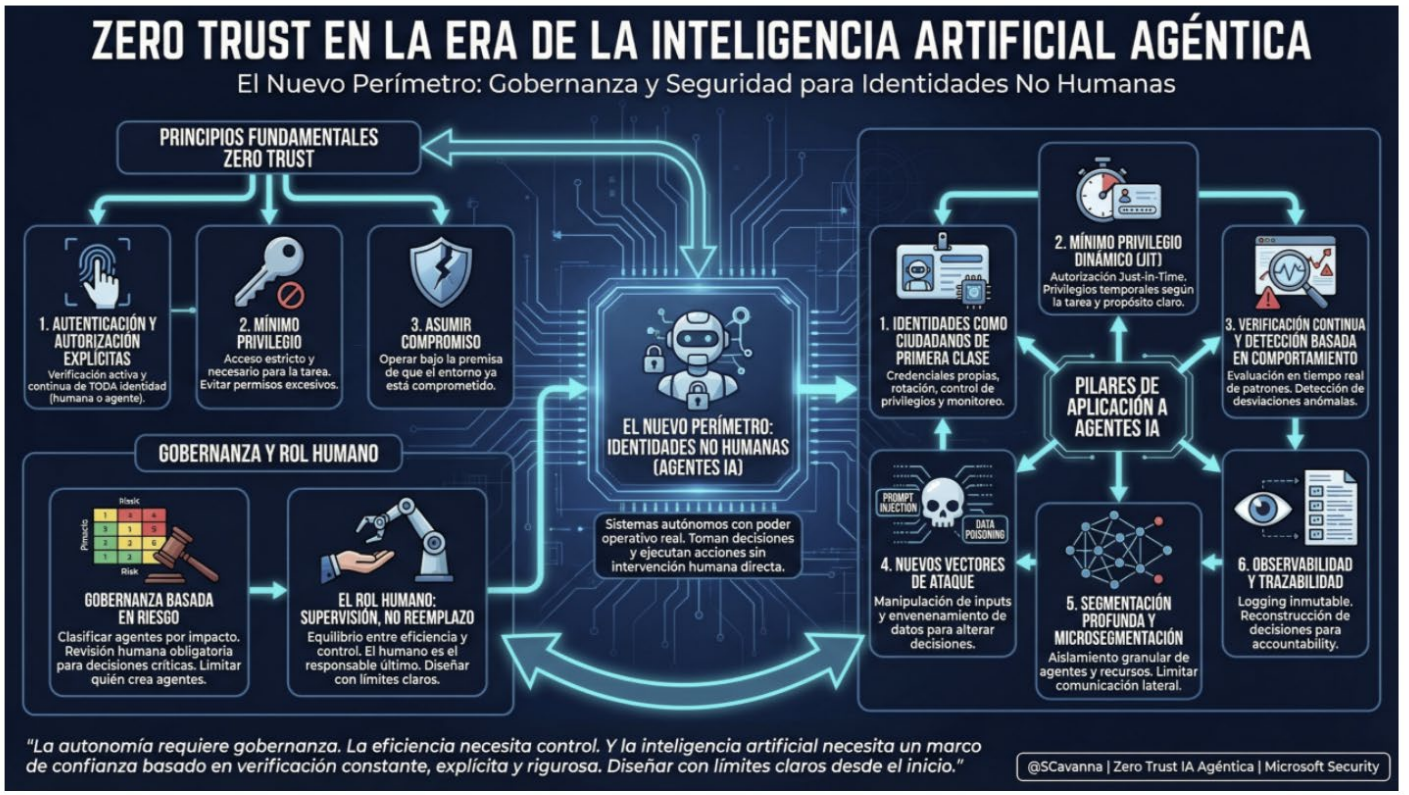


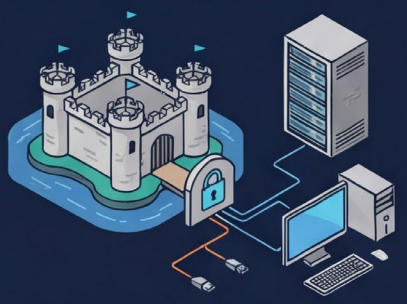

# Microsoft Security CSU MCSA - ZeroTrust Academy (E01): "Zero Trust en la Era de los Agentes de IA" + > Ticket de salida by SCavanna.


**Microsoft Security | MCSA CSU**
66 seguidores


20 de marzo de 2026

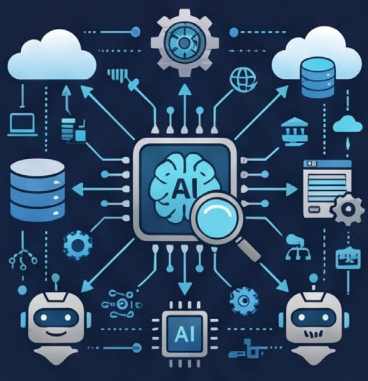
# ZERO TRUST EN LA ERA DE LA INTELIGENCIA ARTIFICIAL AGÉNTICA

«El perímetro ya no es la red. Es el conjunto de entidades que toman decisiones por la organización.»



**PASADO: PERÍMETRO DE RED**
La seguridad se basaba en la ubicación física y la conexión a la red corporativa.

**PRESENTE: IDENTIDAD HUMANA**
El trabajo remoto y móvil desplezó el control a la verificación de la identidad del usuario.




**FUTURO (HOY): IDENTIDAD NO HUMANA (IA AGÉNTICA)**
Agentes autónomos, bots y workloads de IA actóen con poder operativo real sobre sistemas críticos.

## EL CAMBIO ESTRUCTURAL: IDENTIDAD HUMANA VS. NO HUMANA

| IDENTIDAD HUMANA | IDENTIDAD NO HUMANA (AGENTE) |
|---|---|
| Usuario autenticado con MFA | Token o API key con ciclo de vida propio |
| Acceso basado en rol organizacional | Acceso basado en propósito funcional |
| Comportamiento predecible con desvios detectables | Patrones de ejecución a velocidad de máquina |
| Credenciales rotadas periódicamente | Secretos en bóveda, rotación automática |
| Sesión con duración razonable | Ejecución continua, sin sesión definida |

**EL DOBLE DESAFÍO**
Gestionar simultáneamente riesgos humanos y no humanos con recursos limitados. La superficle de ataque crece exponencialmente con cada agente.

## PRINCIPIOS FUNDACIONALES DE ZERO TRUST (INVARIABLES)

**1. VERIFICACIÓN EXPLÍCITA**
Toda identidad debe ser verificada de forma activa y continua, sin asumir confianza previa.

**2. MÍNIMO PRIVILEGIO**
El acceso se otorga con los permisos estrictamente oeresarios para la tarea en cuestion, uada más.

**3. ASUMIR COMPROMISO**
Operor siempre hajo la premisa de que el entorno ya esté comprometido y diseñar los sistemas en consecuencia.

→ AGENTES AUTÓNOMOS & ENTIDADES NO HUMANAS

SCavanna

## PRODUCTS BAR

### RESPUESTA DE MICROSOFT: ZERO TRUST FOR AI (ZT4AI)

**Entra Agent ID**
Registro y gestiõo de identidades de agentes usando las experiencias familiares de Microsoft Entte, con autenticación robusta y gubernanza.

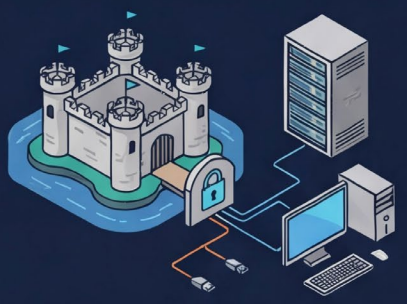
**ZT4AI Workshop**
Taller guiado que ayuda a equipos de seguridad, IT y desarrollo a identificar brechas y construir un camino de implementación para IA agéntica.

**Zero Trust Assessment**
Herramiente de evaluación automatizada, con piler especifico para IA en desarrollo para verano de 2026.

«Zero Trust for AI no introduce nuevos principios. Introduce una nueva forma de aplicarlos sistemáticamente a entornos de IA.»
— Microsoft Security Blog, marzo 2026

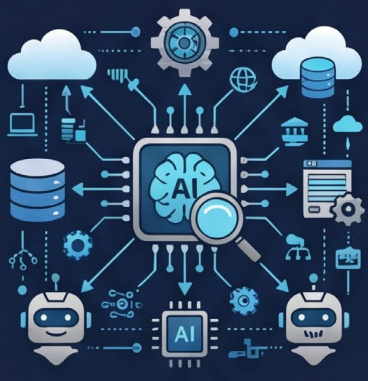
# ZERO TRUST EN LA ERA DE LA INTELIGENCIA ARTIFICIAL AGÉNTICA

«El perímetro ya no es la red. Es el conjunto de entidades que toman decisiones por la organización.»



**PASADO: PERÍMETRO DE RED**
La seguridad se basaba en la ubicación física y la conexión a la red corporativa.

**PRESENTE: IDENTIDAD HUMANA**
El trabajo remoto y móvil desplezó el control a la verificación de la identidad del usuario.




**FUTURO (HOY): IDENTIDAD NO HUMANA (IA AGÉNTICA)**
Agentes autónomos, bots y workloads de IA actóen con poder operativo real sobre sistemas críticos.

## EL CAMBIO ESTRUCTURAL: IDENTIDAD HUMANA VS. NO HUMANA

| IDENTIDAD HUMANA | IDENTIDAD NO HUMANA (AGENTE) |
|---|---|
| Usuario autenticado con MFA | Token o API key con ciclo de vida propio |
| Acceso basado en rol organizacional | Acceso basado en propósito funcional |
| Comportamiento predecible con desvios detectables | Patrones de ejecución a velocidad de máquina |
| Credenciales rotadas periódicamente | Secretos en bóveda, rotación automática |
| Sesión con duración razonable | Ejecución continua, sin sesión definida |

**EL DOBLE DESAFÍO**
Gestionar simultáneamente riesgos humanos y no humanos con recursos limitados. La superficle de ataque crece exponencialmente con cada agente.

## PRINCIPIOS FUNDACIONALES DE ZERO TRUST (INVARIABLES)

**1. VERIFICACIÓN EXPLÍCITA**
Toda identidad debe ser verificada de forma activa y continua, sin asumir confianza previa.

**2. MÍNIMO PRIVILEGIO**
El acceso se otorga con los permisos estrictamente oeresarios para la tarea en cuestion, uada más.

**3. ASUMIR COMPROMISO**
Operor siempre hajo la premisa de que el entorno ya esté comprometido y diseñar los sistemas en consecuencia.

→ AGENTES AUTÓNOMOS & ENTIDADES NO HUMANAS

SCavanna

## PRODUCTS BAR

### RESPUESTA DE MICROSOFT: ZERO TRUST FOR AI (ZT4AI)

**Entra Agent ID**
Registro y gestiõo de identidades de agentes usando las experiencias familiares de Microsoft Entte, con autenticación robusta y gubernanza.

**ZT4AI Workshop**
Taller guiado que ayuda a equipos de seguridad, IT y desarrollo a identificar brechas y construir un camino de implementación para IA agéntica.

**Zero Trust Assessment**
Herramiente de evaluación automatizada, con piler especifico para IA en desarrollo para verano de 2026.

«Zero Trust for AI no introduce nuevos principios. Introduce una nueva forma de aplicarlos sistemáticamente a entornos de IA.»
— Microsoft Security Blog, marzo 2026

# INFOGRAFÍA 2: Mínimo Privilegio y Control de Acceso

## Gestión Dinámica de Permisos para Agentes de IA

El principio de mínimo privilegio es uno de los pilares más antiguos de la ciberseguridad. La llegada de la IA agéntica amplifica este desafío de forma exponencial.

### 1. DEFINICIÓN DE PROPÓSITO

Agente con propósito claro y acotado.

### 2. IDENTIFICACIÓN DE RECURSOS

Qué recursos necesita para cumplir ese propósito.

### 3. ASIGNACIÓN DE PERMISOS MÍNIMOS

Otorgar únicamente los accesos esenciales.

### 4. GESTIÓN DINÁMICA (JIT & REVOCACIÓN)

Privilegios temporales para tareas específicas, revocados al finalizar.

## LOS TRES FACTORES DE COMPLEJIDAD

### ESCALA

Organizaciones despliegan decenas o cientos de agentes. Multiplica identidades con acceso crítico.

### DINAMISMO

Perfil de acceso cambia continuamente según la tarea. Necesita permisos temporales.

### OPACIDAD

Sin presencia visual, no están en el organigrama. Actividad difícil de interpretar.

## SEPARACIÓN DE FUNCIONES: EJEMPLOS CONCRETOS

| | CAPACIDAD DEL AGENTE | LO QUE NO DEBE PODER HACER SOLO |
|---|---|---|
| 1 | Escribir código | Aprobar sus propios pull requests |
| 2 | Analizar código | Hacer deployment a producción |
| 3 | Acceder a datos sensibles | Exportar esos datos externamente |
| 4 | Generar propuestas de pago | Aprobar y ejecutar los pagos |
| 5 | Clasificar correos de phishing | Modificar reglas del motor antispam |

## AUTORIZACIÓN JUST-IN-TIME (JIT)

**SISTEMA DE IDENTIDAD** (Contexto & Propósito)

**MOTOR DE POLÍTICAS** (Evaluación en Tiempo Real)

**PLATAFORMA DE EJECUCIÓN** (Activación/Revocación)

Privilegios otorgados temporalmente para una tarea específica y revocados automáticamente.

**DATO DESTACADO:** Más del 80% de las empresas Fortune 500 ya tienen agentes activos construidos con low-code/no-code. **80%**

## PRODUCTOS MICROSOFT QUE MATERIALIZAN ESTE PRINCIPIO

### ENTRA AGENT ID

Registro, autenticación y gestión de ciclo de vida de identidades de agentes.

### ENTRA PIM

Privileged Identity Management para autorización JIT y auditoría automática.

### ENTRA SUITE

Acceso condicional unificado para usuarios y agentes con políticas de contexto.

### AZURE KEY VAULT

Bóveda de secretos para gestión segura de credenciales, tokens y API keys.

"El diseño del agente es el primer control de seguridad." - Architects Daughter

"Los mismos principios de Zero Trust que aplican a empleados humanos aplican a los agentes de IA. Ahora se pueden usar las mismas herramientas para gestionar ambos." - Microsoft Security, 2026

@SCavanna

# INFOGRAFÍA 4: Verificación Continua, Observabilidad y Trazabilidad

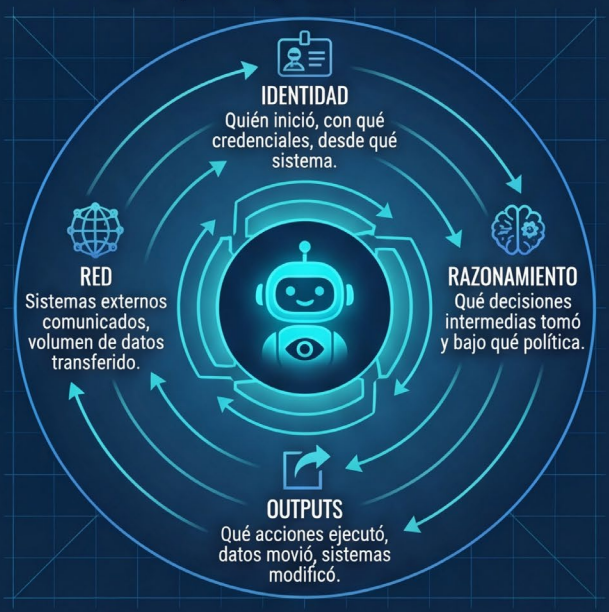
## Sin Visibilidad No Hay Accountability — Sin Accountability la Autonomía es Riesgo

Zero Trust asume compromiso: la validación de confianza debe recalcularse continuamente. En el mundo de los agentes autónomos, esto es más complejo y crítico. Es fuego contra fuego: no es posible monitorear IA a escala humana sin la propia inteligencia artificial.

### VERIFICACIÓN CONTINUA: HUMANO VS. AGENTE

| INDICADOR HUMANO | INDICADOR EN AGENTE |
|---|---|
| Impossible travel (ubicación geográfica) | Ejecución en entornos no previstos en el diseño |
| Dispositivo fuera de compliance | Versión del modelo o runtime no autorizada |
| Horario de acceso inusual | Actividad fuera del horario operacional definido |
| Volumen de descarga inusual | Volumen de requests que supera el baseline |
| Acceso a recursos fuera del rol | Acceso a recursos fuera del propósito declarado |

### OBSERVABILIDAD TOTAL: EL REQUISITO QUE NO ES OPCIONAL




### DETECCIÓN BASADA EN COMPORTAMIENTO (SEMÁFORO DE ALERTAS)

- **CAMBIO DE PATRÓN** — De operaciones de solo lectura a escritura/eliminación.
- **ORDEN INUSUAL** — Acceso a recursos en orden inusual (reconocimiento).
- **APIs EXTERNAS** — Llamadas a APIs no parte del pipeline normal.
- **LATENCIA ABRUPTA** — Aumento abrupto en latencia (procesamiento no previsto).
- **OUTPUTS ANÓMALOS** — Outputs inusualmente largos o formatos distintos.

### FLUJO TEMPORAL: EL VALOR DE LA TRAZABILIDAD

**SIN TRAZABILIDAD (INVESTIGACIÓN A CIEGAS)**

Incidente → Análisis forense imposible → Sin atribución → Riesgo absoluto.

**CON TRAZABILIDAD (RECONSTRUCCIÓN ATRIBUIBLE)**

Incidente → Reconstrucción de la cadena de eventos → Identidad, Contexto, Política verificados → Gobernanza real.

> "No existe la manera de monitorear inteligencia artificial sin inteligencia artificial. Cuando los atacantes operan a velocidad de máquina, los defensores no pueden operar solo a velocidad humana."

### PRODUCTOS MICROSOFT QUE MATERIALIZAN ESTE PRINCIPIO

**MICROSOFT SENTINEL**
SIEM nativo en la nube para correlación de señales y detección de comportamiento para agentes.

**AGENT 365**
Plataforma de observabilidad, seguridad y gobernanza. Registry y visibilidad de permisos.

**AZURE AI FOUNDRY**
Tracing, monitoring y evaluaciones integradas en el runtime. Gestión unificada.

**MICROSOFT PURVIEW AUDIT**
Logging inmutable y búsqueda de actividad para identidades humanas y no humanas.

"Sin trazabilidad no hay accountability. Sin accountability, la autonomía es un peligro absoluto."
— Principio central de Zero Trust para IA agéntica

# INFOGRAFÍA 4: Verificación Continua, Observabilidad y Trazabilidad

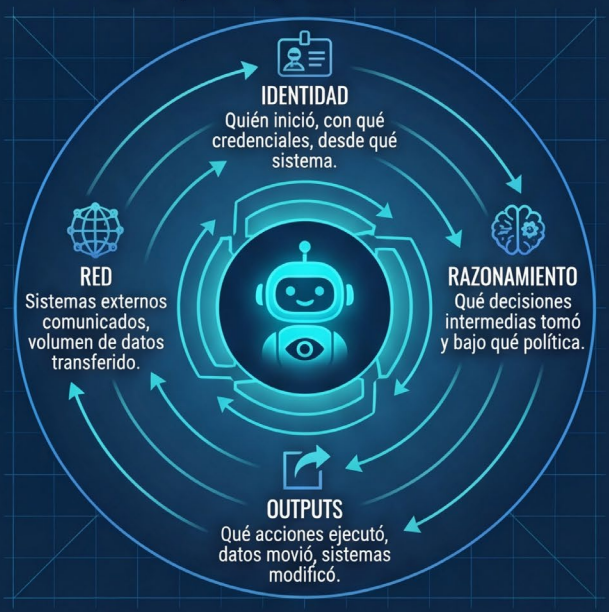
## Sin Visibilidad No Hay Accountability — Sin Accountability la Autonomía es Riesgo

Zero Trust asume compromiso: la validación de confianza debe recalcularse continuamente. En el mundo de los agentes autónomos, esto es más complejo y crítico. Es fuego contra fuego: no es posible monitorear IA a escala humana sin la propia inteligencia artificial.

### VERIFICACIÓN CONTINUA: HUMANO VS. AGENTE

| INDICADOR HUMANO | INDICADOR EN AGENTE |
|---|---|
| Impossible travel (ubicación geográfica) | Ejecución en entornos no previstos en el diseño |
| Dispositivo fuera de compliance | Versión del modelo o runtime no autorizada |
| Horario de acceso inusual | Actividad fuera del horario operacional definido |
| Volumen de descarga inusual | Volumen de requests que supera el baseline |
| Acceso a recursos fuera del rol | Acceso a recursos fuera del propósito declarado |

### OBSERVABILIDAD TOTAL: EL REQUISITO QUE NO ES OPCIONAL




### DETECCIÓN BASADA EN COMPORTAMIENTO (SEMÁFORO DE ALERTAS)

- **CAMBIO DE PATRÓN** — De operaciones de solo lectura a escritura/eliminación.
- **ORDEN INUSUAL** — Acceso a recursos en orden inusual (reconocimiento).
- **APIs EXTERNAS** — Llamadas a APIs no parte del pipeline normal.
- **LATENCIA ABRUPTA** — Aumento abrupto en latencia (procesamiento no previsto).
- **OUTPUTS ANÓMALOS** — Outputs inusualmente largos o formatos distintos.

### FLUJO TEMPORAL: EL VALOR DE LA TRAZABILIDAD

**SIN TRAZABILIDAD (INVESTIGACIÓN A CIEGAS)**

Incidente → Análisis forense imposible → Sin atribución → Riesgo absoluto.

**CON TRAZABILIDAD (RECONSTRUCCIÓN ATRIBUIBLE)**

Incidente → Reconstrucción de la cadena de eventos → Identidad, Contexto, Política verificados → Gobernanza real.

> "No existe la manera de monitorear inteligencia artificial sin inteligencia artificial. Cuando los atacantes operan a velocidad de máquina, los defensores no pueden operar solo a velocidad humana."

### PRODUCTOS MICROSOFT QUE MATERIALIZAN ESTE PRINCIPIO

**MICROSOFT SENTINEL**
SIEM nativo en la nube para correlación de señales y detección de comportamiento para agentes.

**AGENT 365**
Plataforma de observabilidad, seguridad y gobernanza. Registry y visibilidad de permisos.

**AZURE AI FOUNDRY**
Tracing, monitoring y evaluaciones integradas en el runtime. Gestión unificada.

**MICROSOFT PURVIEW AUDIT**
Logging inmutable y búsqueda de actividad para identidades humanas y no humanas.

"Sin trazabilidad no hay accountability. Sin accountability, la autonomía es un peligro absoluto."
— Principio central de Zero Trust para IA agéntica