

evolutio
Empowering secure AI

IBM
Platinum Partner

Accesos seguros en la era de la IA agéntica

Cómo proteger usuarios, aplicaciones y agentes de IA bajo un modelo Zero Trust

Índice

01 La IA agéntica convierte la identidad en el nuevo perímetro

02 Cuatro riesgos que cambian el modelo de acceso

03 Zero Trust para un mundo de agentes

04 IBM Verify: identidad y acceso para el nuevo entorno digital

05 Evolutio + IBM: de la tecnología al modelo de Identity Security

06 Identidad y operaciones de seguridad convergen

07 Cómo empezar

08 Conclusiones

evolutio | IBM Platinum Partner

01 La IA agéntica convierte la identidad en el nuevo perímetro

Durante años, el modelo de acceso empresarial ha partido de una relación relativamente sencilla: **una persona se identifica y accede a una aplicación, un sistema o un recurso**. La IA agéntica introduce un nuevo elemento en esta relación.

Un agente puede recibir una instrucción y, a partir de ella, **consultar información, utilizar herramientas, invocar APIs o ejecutar acciones** para alcanzar un objetivo. Para hacerlo, necesita acceder a recursos corporativos y, por tanto, necesita una identidad y unos permisos que determinen qué puede hacer.

La relación ya no se limita a un usuario que accede directamente a una aplicación. Ahora puede intervenir un agente que **actúa en nombre de una persona o de un proceso, utiliza credenciales y permisos propios y se relaciona con múltiples aplicaciones, APIs, datos y sistemas.**

La identidad ya no pertenece únicamente a las personas.

En un entorno con IA agéntica, también hay que identificar, autorizar y supervisar a las entidades que actúan en su nombre.

Este cambio plantea nuevas preguntas para la seguridad.

- **¿Qué agente está actuando?**
- **¿En nombre de quién?**
- **¿Qué puede hacer?**
- **¿A qué recursos puede acceder y durante cuánto tiempo?**
- **¿Quién ha autorizado la acción?**
- **¿Cómo queda registrada?**

La cuestión no es solo identificar al agente, sino poder relacionar su actuación con una identidad, una autorización y un contexto concreto.

Una nueva dimensión de la identidad

La magnitud del cambio empieza a ser visible también en las cifras. Según el **2026 Identity Security Landscape** de Palo Alto Networks, las organizaciones gestionan **109 identidades de máquina por cada identidad humana**. El informe, basado en una encuesta a 2.930 responsables de ciberseguridad a nivel mundial, sitúa a las identidades de máquina muy por encima de las humanas.

La cifra no implica que todas esas identidades tengan el mismo nivel de autonomía o riesgo. Sí refleja, sin embargo, una realidad cada vez más evidente: **el ecosistema digital ya no está formado únicamente por personas y aplicaciones.** Servicios, automatizaciones, máquinas y agentes necesitan también identidades para interactuar con los recursos de la organización.

Esta evolución ya está siendo abordada desde el ámbito de los estándares y las buenas prácticas. En 2026, el **National Institute of Standards and Technology (NIST)** publicó un documento conceptual específico sobre **la identidad y autorización de agentes de software y de IA**, planteando cuestiones como su identificación, autenticación, autorización, mínimo privilegio, delegación, relación entre la identidad humana y la del agente y auditoría de sus acciones.

La identidad se convierte así en una **capa de control que debe acompañar a cualquier entidad capaz de actuar dentro del ecosistema digital.**

Y esto supone **ampliar el alcance de la Identity Security**: ya no se trata únicamente de proteger el acceso de los usuarios, sino de gobernar también las identidades no humanas que interactúan con aplicaciones, APIs, datos, automatizaciones y agentes de IA.

Cuanto mayor sea la capacidad de actuación de un agente, mayor será también la necesidad de conocer **quién es, qué puede hacer y bajo qué condiciones puede hacerlo.**

Ese es el punto de partida para entender los nuevos riesgos que introduce la IA agéntica.

evolutio | IBM Platinum Partner

02 Cuatro riesgos que cambian el modelo de acceso

La incorporación de agentes de IA no crea todos los riesgos desde cero. Muchos ya forman parte de la gestión tradicional de identidades y accesos. Lo que cambia es **la capacidad de los agentes para actuar de forma automatizada, encadenar acciones y acceder a diferentes recursos para alcanzar un objetivo.**

Por eso, trasladar directamente los modelos de acceso pensados para usuarios humanos no siempre es suficiente.

Hay cuatro riesgos especialmente relevantes:

EXCESO DE PRIVILEGIOS

Un agente necesita permisos para realizar una tarea, pero el riesgo aparece cuando esos permisos son **más amplios, más duraderos o más difíciles de controlar de lo necesario.**

Su capacidad para actuar de forma automatizada puede ampliar el impacto de una credencial comprometida o de una acción inesperada.

El acceso debe limitarse a lo necesario para cada tarea, recurso y momento.

DELEGACIÓN INVISIBLE

Un agente puede actuar en nombre de una persona, pero esa relación **no debería quedar oculta detrás de una cuenta técnica.**

La organización debe poder saber **quién inició la solicitud, qué agente intervino y con qué autorización actuó**. Sin esta trazabilidad, una acción del agente puede terminar siendo indistinguible de una acción realizada directamente por una identidad técnica.

La delegación debe ser explícita, limitada y trazable.

PÉRDIDA DE CONTROL EN TIEMPO REAL

Un agente puede interactuar con diferentes aplicaciones, APIs, fuentes de información y herramientas durante una misma tarea. Una **autorización concedida** al inicio puede no ser suficiente para controlar todo lo que sucede después.

Por eso, el acceso debe poder adaptarse **a la acción y al contexto en el que se produce**, especialmente cuando cambia el nivel de riesgo.

La autorización no debería ser estática cuando la acción tampoco lo es.

SHADOW AI Y NUEVAS IDENTIDADES NO GOBERNADAS

La **rápida adopción de IA** puede llevar a los equipos a desplegar agentes y automatizaciones fuera de los procesos corporativos habituales: con nuevas credenciales, conexiones a APIs y permisos que no siempre están inventariados o supervisados.

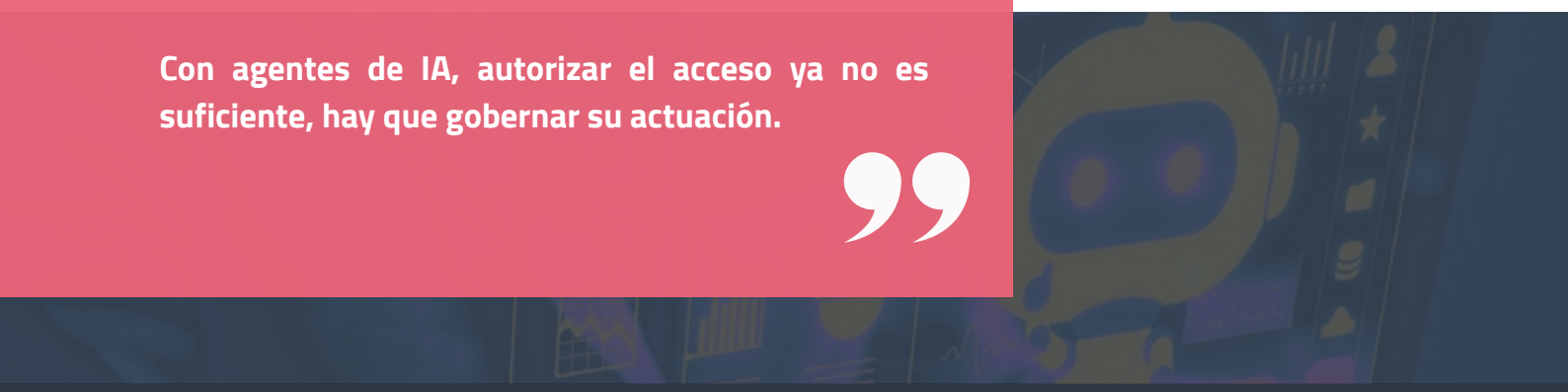
El reto no es solo saber qué agentes existen, sino conocer **qué identidades utilizan, a qué recursos acceden, qué permisos tienen y quién es responsable de ellos.**

Toda identidad de agente necesita un propietario, un propósito y un modelo de gobierno.

Los cuatro riesgos apuntan a una misma necesidad: el acceso de un agente debe poder conocerse, limitarse y controlarse durante todo su ciclo de actuación. No basta con saber que un agente está autorizado. Hay que poder determinar qué puede hacer, en nombre de quién, en qué contexto y durante cuánto tiempo.

Ese es precisamente el reto que aborda un modelo de Zero Trust aplicado a un entorno de agentes.

Con agentes de IA, autorizar el acceso ya no es suficiente, hay que gobernar su actuación.



evolutio | IBM Platinum Partner

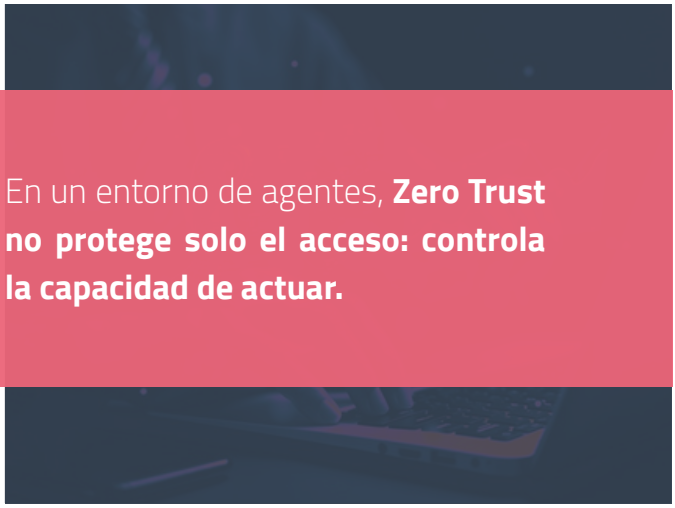
03 Zero Trust para un mundo de agentes

Zero Trust parte de un principio sencillo: **ningún acceso debe considerarse confiable por defecto.**

En un entorno tradicional, esto implica verificar la identidad, evaluar el contexto y conceder únicamente los permisos necesarios. En un **entorno agéntico**, los mismos principios **deben aplicarse también a las identidades no humanas** y, especialmente, a las acciones que realizan los agentes.

La autenticación inicial de un usuario o de un agente **no garantiza** que todas las acciones posteriores sean legítimas.

Un agente puede recibir una instrucción, acceder a una aplicación, consultar información y utilizar una API para completar una tarea. Cada una de estas interacciones puede implicar **diferentes recursos, permisos y niveles de riesgo.**



En un entorno de agentes, **Zero Trust no protege solo el acceso: controla la capacidad de actuar.**

Por eso, Zero Trust debe evolucionar desde la simple verificación de quién accede hacia una evaluación continua de **quién actúa, en nombre de quién, qué quiere hacer, sobre qué recurso, en qué contexto y durante cuánto tiempo.**

Aplicar este enfoque requiere trasladar los principios de Zero Trust a cada etapa de la actuación de un agente. **No se trata de añadir controles aislados, sino de establecer un modelo coherente que permita verificar, limitar, autorizar, revocar y registrar sus acciones.**

Estos principios pueden concretarse en **siete ámbitos clave**:



VERIFICACIÓN CONTINUA: La identidad y las condiciones de acceso deben poder reevaluarse cuando cambia el contexto, especialmente antes de realizar **acciones sensibles o de mayor riesgo.** No se trata de asumir que una autorización inicial es válida indefinidamente.

MÍNIMO PRIVILEGIO: Un agente debe disponer únicamente de los permisos necesarios para realizar una tarea concreta. Esto implica evitar accesos excesivamente amplios y, siempre que sea posible, **limitar los permisos al recurso, acción y periodo necesarios.**

CREDENCIALES TEMPORALES: Las credenciales de larga duración aumentan el impacto potencial de una exposición. Cuando el caso de uso lo permite, resulta preferible utilizar **credenciales o tokens de corta duración y alcance limitado**, vinculados a la operación que debe realizar el agente.

AUTORIZACIÓN CONTEXTUAL: La decisión de permitir una acción debe tener en cuenta algo más que la identidad. También importan **el recurso solicitado, la operación que se quiere realizar, el contexto y el nivel de riesgo.** Esto permite diferenciar entre acciones aparentemente similares que, sin embargo, pueden tener consecuencias muy distintas para la organización.

REVOCACIÓN: El acceso debe poder retirarse cuando deja de ser necesario o cuando cambian las condiciones que lo justificaban. En un entorno donde los agentes pueden actuar de forma autónoma durante una tarea, la **capacidad de interrumpir o revocar** sus permisos es especialmente relevante.

evolutio | IBM Platinum Partner



06

TRAZABILIDAD DE EXTREMO A EXTREMO: Cada acción debe poder relacionarse con **la identidad que la ejecuta, la identidad en cuyo nombre se realiza, el recurso al que se accede y la autorización que la permite.** La trazabilidad no solo facilita la auditoría posterior. También permite investigar comportamientos anómalos y entender cómo se ha producido una determinada actuación.

07

DEL ACCESO A LA ACCIÓN: Aplicar Zero Trust a agentes supone, por tanto, cambiar ligeramente el foco. No basta con proteger **quién entra**. Hay que controlar también **qué puede hacer una identidad una vez que está dentro del entorno.** Esto es especialmente importante cuando un agente puede encadenar diferentes acciones para alcanzar un objetivo. La confianza no debería heredarse automáticamente de una interacción a la siguiente: cada acción debe estar condicionada por **identidad, autorización, contexto y alcance.**

El objetivo no es impedir que los agentes actúen, sino establecer los controles necesarios para que puedan hacerlo **dentro de unos límites definidos, verificables y revocables.**

En este modelo, **Zero Trust** deja de ser únicamente un principio aplicado al acceso de usuarios y se convierte en una forma de **gobernar la capacidad de actuación de las identidades humanas y no humanas.**

Y para hacerlo realidad, esos principios deben trasladarse a la arquitectura, las aplicaciones, las APIs y los sistemas que forman parte del entorno digital. **Ahí es donde entra en juego la capa de identidad.**

04 IBM Verify: identidad y acceso para el nuevo entorno digital

Los principios de **Zero Trust** necesitan una capa tecnológica capaz de llevarlos a la práctica en todo el ecosistema de identidad.

En un entorno donde conviven **usuarios, aplicaciones, servicios, automatizaciones y agentes de IA,** esa capa debe permitir no solo autenticar identidades, sino también gestionar sus permisos, controlar las delegaciones, adaptar el acceso al contexto y mantener la trazabilidad de las acciones.

IBM Verify proporciona capacidades para gestionar y proteger identidades humanas y no humanas, con funciones de autenticación, evaluación adaptativa del riesgo, gobierno del ciclo de vida, delegación, consentimiento y auditoría.

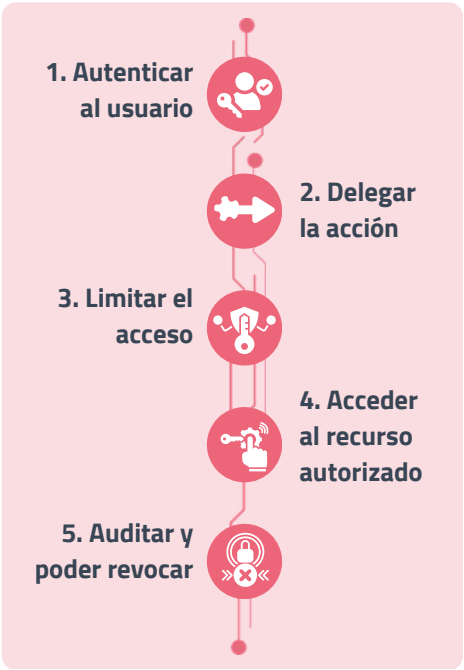
En el **ámbito de la IA agéntica**, **IBM** incorpora además capacidades orientadas a gestionar la identidad de los agentes, sus autorizaciones y sus interacciones con los recursos corporativos.

La aplicación de estos principios puede entenderse mejor a través de un caso práctico:

Caso práctico: un agente que necesita acceder a información corporativa

Imaginemos un **agente de soporte** que necesita consultar información de clientes para responder a una solicitud.

El objetivo no debería ser proporcionarle una credencial permanente con acceso amplio a una base de datos. El acceso puede estructurarse de forma que la identidad de la persona, la identidad del agente, el propósito de la acción y los permisos necesarios **estén relacionados durante todo el proceso.**



evolutio | IBM Platinum Partner

05 Evolutio + IBM: de la tecnología al modelo de Identity Security

La adopción de un **modelo de identidad preparado para la IA agéntica** no se resuelve únicamente incorporando una nueva tecnología. Requiere entender **qué identidades existen, qué pueden hacer, cómo se relacionan entre sí y cómo se controla su actividad** dentro del entorno tecnológico de cada organización.

Aquí es donde la tecnología y el conocimiento del entorno deben ir de la mano. **IBM aporta las capacidades tecnológicas de identidad. Evolutio diseña, integra y opera el modelo que permite aplicarlas de forma segura al negocio real de cada organización.**

El punto de partida es conocer el ecosistema completo. Ya no basta con identificar a los usuarios y las aplicaciones tradicionales. Es necesario considerar también **servicios, automatizaciones, APIs, credenciales, agentes de IA e identidades no humanas**, así como las relaciones de acceso entre ellos.

De conocer las identidades a gobernar su actividad

El primer paso es obtener una visión del entorno: qué identidades existen, quién es responsable de ellas, a qué recursos acceden, con qué privilegios y bajo qué condiciones.

Este análisis permite identificar situaciones como **privilegios excesivos, credenciales permanentes, identidades sin propietario claro o agentes y automatizaciones que han quedado fuera de los mecanismos habituales de gobierno.**



A partir de esta visión, **Evolutio** puede definir una arquitectura de **Identity Security** alineada con los principios de **Zero Trust** y con las necesidades concretas de cada organización.

Esto puede implicar combinar capacidades de **IAM, IGA, PAM y gobierno de identidades no humanas**, estableciendo políticas de acceso que tengan en cuenta no solo quién solicita una acción, sino también **qué identidad la ejecuta, para qué, sobre qué recurso y durante cuánto tiempo.**

Pero una arquitectura de identidad **no funciona de manera aislada**, sino que debe integrarse con las aplicaciones, APIs, directorios, entornos cloud y on-premise, sistemas corporativos y herramientas de seguridad que forman parte del ecosistema tecnológico.

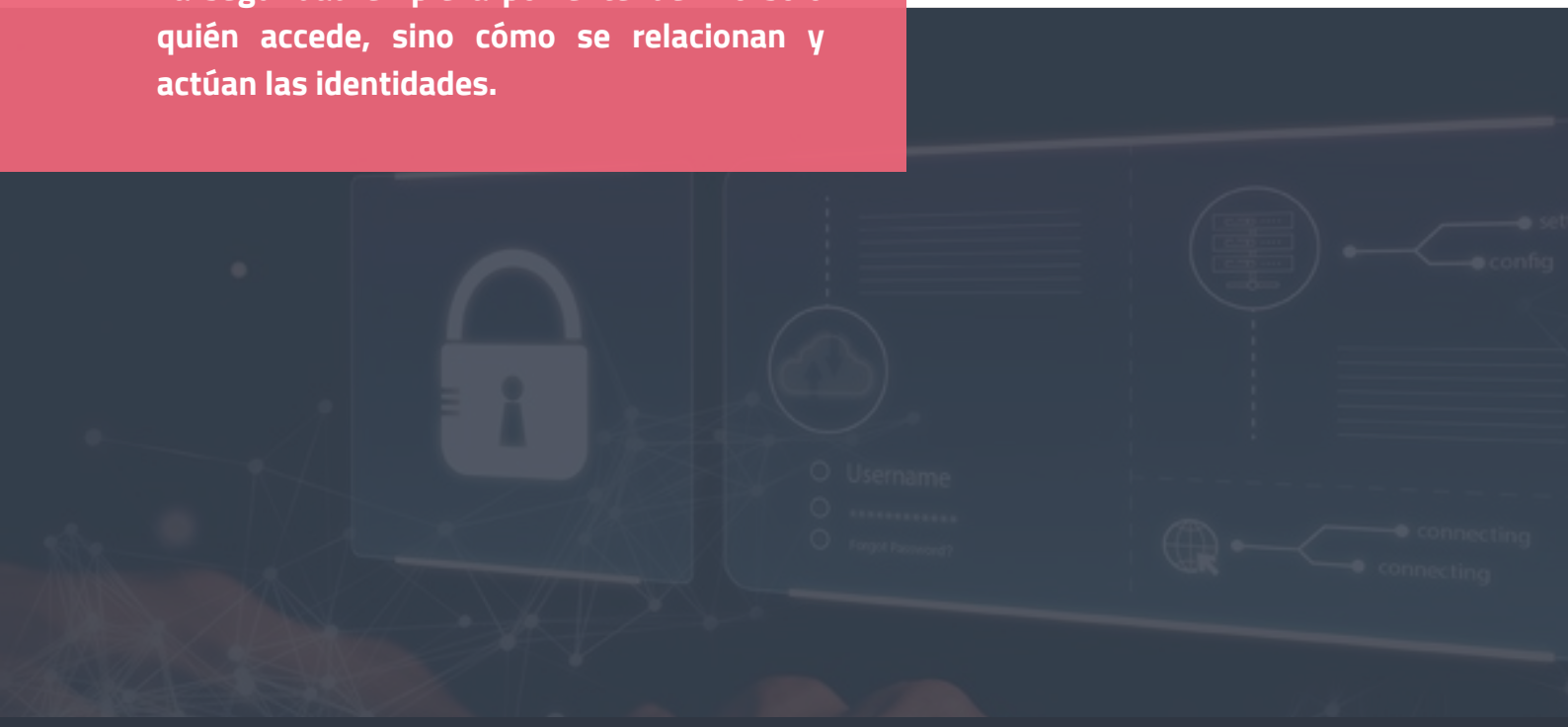
En un entorno agéntico, esta integración adquiere todavía más importancia: **la identidad debe acompañar a la acción allá donde se produzca.**

Por último, el modelo debe poder mantenerse y evolucionar.

La revisión de accesos, la monitorización de la actividad, la detección de comportamientos anómalos, la automatización de respuestas y la coordinación con las operaciones de seguridad permiten pasar de una gestión puntual de identidades a un **modelo continuo de gobierno y protección**.

El resultado no es únicamente una plataforma de identidad, sino una capacidad integrada de seguridad que permite a la organización saber **qué puede hacer cada identidad, en qué contexto y con qué nivel de control.**

La seguridad empieza por entender no solo quién accede, sino cómo se relacionan y actúan las identidades.



06 Identidad y operaciones de seguridad convergen

La **evolución hacia agentes de IA** no afecta únicamente a la forma en que las organizaciones gestionan los accesos. También está transformando la manera de operar la seguridad.

Durante años, los equipos de SOC han incorporado automatización, orquestación y herramientas de apoyo a la investigación. La incorporación de capacidades de IA permite avanzar hacia un modelo en el que **la tecnología no solo ayuda a analizar la información, sino que puede asumir determinadas tareas de investigación y respuesta.**

El cambio más relevante no está tanto en las herramientas como en **el papel que desempeñan las personas y los sistemas en cada fase de la operación.**

En un **modelo tradicional**, el analista recibe una alerta, recopila información, investiga lo ocurrido y decide qué respuesta aplicar. La **automatización** permite ejecutar tareas repetitivas y la orquestación coordina diferentes acciones y herramientas.

Con capacidades de IA, el modelo puede evolucionar hacia una operación copilotada, en la que el analista mantiene el liderazgo mientras la IA **resume información, relaciona señales, propone hipótesis y recomienda acciones.**

En este contexto, determinados agentes pueden asumir una parte mayor de ese proceso: **investigar una alerta, consultar diferentes fuentes, correlacionar información y ejecutar acciones de respuesta dentro de unas políticas y límites previamente definidos.**



No se trata, por tanto, de sustituir el papel del analista, sino de **desplazar progresivamente hacia los agentes aquellas tareas que pueden realizarse de forma automatizada y controlada, manteniendo la supervisión humana allí donde sea necesaria.**

Este cambio introduce una conexión directa con lo que hemos visto en los capítulos anteriores.

Un agente que investiga una alerta, consulta información sensible o ejecuta una acción de respuesta **también es una identidad que debe ser autenticada, autorizada y auditada.**

Por eso, la evolución del SOC y la evolución de Identity Security empiezan a converger. Cuanto mayor sea la capacidad de un agente para actuar de forma autónoma, mayor será la necesidad de controlar **qué puede hacer, sobre qué sistemas puede actuar y bajo qué condiciones.**

Del SOC automatizado al SOC agéntico

El modelo de **Agentic SOC de Evolutio** parte de esta evolución y combina las capacidades de las operaciones de seguridad con mecanismos de automatización e inteligencia para facilitar la investigación y la respuesta.

En este entorno **pueden convivir las personas y los agentes** con las diferentes fuentes y herramientas de seguridad: SIEM, EDR, sistemas de identidad, firewalls, WAF, XDR, inteligencia de amenazas, cloud, SaaS, gestión de vulnerabilidades, observabilidad y otras fuentes de información.

El valor no está en sumar herramientas, sino en **conectar la información y las capacidades de actuación.**

Un agente puede, por ejemplo, recibir una alerta, relacionarla con información procedente de diferentes sistemas, investigar su contexto y proponer o ejecutar determinadas acciones de respuesta. **Cada una de esas acciones debe mantenerse dentro de los límites establecidos y quedar registrada.**

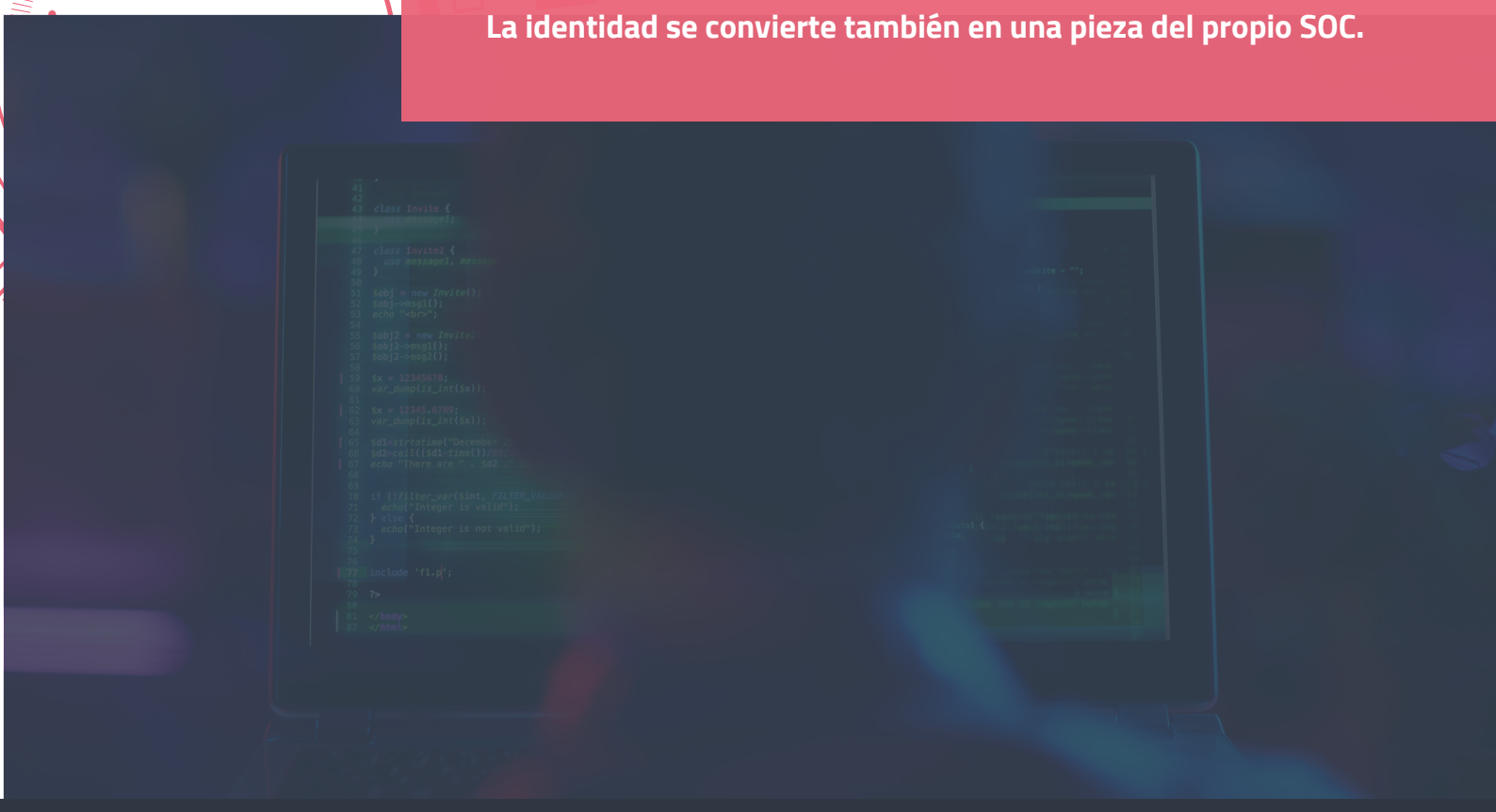
Por eso, **la identidad se convierte también en una pieza del propio SOC**.

La misma arquitectura que permite **controlar el acceso** de un agente a los recursos corporativos debe permitir **gobernar su actividad** cuando participa en una investigación o en una respuesta de seguridad.

El resultado es una convergencia entre dos capacidades que tradicionalmente se han gestionado de manera más separada: **quién puede acceder y qué puede hacer una identidad y qué puede ejecutar un sistema de seguridad ante una amenaza.**

En la **era agéntica**, ambas preguntas forman parte de la misma conversación.

La identidad se convierte también en una pieza del propio SOC.



evolutio | IBM Platinum Partner

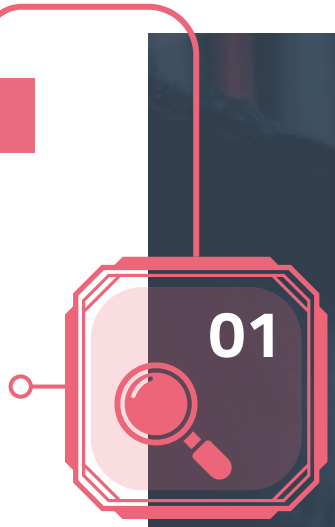
07 Cómo empezar

La adopción de este modelo no requiere transformar todo el entorno tecnológico de una organización de una sola vez. El punto de partida es **entender dónde se encuentran las identidades y los accesos que necesitan mayor control, y avanzar desde ahí.**

DESCUBRIR

El primer paso es construir una visión del ecosistema de identidades. Esto incluye **usuarios, aplicaciones, servicios, APIs, automatizaciones, agentes de IA, credenciales y privilegios,** identificando además sus relaciones con los recursos corporativos.

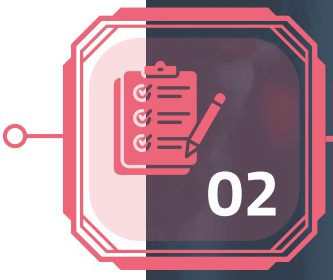
Sin esta **visibilidad**, resulta difícil determinar qué accesos son necesarios y cuáles representan una exposición innecesaria.



EVALUAR

Con el **inventario disponible**, es necesario analizar **cómo se utilizan esas identidades**. ¿Existen privilegios superiores a los necesarios? ¿Hay credenciales permanentes allí donde podrían utilizarse accesos temporales? ¿Existen agentes o automatizaciones sin propietario definido? ¿Se pueden reconstruir las acciones realizadas y saber en nombre de quién se ejecutaron?

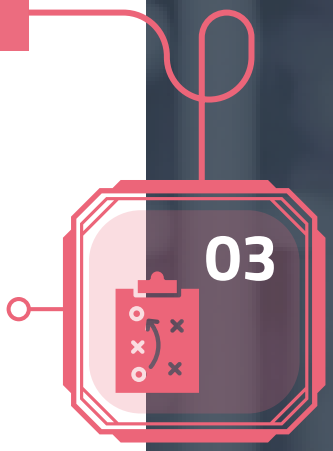
Esta evaluación permite **priorizar los riesgos y determinar dónde aplicar primero los controles**.



DISEÑAR

El siguiente paso es definir el modelo de **Identity Security** que debe sostener el entorno. Aquí se concretan los principios de **Zero Trust, mínimo privilegio, autorización contextual, delegación controlada, credenciales temporales y trazabilidad**, adaptándolos a las características de cada organización.

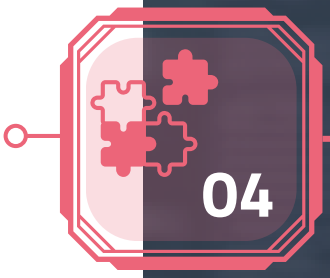
La arquitectura debe contemplar **tanto las identidades humanas como las no humanas** y establecer cómo se relacionan entre ellas.



INTEGRAR

El modelo debe llegar a los sistemas donde realmente se producen las acciones. Esto implica integrar las capacidades de identidad con **aplicaciones, APIs, directorios, cloud, infraestructura, plataformas de seguridad y agentes o automatizaciones**.

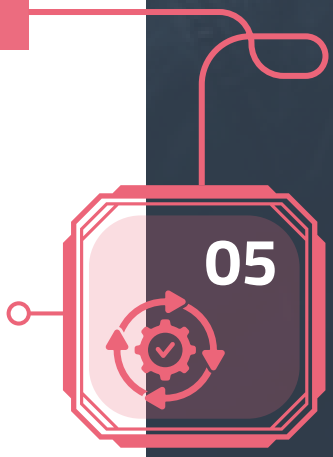
La integración permite que las políticas de acceso no se queden en una capa teórica, sino que puedan aplicarse y verificarse en las operaciones reales.



OPERAR Y EVOLUCIONAR

La identidad no es un proyecto que termina cuando se configura una plataforma. Los accesos cambian, aparecen nuevas aplicaciones y agentes, se modifican los riesgos y evolucionan las propias capacidades de IA. Por eso, el modelo debe mantenerse mediante **monitorización, revisión de accesos, detección de anomalías, automatización y respuesta,** incorporando nuevos controles a medida que cambia el entorno.

El objetivo es pasar de una gestión estática de los accesos a un **modelo continuo de gobierno de las identidades y de sus acciones.**



08 Conclusiones

La **IA agéntica** amplía de forma significativa el número de identidades capaces de interactuar con los sistemas de una organización y, con ello, el alcance de lo que debe protegerse.

El perímetro ya no está formado únicamente por usuarios y dispositivos. Incluye **personas, aplicaciones, APIs, automatizaciones y agentes de IA**, todos ellos capaces de participar en procesos que afectan a datos y recursos corporativos.

En este contexto, **Identity Security** y **Zero Trust** proporcionan los principios para establecer **quién puede actuar, en nombre de quién, sobre qué recursos, con qué permisos y durante cuánto tiempo.**

La tecnología permite llevar estos principios a la práctica. **IBM aporta las capacidades de identidad y acceso; Evolutio diseña, integra y opera el modelo de seguridad que las conecta con el entorno real de cada organización.**

Y esta evolución no termina en la gestión de accesos: a medida que los agentes participan también en las operaciones de seguridad, **Identity Security y SOC convergen** para controlar no solo quién puede acceder, sino también quién puede investigar, decidir y ejecutar acciones.

El reto no consiste en impedir que los agentes actúen. Consiste en conseguir que puedan hacerlo **dentro de límites definidos, verificables y revocables**.

Porque en la era de la IA agéntica, **cada agente es una nueva identidad, y cada identidad debe estar gobernada.**

Dé el primer paso hacia una Identity Security más segura.

evolutio.com 91 270 6000 info@evolutio.com

evolutio | IBM Platinum Partner