS

Mismos principios. Aplicación continua. Confianza nunca implícita.

4 TECNOLOGÍAS HABILITADORAS DE ZT4AI

IDENTIDAD
Microsoft Entra Agent ID, identidades administradas, federación y ciclos de vida.

ACCESO Y PERMISOS
Conditional Access, PIM, acceso just-in-time y políticas basadas en atributos.

PROTECCIÓN DE DATOS
Microsoft Purview, DLP, cifrado, clasificación y linaje.

DETECCIÓN Y RESPUESTA
Microsoft Defender, UEBA, alertas y playbooks automáticos.

GOBERNANZA Y CUMPLIMIENTO
Políticas, auditabilidad, retención, evaluación de riesgos y privacidad.

INTEGRACIÓN CONTINUA: los controles trabajan de forma orquestada en todo el ciclo de vida.

5 MENSAJE CLAVE

"Zero Trust no es un punto de control, es un ciclo continuo de confianza.
En cada etapa, cada identidad, cada acción.

ZT4AI EN ACCIÓN

- Reduce superficie de ataque
- Limita impacto de brechas
- Mejora cumplimiento y trazabilidad
- Acelera innovación con seguridad

EN LA SIGUIENTE INFOGRAFÍA

Controles clave para agentes y herramientas: cómo aplicar Zero Trust en la operación diaria.

Infografía 4 de 5

4 DE 5

CONTROLES CLAVE PARA AGENTES

Aplicando Zero Trust a identidades no humanas

Los agentes necesitan los mismos principios de Zero Trust, con controles específicos para su naturaleza y operación.

SERIE: ZERO TRUST EN LA ERA DE LA IA AGÉNTICA
4 DE 5

1 PRINCIPIOS, CONTROLES, APLICACIÓN A AGENTES Y RESULTADO

PRINCIPIO ZERO TRUST	CONTROLES CLAVE	APLICACIÓN A AGENTES	RESULTADO
VERIFICAR EXPLÍCITAMENTE	• Identidad y contexto • Validación continua • Señales de comportamiento	Verificar identidad del agente, propósito, origen, contexto y comportamiento en cada solicitud.	Acceso solo para agentes confiables en el contexto adecuado.
APLICAR MÍNIMO PRIVILEGIO	• Acceso JIT (Just-In-Time) • Alcance mínimo • Segmentación y aislamiento	Otorgar permisos mínimos por tarea, recurso y tiempo necesario.	Menor superficie de ataque y reducción de impacto ante incidentes.
ASUMIR COMPROMISO	• Monitoreo y detección • Respuesta automática • Resiliencia y recuperación	Detectar comportamientos anómalos, abuso de permisos y desviaciones del propósito.	Contención rápida, respuesta efectiva y continuidad del negocio.

2 CONTROLES DE IDENTIDAD PARA AGENTES

IDENTIDAD ÚNICA
- Cada agente tiene su identidad única y verificable.
- Sin compartir credenciales.

REGISTRO Y APROBACIÓN
- Altas de agentes registradas y aprobadas.
- Propietario y propósito definidos.

CREDENCIALES GESTIONADAS
- Uso de tokens o identidades administradas.
- Rotación y revocación automática.

ACCESO JUSTO A TIEMPO
- Acceso por tiempo limitado y por tarea.
- Revocación automática al finalizar.

GOBIERNO DEL CICLO DE VIDA
- Inventario completo de agentes.
- Revisión periódica y baja segura.

3 CONTROLES DE ACCESO Y SEGMENTACIÓN

AUTORIZACIÓN POR PROPÓSITO
- Permisos alineados al propósito funcional.
- Nada más.

SEGMENTACIÓN Y AISLAMIENTO
- Agentes aislados por entorno, red y datos.
- Principio de mínima exposición.

CONTROL DE RECURSOS
- Restricción a API, datos, herramientas y modelos.
- Políticas granulares.

ACCESO A INTERNET
- Egreso controlado y filtrado por destino.
- Bloqueo de destinos riesgosos.

El acceso de un agente debe ser tan restringido y verificable como el de cualquier usuario humano... o más.

4 OBSERVABILIDAD, DETECCIÓN Y RESPUESTA

TELEMETRÍA COMPLETA
- Registrar acciones, decisiones, llamadas a herramientas y accesos a datos.

→ **DETECCIÓN DE ANOMALÍAS**
- Modelos de detección de comportamiento.
- Umbrales y baselines.

→ **ALERTAS CON CONTEXTO**
- Alertas ricas con propósito, identidad, recurso y riesgo.

→ **RESPUESTA AUTOMÁTICA**
- Revocar acceso.
- Aislar agente.
- Bloquear acciones.
- Notificar responsables.

Visibilidad y respuesta en tiempo real para detener el abuso antes de que se convierta en un incidente.

5 PROTECCIÓN DE DATOS Y MODELOS UTILIZADOS POR AGENTES

CLASIFICACIÓN DE DATOS
- Datos etiquetados por sensibilidad.
- Políticas DLP aplicadas.

ACCESO A DATOS
- Acceso solo a los datos necesarios para la tarea.
- Controles basados en atributos.

PROTECCIÓN DE MODELOS
- Control de acceso a modelos y prompts.
- Protección contra prompt injection y abuso.

AUDITORÍA Y EXPLICABILIDAD
- Trazabilidad de decisiones y fuentes.
- Explicabilidad y rendición de cuentas.

Proteger los datos y modelos es proteger el valor y la confianza del negocio.

6 IMPLEMENTAR, GOBERNAR Y MEJORAR CONTINUAMENTE

DEFINIR ESTRATEGIA
Establecer políticas, estándares y tolerancia al riesgo para agentes.

> **IMPLEMENTAR CONTROLES**
Aplicar controles de identidad, acceso, protección, detección y respuesta.

> **MEDIR Y EVALUAR**
Evaluar efectividad con métricas, auditorías y simulaciones de amenazas.

> **MEJORAR CONTINUAMENTE**
Ajustar controles, actualizar políticas y incorporar lecciones aprendidas.

RECUERDA

Zero Trust no es un proyecto, es una disciplina operativa.

La seguridad de tus agentes depende de la consistencia de tus controles.

EN LA SERIE:

1. El nuevo perímetro
2. Identidades no humanas
3. Ciclo de vida de IA con ZT
4. Controles clave para agentes
5. Arquitectura y herramientas

Próxima infografía: Arquitectura y herramientas para ZT4AI

@SCavanna - Microsoft MCSA - Security

5 DE 5

ARQUITECTURA Y HERRAMIENTAS para ZT4AI

Construyendo una plataforma segura para agentes con Zero Trust en cada capa y en cada interacción.

SERIE: ZERO TRUST EN LA ERA DE LA IA AGÉNTICA
5 DE 5

1 ARQUITECTURA DE REFERENCIA ZT4AI

Capas de protección Zero Trust para agentes

IDENTIDADES
Identidades humanas y no humanas gestionadas y verificadas.

ACCESO
Acceso mínimo, just-in-time y basado en riesgo.

APLICACIONES Y AGENTES
Agentes y servicios orquestados, aislados y monitoreados.

DATOS Y MODELOS
Datos y modelos protegidos, clasificados y con DLP.

INFRAESTRUCTURA
Entornos aislados, cifrados y con segmentación.

OBSERVABILIDAD Y RESPUESTA
Visibilidad integral y respuesta automatizada ante amenazas.

FLUJO ZERO TRUST PARA AGENTES

El agente se identifica. → Se verifica contexto y comportamiento. → Se otorgan permisos mínimos. → Ejecuta la tarea en un entorno aislado. → Se monitorea y se responde en tiempo real.

PRINCIPIOS APLICADOS EN CADA INTERACCIÓN

- Verificar explícitamente
- Aplicar mínimo privilegio
- Asumir compromiso

2 CAPACIDADES CLAVE DE LA PLATAFORMA

MICROSOFT ENTRA AGENT ID
Identidad, ciclo de vida y gobernanza de agentes. Autenticación y autorización basadas en Microsoft Entra.

ACCESO CONDICIONAL PARA AGENTES
Políticas basadas en contexto, riesgo, dispositivo, ubicación y comportamiento.

CONTROLES DE RED Y APLICACIONES
Segmentación, aislamiento de cargas de trabajo y control de salida a Internet.

PROTECCIÓN DE DATOS Y MODELOS
Microsoft Purview, DLP, clasificación, cifrado y gestión de claves.

DETECCIÓN Y RESPUESTA AVANZADAS
Microsoft Defender XDR, detección de anomalías y respuesta automatizada.

3 HERRAMIENTAS Y RECURSOS DE MICROSOFT

MICROSOFT ENTRA AGENT ID
Administra, protege y gobierna identidades de agentes y workloads.
- ✓ Identidad única
- ✓ Permisos granulares
- ✓ Ciclo de vida y rotación

ZERO TRUST WORKSHOP
Guía práctica para diseñar e implementar controles Zero Trust para IA.
- ✓ Escenarios y patrones
- ✓ Mapeo de controles
- ✓ Roadmap de adopción

ZERO TRUST ASSESSMENT
Evalúa la postura Zero Trust de tu entorno de IA y agentes.
- ✓ Evaluación automatizada
- ✓ Hallazgos priorizados
- ✓ Recomendaciones accionables

4 PATRONES DE ARQUITECTURA PARA AGENTES

AGENTE CON ACCESO A API
- ✓ Identidad del agente
- ✓ Token con acceso mínimo
- ✓ Monitoreo y control de salida

AGENTE CON ACCESO A DATOS
- ✓ Acceso JIT a datos
- ✓ DLP y clasificación
- ✓ Auditoría de consultas

AGENTE CON HERRAMIENTAS EXTERNAS
- ✓ Aprobación de herramientas
- ✓ Permisos por propósito
- ✓ Restricción por contexto

AGENTES EN RED CORPORATIVA
- ✓ Segmentación de red
- ✓ Control de tráfico Este-Oeste
- ✓ Inspección y filtrado

AGENTES EN ENTORNOS CLOUD
- ✓ Identidades administradas
- ✓ Políticas en la nube
- ✓ Aislamiento de recursos

DISEÑAR PARA CONFIANZA ADAPTATIVA
Arquitecturas flexibles que responden al contexto y al riesgo en tiempo real.

Confianza dinámica.
Riesgo reducido.
Negocio habilitado.

5 Hoja de ruta recomendada para tu organización

1. **EVALUAR** — Evalúa tu postura actual y escenarios de uso de agentes.
2. **DEFINIR** — Define identidades, políticas y límites de confianza.
3. **DISEÑAR** — Diseña arquitectura Zero Trust para agentes.
4. **IMPLEMENTAR** — Implementa controles por etapas y valida resultados.
5. **OPERAR** — Monitorea, detecta y responde de forma continua.
6. **MEJORAR** — Aprende, ajusta y mejora de forma continua.

MENSAJE FINAL

"Zero Trust no es un destino, es una disciplina operativa. Aplica los mismos principios a cada agente, herramienta y decisión que impacta a tu organización."

EN LA SERIE: 1 El nuevo perímetro · 2 Identidades no humanas · 3 Ciclo de vida de IA con ZT · 4 Controles clave para agentes · 5 Arquitectura y herramientas

¡Completaste la serie! Lleva Zero Trust para IA a toda tu organización.