



EBOOK ONESEC · SECURITY DAYS MÉXICO 2026 — EXECUTIVE GUIDE

# Una transformación empresarial segura a la velocidad de la IA

Cómo gobernar, asegurar, adoptar y escalar la IA sin frenar el negocio.

*Usted acaba de escuchar a Microsoft describir la nueva realidad de seguridad de la IA. Pero la seguridad es solo la mitad de la historia. A través de este ebook usted podrá conocer como transformar su organización en una empresa agéntica y hacer realidad los beneficios de la IA, administrando efectivamente los riesgos que ello conlleva.*

## RESUMEN EJECUTIVO

# Un minuto para entender de qué trata este Executive Guide

La IA ya cambió cómo decide y opera la empresa, con o sin gobierno formal. Escalarla con confianza exige más que tecnología: exige gobierno y seguridad como capa de confianza, especialmente cuando los agentes empiezan a actuar por cuenta propia.

Microsoft aporta la plataforma para construir esta transformación de extremo a extremo. ONESEC convierte esa plataforma en capacidades reales de negocio: gobernadas, seguras y operables, a través de Enterprise Secure AI Business Transformation.

En las siguientes páginas encontrará el reto de negocio, la cadena de gobierno de IA, la empresa agéntica, el rol de Microsoft, el modelo de ONESEC y, al cierre, un autodiagnóstico para medir dónde está su organización hoy.

### CONTINÚA — 02 · EL RETO DE LA TRANSFORMACIÓN EMPRESARIAL CON IA

**La adopción de IA generativa y agéntica ya no es una iniciativa de innovación aislada: es una decisión de negocio de primer nivel.**

## 02 — EL RETO DE LA TRANSFORMACIÓN EMPRESARIAL CON IA

# La ambición va más rápido que la preparación organizacional

Colaboradores de todas las áreas ya utilizan IA generativa y agéntica para escribir, analizar, resumir, programar y tomar decisiones, muchas veces por iniciativa propia. Esta adopción avanza con o sin gobierno formal, y con frecuencia lo hace mediante herramientas de consumo fuera de cualquier proceso corporativo: es lo que se conoce como **Shadow AI**. No es una acusación contra los colaboradores; casi siempre nace de una intención legítima de ser más productivos. Pero cuando ese uso no está gobernado, puede exponer información sensible, producir resultados fuera de contexto y afectar decisiones sin que nadie lo sepa. El riesgo no es que la empresa esté usando IA: es que la esté usando sin la capa de gobierno que permite aprovecharla y escalarla de forma segura y verificable.

### 70%

del éxito al escalar IA depende de personas y procesos, no de tecnología — BCG.

### 74%

de las empresas no ha desarrollado las capacidades para escalar ese valor.

### 21%

ha rediseñado sus flujos de trabajo alrededor de la IA generativa — McKinsey.

### 95%

de los pilotos de IA generativa (MIT) no mostraron impacto financiero medible.

***Los proyectos de IA no fracasan porque la IA no funcione. Se estancan cuando la empresa alrededor de la IA no está lista.***

### 03 — GOBIERNO DE IA: LA CAPA DE CONFIANZA

## El gobierno no es burocracia. Es la capa de confianza que permite escalar la IA empresarial.

Gobernar no significa frenar la creatividad ni desacelerar la innovación: significa detectar oportunamente dónde y cómo se está usando la IA para que esas buenas intenciones no terminen materializando riesgos que pudieron administrarse a tiempo. Cada nuevo agente, modelo, integración y flujo de datos amplía la superficie de ataque de la organización, a una velocidad y escala que la seguridad tradicional no había enfrentado antes.

### La cadena de gobierno de la IA



La estrategia define qué casos de uso importan; corre sobre datos confiables que alimentan un modelo entendido y probado; el modelo se invoca a través de una identidad con permisos definidos; esa identidad autoriza una acción real; cada acción conlleva un riesgo que se contiene con seguridad y se verifica contra cumplimiento; y solo entonces el sistema produce valor de negocio sostenible.

### ¿Están verificadas cada una de estas capas en su organización?

#### EVIDENCIA — DELOITTE 2026

3,235 líderes globales: **94%** de las firmas financieras planea aumentar su inversión en IA, pero solo **1 de cada 5** tiene un gobierno maduro sobre sus agentes autónomos.

**La ambición ya está. El gobierno, en la mayoría de las empresas, todavía no.**

## 04 — LA EMPRESA AGÉNTICA

# Un agente necesita supervisión

La IA cambia de naturaleza cuando deja de responder y empieza a actuar.

Un copiloto puede sugerir una respuesta. Un agente puede interpretar un contexto, decidir el siguiente paso, consultar información, utilizar herramientas y ejecutar una acción en nombre de una persona o de la organización. La pregunta deja de ser si la IA es inteligente: es si la empresa puede confiar en lo que esa IA puede hacer.

### COPILOTO / ASISTENTE

Interpreta, sugiere y genera para ayudar a una persona a decidir.

### AGENTE

Interpreta, decide, consulta y **ejecuta una acción** en nombre de una persona o la organización.

*Una empresa agéntica no es permitir que la IA actúe, sino asegurarse de que la organización pueda confiar en lo que esa IA hace.*

## La cadena de la empresa agéntica

Agente → Identidad → Permisos → Acción → Datos

Monitoreo → Gobierno → Seguridad → Supervisión humana

El reto también cambia de escala: una organización puede pasar de gestionar un número limitado de usuarios y sistemas a tener decenas o cientos de agentes digitales actuando sobre procesos, información y activos empresariales. La supervisión humana ya no puede depender de observar manualmente cada acción; necesita una capa de control digital que permita saber qué agentes existen, quién responde por ellos, a qué acceden y cómo se detecta un comportamiento anómalo.

### IBM / PONEMON 2025

Brechas con **Shadow AI** costaron **US\$670K más. 63%** no tenía política de gobierno de IA.

*[Caso de agente — requiere fuente validada]*

Hacer que un agente funcione es el primer paso. Ahí es donde ONESEC aporta valor: ayudando a convertir agentes que funcionan en capacidades empresariales en las que se puede confiar.

## 05 — MICROSOFT: LA PLATAFORMA PARA HACER REAL LA TRANSFORMACIÓN CON IA

### La transformación ocurre cuando la empresa rediseña cómo trabaja, decide y crea valor — no por añadir IA a lo que ya existe.

Microsoft está convergiendo IA, agentes, datos, nube, aplicaciones, productividad y seguridad en una plataforma que permite recorrer ese camino de extremo a extremo.

#### 01 — FRONTIER

##### La nueva forma de trabajar

Personas y agentes colaboran; la IA pasa de ser una herramienta aislada a formar parte de cómo opera el negocio.

#### 02 — CORE

##### La base que lo hace posible

Datos, aplicaciones, nube, identidad, productividad, seguridad y gobierno permiten escalar con confianza.

*Lo importante no es tener más tecnología. Es saber conectar las piezas.*

#### 01 — Transformar

Identificar dónde la IA cambia el negocio.

#### 02 — Construir

Llevar agentes, Copilot y datos a procesos reales.

#### 03 — Proteger y gobernar

Asegurar identidades, datos, agentes y decisiones.

#### 04 — Adoptar y operar

Convertir despliegues en uso, y uso en transformación.

Aquí es donde ONESEC aporta valor: combinando estrategia, arquitectura, tecnología, ciberseguridad, gobierno, implementación, adopción y operación para que la transformación se convierta en una capacidad empresarial real.

## 06 — DENTRO DE LA ARQUITECTURA TECNOLÓGICA DE MICROSOFT

### Organizada por lo que cada pieza habilita

#### ASEGURAR

##### Entra • Defender XDR • Sentinel • Security Copilot

Identidad y acceso extendidos a agentes; operaciones de seguridad unificadas. Security Copilot redujo el tiempo de respuesta a incidentes en un **78%** y aumentó la precisión hasta **77%**.

#### GOBERNAR

##### Microsoft Agent 365 • Entra Agent ID

Plano de control para inventariar, auditar y gobernar agentes. Identidad propia por agente; permisos vía Conditional Access for Agents (preview).

#### TRANSFORMAR

##### 365 Copilot • Copilot Studio • Microsoft Foundry

Llevan la IA generativa y agéntica al trabajo diario. Foundry construye y orquesta agentes y modelos a escala.

**Identidad sin gobierno es un riesgo sin nombre; gobierno sin identidad es una política sin dientes; y ninguna de las dos genera valor sin adopción real.**

**La tecnología hace posible esta transformación. Pero saber qué gobernar, cómo protegerlo, implementarlo, operarlo y adoptarlo requiere algo más que tecnología.**

Requiere capacidad de ejecución.

**Ahí es donde entra ONESEC.**

## 07 — ENTERPRISE SECURE AI BUSINESS TRANSFORMATION

# El gobierno hace que la transformación sea confiable. La transformación convierte la IA en valor de negocio.

**Enterprise Secure AI Business Transformation** es el nombre que ONESEC le ha dado al conjunto de capacidades que ayudan a convertir la IA en una capacidad real del negocio: identificar dónde puede generar valor, preparar los datos y la seguridad, incorporar agentes de forma responsable y establecer los controles necesarios para escalar con confianza.

*Enterprise Secure AI Business Transformation no es el nombre de un producto — es la trayectoria completa que conecta cada pieza en una sola respuesta integral.*

### 1 · IDENTIFICAR

**Dónde la IA  
genera valor**

### 2 · PREPARAR

**Datos,  
identidad y  
seguridad**

### 3 · TRANSFORMAR

**De  
experimentos  
a capacidades**

### 4 · ESCALAR

**Operar, medir  
y mejorar**

## Capacidad Empresarial de IA

Segura · Gobernada · Operable · Escalable

La IA genera valor cuando puede convertirse en una capacidad que la empresa puede confiar, operar y escalar.

## 08 — DE LA ESTRATEGIA A LA TECNOLOGÍA Y LA OPERACIÓN

### Core Offerings de ONESEC, alineadas a las plataformas de Microsoft

Cada organización necesita un camino diferente para transformar su negocio con IA. Enterprise Secure AI Business Transformation permite construir ese camino combinando las capacidades de ONESEC que cada empresa necesita, de acuerdo con su madurez, prioridades, objetivos y punto de partida.

**ONESEC empieza donde está el cliente: la combinación de Core Offerings depende de su situación actual, no de un paquete fijo.**

#### 01 · Cloud & AI Platforms

Base de Datos para IA ·  
Modernización de Plataformas de Datos

#### 02 · AI Business Solutions

Transformación Empresarial con IA · Adopción y  
Habilitación de Copilot

#### 03 · Security

Gobierno de IA Empresarial ·  
Servicios de Seguridad Administrados · Modernización de Ciberseguridad



Enterprise Secure AI Business Transformation

Transformación segura y operable

La tecnología por sí sola no genera transformación. El resultado de negocio surge cuando ONESEC la convierte en capacidades diseñadas, gobernadas, seguras y operables alrededor de la estrategia de cada cliente.

## 09 — ONESEC + TWINFACT + UDE: EL ECOSISTEMA DE TRANSFORMACIÓN

# ONESEC integra estas capacidades dentro de un solo ciclo de vida de transformación

ONESEC se ha convertido en un grupo de empresas capaces de conectar estrategia, datos, nube, ciberseguridad, gobierno, implementación, operaciones y adopción dentro de un mismo ciclo de vida.

*"Independientes por diseño. Integradas por estrategia."*



Datos, conocimiento e IA sobre Microsoft Fabric y Copilot.



Ciberseguridad, identidad y gobierno de la transformación.



Adopción, cultura y habilitación organizacional.

**El cliente puede activar las capacidades que necesita de manera independiente o integrarlas bajo una misma estrategia de transformación.**

## 10 — PROFUNDIDAD PROFESIONAL

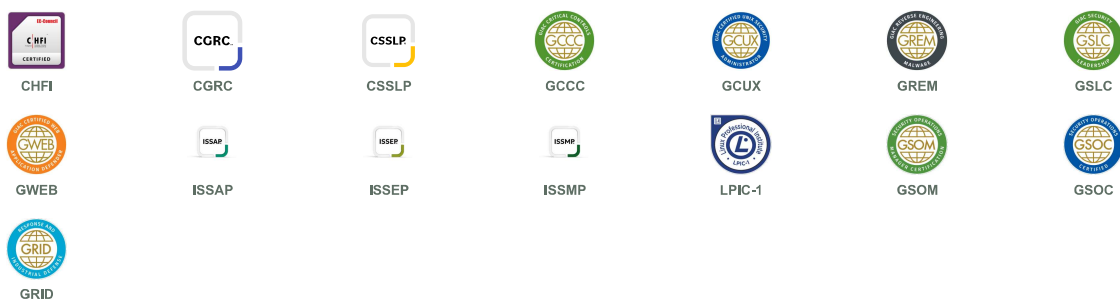
### Profundidad profesional para transformar, proteger y operar

ONESEC sostiene **más de 60 certificaciones de industria** en ciberseguridad, operación, administración y mejores prácticas, distribuidas en el equipo. Muestra representativa a continuación, agrupada por disciplina.

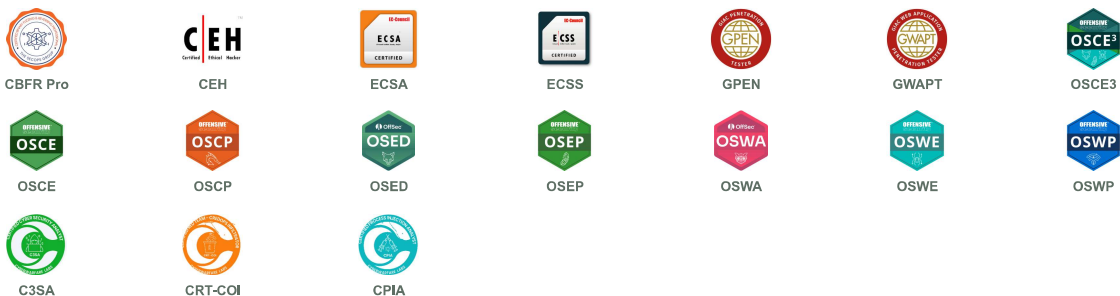
#### Mejores prácticas



#### Defensiva



#### Ofensiva



#### Gobierno y seguridad de IA



## 11 — ¿QUÉ PUEDE HACER ONESEC CON ESTA PROFUNDIDAD?

# Capacidades de ejecución

### Consultoría de Ciberseguridad / GRC

Estrategia · Riesgo · Gobierno · Cumplimiento ·  
Arquitectura · Advisory.

### Operaciones de Seguridad

SOC · MDR · Monitoreo · Detección ·  
Investigación · Respuesta.

### Servicios Administrados

Administración · Operación continua · Soporte  
· Optimización.

### Transformación y Delivery

Diseño · Arquitectura · Implementación ·  
Integración · Evolución.

Estas capacidades pueden ejecutarse sobre Microsoft y también mediante un ecosistema tecnológico más amplio, según la estrategia y necesidades del cliente.

## 12 — PRUEBA: CAPACIDADES, CREDENCIALES Y ECOSISTEMA

### Reconocimiento de Microsoft, profundidad técnica y confianza institucional

ONESEC es **Microsoft Solutions Partner**, con Advanced Specializations vigentes en identidad y acceso, seguridad de datos, protección contra amenazas, seguridad en la nube, modernización de endpoints y Copilot, y sostiene 4 Designations de Solutions Partner (Security, AI Business Solutions, Microsoft Cloud, Cloud & AI Platforms). También es **Microsoft Country Partner of the Year — México (2022–2023)**.

# 400+

certificaciones técnicas distribuidas en el equipo de ONESEC.



**ISO/IEC 27001 y SOC 2 Type II** respaldan la operación de ONESEC.

La profundidad de ONESEC no se mide en logos: se mide en la combinación de reconocimiento oficial de Microsoft, credenciales de industria, y un ecosistema tecnológico real detrás de cada capacidad descrita en este documento.

## 13 — SOBRE ONESEC + SIGUIENTE PASO

**ONESEC** es una plataforma empresarial integrada, con presencia en México, Colombia y Estados Unidos. Ayudamos a las organizaciones a convertir la tecnología en transformación segura, gobernada, adoptada y medible: gobernando el riesgo, asegurando la identidad y los datos, implementando sobre la plataforma correcta, operando con servicios administrados y monitoreo continuo, y logrando que las personas realmente adopten lo que se construyó. Junto con TwinFact y Un Día Extra acompañamos al cliente de principio a fin.

México

Colombia

Estados Unidos

## 14 — AI GOVERNANCE SELF-ASSESSMENT 2026

# ¿Su empresa está gobernando la IA al mismo ritmo al que la está adoptando?

La mayoría de las organizaciones puede responder cuánta IA está usando. Muy pocas pueden responder, con la misma certeza, si están preparadas para operarla, protegerla y escalarla con confianza. Ese autodiagnóstico hace visible esa distancia.

### Más que una encuesta de madurez.

Cada uno de sus **48 controles** tiene un nivel objetivo definido por el marco. El resultado es la distancia entre dónde está y dónde necesita estar, priorizada por lo que más importa resolver primero.

#### 01 • Gobernanza

Marco, roles y evidencia auditable.

#### 02 • Viabilidad

Caso de negocio real y medible.

#### 03 • Modelo

Apto, resistente y explicable.

#### 04 • Datos

Aptos, lícitos, trazables.

#### 05 • Seguridad

Resistencia adversaria.

#### 06 • Operación

Gobernada y reversible.

#### 07 • Monitoreo

Cumplimiento sostenido y demostrable.

#### 08 • Adopción

Personas y cambio organizacional.

Este autodiagnóstico no sustituye una evaluación detallada con su equipo, ni constituye una auditoría o certificación — es el primer paso para entender dónde está su organización.

**Realice su autodiagnóstico → [onesec.mx/autodiagnostico-gobierno-de-ia](https://onesec.mx/autodiagnostico-gobierno-de-ia)**

# Inicie su Transformación Empresarial Segura con IA.

Descargue este Executive Guide, complete su autodiagnóstico de preparación, o converse directamente con ONESEC.

[www.onesec.mx](https://www.onesec.mx)[onesec.mx/contacto](https://onesec.mx/contacto)

## SÍGANOS



**Facebook**  
[facebook.com/onesec.lat](https://facebook.com/onesec.lat)



**Instagram**  
[@onesec.lat](https://@onesec.lat)



**TikTok**  
[tiktok.com/@onesec.lat](https://tiktok.com/@onesec.lat)



**YouTube**  
[youtube.com/@onesec.lat](https://youtube.com/@onesec.lat)



[www.onesec.mx](https://www.onesec.mx) · [contacto@onesec.lat](mailto:contacto@onesec.lat) · Tel. +52 55 8525 4111 · WhatsApp +52 55 5069 5488

ONESEC Security Days México 2026 — Executive Guide v3.0. Enterprise Secure AI Business Transformation es nombre propio del Core Solution Play de ONESEC.

Todos los derechos reservados. Secure Nextgen Systems 2026. ONESEC, TWINFACT y UN DÍA EXTRA son marcas registradas.