evolutio
Empowering a secure cloud

Ciberseguridad en la era de la inteligencia artificial: protección inteligente de accesos privilegiados en entornos híbridos_

La gestión avanzada de accesos privilegiados, combinada con IA, refuerza la seguridad en las organizaciones

Índice

01 El nuevo escenario: ciberseguridad en tiempos de IA, automatización y multicloud

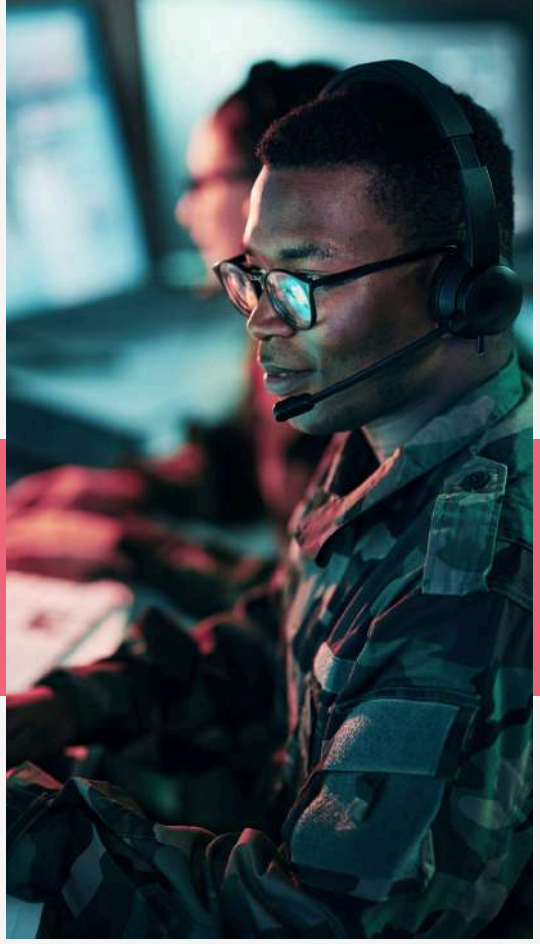
Vivimos un momento apasionante, pero también desafiante, para la ciberseguridad empresarial. La **transformación digital** ha reconfigurado de raíz los ecosistemas tecnológicos, impulsando la adopción de **arquitecturas híbridas**, **entornos multicloud** y el uso extendido de tecnologías como la **inteligencia artificial (IA)** y la **automatización**.

Esta evolución ofrece a las organizaciones un potencial sin precedentes para innovar, escalar y optimizar sus operaciones, pero también **multiplica los vectores de exposición** a amenazas cada vez más sofisticadas.

La consolidación de **entornos híbridos y multicloud** ha dejado atrás el perímetro tradicional de seguridad.

Hoy, los datos y las aplicaciones **se encuentran dispersos** entre infraestructuras locales, múltiples proveedores de nube pública y los entornos privados. Esta nueva realidad **exige estrategias de protección más dinámicas** y adaptables, capaces de ofrecer visibilidad, control y respuesta en tiempo real a lo largo de toda la superficie de ataque.

A la vez, la adopción acelerada de la **inteligencia artificial** y la **automatización** está transformando tanto la forma en que operan los negocios como la manera en que los atacantes diseñan sus **ciberamenazas**.



Las herramientas impulsadas por IA permiten a las empresas **analizar grandes volúmenes de datos**, detectar anomalías y responder con rapidez a incidentes.

Sin embargo, esta flexibilidad trae consigo un aumento significativo en la superficie de ataque y una **diversificación de las amenazas**, poniendo a prueba los enfoques tradicionales de ciberseguridad.

En este contexto, **los accesos y credenciales privilegiadas** adquieren un protagonismo especial. Ya no son solo un componente más de la arquitectura de seguridad, sino auténticos puntos críticos que, en caso de ser comprometidos, pueden otorgar a los atacantes **acceso devastador** a sistemas sensibles, datos confidenciales y recursos estratégicos.

De hecho, según el informe M-Trends 2025 de **Mandiant**, el uso de credenciales robadas ya representa el segundo vector de ataque más común, implicado en el **16% de los incidentes analizados**, solo por detrás de la explotación de vulnerabilidades.

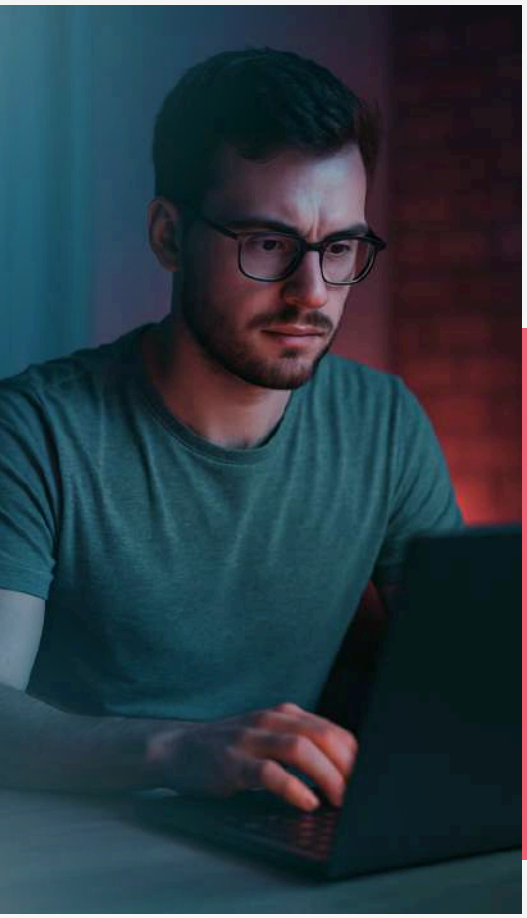
Además, el **41% de las brechas** de seguridad que tuvieron lugar durante el año 2024 estuvieron relacionadas con **credenciales comprometidas,** llegando a consolidarse como **la principal causa** de los ataques por segundo año consecutivo.

Por tanto, **proteger y gestionar de forma avanzada** los accesos privilegiados no es solo una recomendación, sino una necesidad imperativa para cualquier organización que quiera garantizar su resiliencia digital en un mundo multicloud e impulsado por IA.

Este es **el punto de partida** para adentrarnos en los retos y oportunidades que supone evolucionar hacia una protección inteligente de accesos en la era de la inteligencia artificial.

02 La amenaza silenciosa: credenciales privilegiadas como objetivo de alto valor

En el complejo **panorama de ciberamenazas actual**, los atacantes han aprendido a moverse con mayor sutileza y estrategia. Ya no se conforman con explotar vulnerabilidades técnicas al azar; ahora centran sus esfuerzos en las **credenciales privilegiadas**, auténticas llaves maestras de los sistemas críticos.



No es casualidad: quien controla una credencial privilegiada, **controla gran parte de la infraestructura** y, por tanto, el pulso digital de la organización.

El uso indebido de estos accesos ya sea por actores internos o externos, puede tener **consecuencias devastadoras**: desde la interrupción de operaciones hasta el robo de datos sensibles o el daño reputacional.

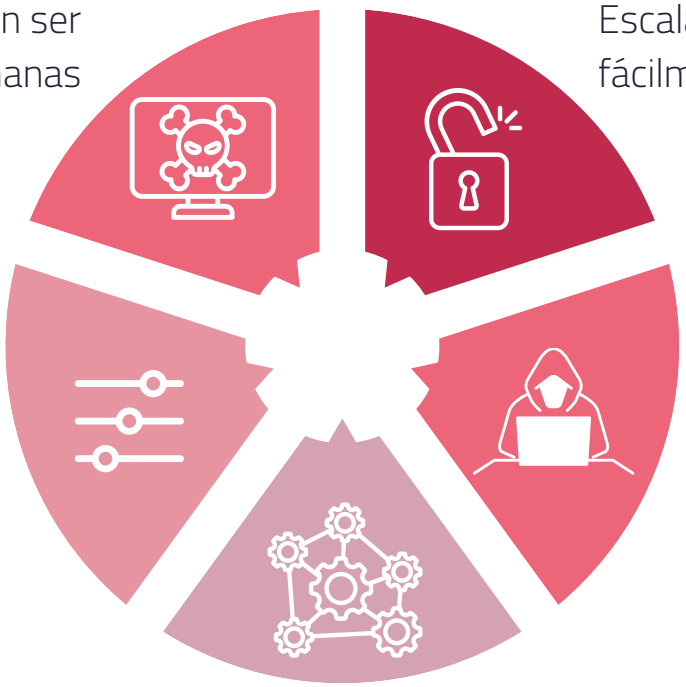
Casos recientes, como los **incidentes de Snowflake** (2024), **Change Healthcare** (2024) o **23andMe** (2023), ilustran cómo el robo o abuso de credenciales puede comprometer millones de registros personales y poner en jaque la continuidad del negocio.

En muchos de estos episodios, los atacantes **lograron acceder a sistemas críticos** a través de cuentas privilegiadas, eludiendo controles y escalando privilegios con sorprendente facilidad.

Las credenciales privilegiadas permiten **administrar sistemas críticos**, gestionar **bases de datos sensibles**, modificar **configuraciones** o incluso **desactivar controles de seguridad**. Su valor para un actor malicioso es incalculable: con una sola credencial comprometida, pueden desplazarse lateralmente dentro de la organización, escalar privilegios, ocultar su presencia y ejecutar ataques **que impactan directamente en la continuidad operativa** y en la reputación de la empresa.

¿Por qué las credenciales privilegiadas son un objetivo prioritario?

Porque permiten a un atacante:



Ejecutar ataques sin ser detectado durante semanas

Escalar privilegios fácilmente

Controlar y modificar configuraciones clave

Ocultar su presencia dentro del sistema

Moverse lateralmente entre sistemas

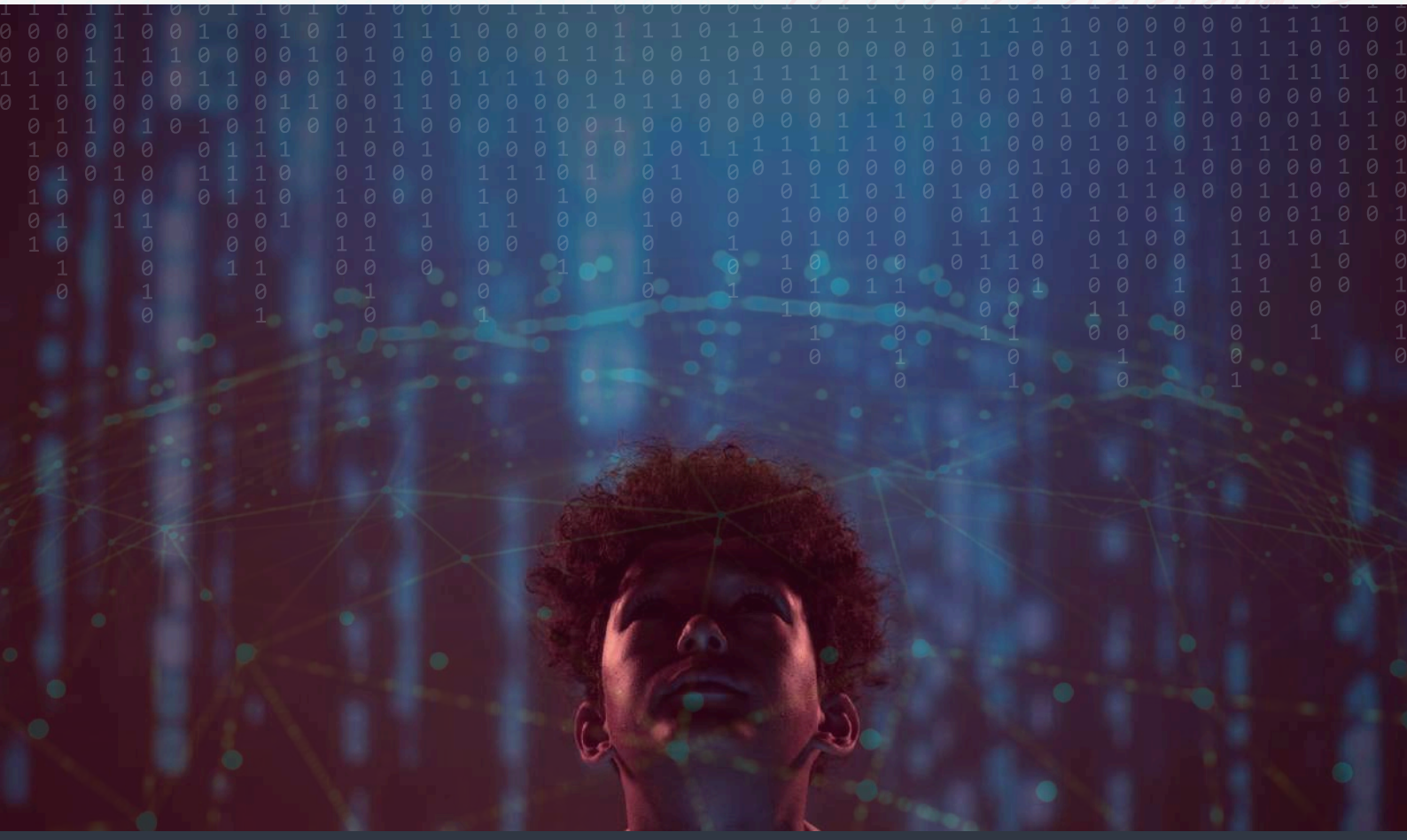
Esta tendencia preocupante se refleja también en los datos recientes. Según el **IBM Cost of a Data Breach Report 2024**, el coste medio global de una brecha de datos alcanzó los **4,88 millones de dólares**, el mayor incremento registrado desde la pandemia.

Además, los incidentes relacionados con el robo de credenciales **tardaron casi 300 días en ser detectados y contenidos**. Por otro lado, el informe destaca que las organizaciones que aplicaron IA y automatización lograron **reducir el coste de las brechas en más de 2 millones de dólares**.

No solo eso, sino que este vector fue el más frecuente, implicado en el **16% de las brechas** analizadas a nivel global.

No hablamos solo de amenazas teóricas. Los **accesos indebidos** a infraestructuras críticas y los incidentes en grandes plataformas tecnológicas han demostrado que el robo o abuso de credenciales privilegiadas **puede suponer pérdidas millonarias, sanciones regulatorias y una pérdida de confianza** difícil de recuperar.

Un acceso privilegiado comprometido no solo expone datos: **pone en juego la confianza** que la organización ha construido con clientes, socios y su propio equipo.



Además, la sofisticación de los atacantes hace que muchas de estas intrusiones **pasen desapercibidas** durante semanas o meses, amplificando sus consecuencias y dificultando su detección.

"Una credencial privilegiada comprometida no solo expone datos: pone en juego la confianza de toda la organización."

El impacto de estas brechas **va mucho más allá de las pérdidas financieras inmediatas:** afecta la confianza de clientes y socios, expone a las organizaciones a **sanciones regulatorias** y puede desencadenar litigios costosos.

Por ello, la protección de los accesos privilegiados se ha convertido en una **prioridad estratégica** para cualquier organización que gestione datos sensibles o cargas de trabajo intensivas.

Frente a esta amenaza silenciosa, resulta fundamental **replantear cómo protegemos**, **gestionamos** y **supervisamos** los accesos privilegiados. No basta con almacenarlos de forma segura o aplicar contraseñas robustas; **es necesario evolucionar** hacia modelos de protección más inteligentes, dinámicos y contextuales.

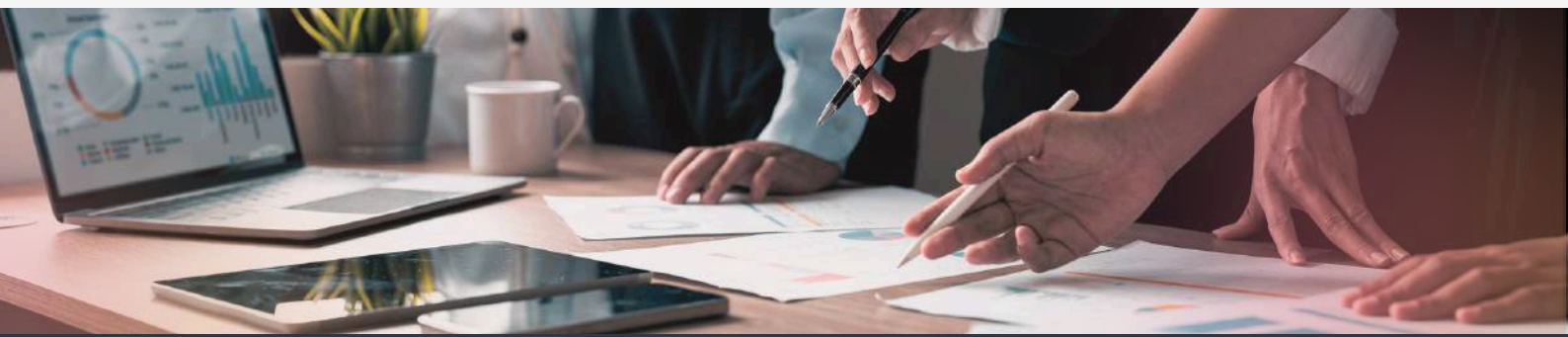
La buena noticia es que las nuevas capacidades **basadas en inteligencia artificial** abren el camino hacia una nueva generación de gestión de accesos privilegiados, donde la **prevención**, la **detección temprana** y la **respuesta automatizada** se convierten en aliados estratégicos para anticipar y mitigar riesgos antes de que se materialicen.

03 Limitaciones de las estrategias PAM tradicionales

Durante años, las soluciones tradicionales de **gestión de accesos privilegiados** (**PAM**, por sus siglas en inglés) han sido una pieza esencial de las **estrategias de ciberseguridad**. Custodiar contraseñas, gestionar accesos administrativos y registrar sesiones eran funciones suficientes en un entorno donde los activos estaban mayoritariamente **bajo control en infraestructuras on-premises**.

Sin embargo, **el escenario ha cambiado**. La adopción de entornos híbridos, la multiplicación de usuarios remotos y la integración de servicios cloud han convertido al modelo tradicional de PAM en una **herramienta insuficiente** para los desafíos actuales. Lo que antes era una barrera eficaz, hoy resulta un enfoque rígido, reactivo y limitado frente a amenazas dinámicas y persistentes.

La **aceleración digital** y la creciente **complejidad de los ecosistemas híbridos** han puesto en evidencia las limitaciones de estas soluciones. Aunque eficaces en su momento, **carecen de la adaptabilidad** y la inteligencia necesarias para anticipar y responder a amenazas sofisticadas en tiempo real.



Una de las principales debilidades radica en la **falta de visibilidad en tiempo real** y de **contexto dinámico**. Las plataformas clásicas pueden registrar quién accede y cuándo, pero no son capaces de interpretar **el por qué**, **el cómo** o si ese comportamiento **representa una amenaza potencial**. Sin una comprensión contextual de las acciones de los usuarios, la **capacidad de anticipar** y mitigar incidentes se ve seriamente comprometida.

Además, la **gestión de usuarios**, **sesiones** y **credenciales** sigue siendo, en muchos casos, un proceso manual o basado en reglas estáticas.

Esta rigidez no solo **ralentiza las operaciones de seguridad**, sino que aumenta el **riesgo de errores humanos,** especialmente en entornos donde la velocidad de reacción es crítica.

Otra limitación importante es la **escasa integración con tecnologías de detección y respuesta**, como los sistemas **SIEM** (Security Information and Event Management) y **SOAR** (Security Orchestration, Automation and Response). Esta desconexión impide que los sistemas PAM tradicionales **participen de forma activa** en la detección, análisis y respuesta frente a amenazas, aislándolos del resto del ecosistema de ciberseguridad.

A ello se suma que, en muchos casos, **su implementación resulta compleja** y lenta, lo que puede dejar expuestos a usuarios críticos durante largos periodos.

Aunque la grabación de sesiones **facilita la auditoría forense**, rara vez se revisa de forma proactiva, y la cobertura de cuentas privilegiadas no gestionadas continúa siendo **un punto ciego relevante**.

El **enfoque clásico basado únicamente en la identidad** —usuario y contraseña — resulta cada vez más **insuficiente**. En un mundo donde el riesgo varía en función de la ubicación, el dispositivo o el comportamiento detectado, la identidad estática ya no puede ser el único criterio de confianza.

Así, aunque el concepto de **PAM** sigue siendo **imprescindible**, su implementación necesita evolucionar para responder a las exigencias del nuevo contexto de amenazas.

No se trata simplemente de almacenar credenciales de forma segura: se trata de dotar a la gestión de accesos privilegiados de **inteligencia**, **adaptabilidad** y **capacidad de anticipación**.

Esta **desconexión** entre las capacidades de las **soluciones PAM tradicionales** y las **necesidades reales** de los entornos modernos está llevando a muchas organizaciones a buscar **enfoques más dinámicos**, **más inteligentes** y **más automatizados** para proteger los accesos críticos.

Antes de ahondar más en este nuevo modelo, es importante contrastar sus capacidades con las de un enfoque tradicional. Esta comparativa ilustra los **principales diferenciales entre ambos enfoques**:

Comparativa: PAM tradicional vs. PAM con IA

Característica	PAM tradicional	PAM con IA
Visibilidad en tiempo real	Limitada	Completa, contextual y dinámica
Detección de anomalías	Basada en reglas	Basada en análisis de comportamiento (UEBA)
Capacidad de respuesta	Manual y reactiva	Automatizada y proactiva
Integración con SIEM/SOAR	Parcial o inexistente	Nativa y bidireccional
Escalabilidad y eficiencia operativa	Limitada	Alta, con automatización inteligente
Experiencia de usuario	Rígida, con fricciones	Adaptativa y fluida
Capacidad de anticipación	Muy baja	Alta, basada en aprendizaje automático

Con este marco comparativo, podemos explorar cómo **la IA transforma el modelo PAM** en una **solución proactiva y estratégica** frente a las ciberamenazas.

Un cambio de paradigma que abre el camino hacia una gestión de accesos privilegiados reforzada con inteligencia artificial: Un modelo que **no solo protege**, sino que también **aprende**, **detecta y responde** de manera proactiva.

04 Evolución del modelo: gestión de accesos privilegiados con inteligencia artificial

La **evolución de las amenazas** y la **creciente complejidad** de los entornos tecnológicos han dejado claro que los modelos tradicionales de gestión de accesos privilegiados (PAM) **necesitan un salto cualitativo**.

Ya no basta con proteger los accesos: es imprescindible convertir la gestión de privilegios en un **elemento activo y estratégico de defensa** frente a ciberamenazas cada vez más sofisticadas.

Es en este contexto donde la **inteligencia artificial** (**IA**) emerge como catalizadora de una nueva generación de protección.

Análisis de comportamiento con UEBA

Integrar **capacidades de IA** en los sistemas de gestión de accesos privilegiados permite pasar de un enfoque reactivo a uno **predictivo y adaptativo**.

Las plataformas avanzadas ya no se limitan a registrar accesos y alertar a posteriori, sino que **analizan de forma continua** el comportamiento de usuarios y entidades, identifican patrones anómalos y son capaces de activar respuestas automáticas **en tiempo real** ante cualquier actividad sospechosa.

Uno de los mayores avances en este ámbito es la incorporación de **análisis de comportamiento de usuarios y entidades**, conocido como **UEBA** (User and Entity Behavior Analytics). Mediante algoritmos de machine learning, estas soluciones construyen perfiles de comportamiento normal para cada usuario o sistema y **detectan desviaciones** que, aunque no infrinjan una regla explícita, pueden anticipar riesgos inminentes.

Por ejemplo, una conexión desde una ubicación inusual o un acceso fuera del horario habitual puede activar automáticamente mecanismos de verificación o restricción, **anticipando posibles amenazas** antes de que se materialicen.

Respuestas automatizadas y adaptativas

La **automatización de respuestas** ante accesos sospechosos representa otro avance fundamental. Frente a una actividad anómala, el sistema **puede actuar sin intervención humana**: bloquear una sesión, solicitar un segundo factor de autenticación o aislar preventivamente al usuario para evitar un compromiso mayor.

Esta capacidad **reduce la dependencia del factor humano**, acelera la reacción ante incidentes y minimiza el impacto de posibles brechas.

Además, las **decisiones basadas en contexto** -como el dispositivo utilizado, la ubicación geográfica, el nivel de riesgo asociado o el historial de comportamiento reciente- permiten aplicar controles adaptativos y personalizados, reforzando la seguridad **sin sacrificar la experiencia de usuario**.

Optimización operativa

El uso de IA en la gestión de accesos privilegiados no solo fortalece la postura de seguridad, sino que también **contribuye a la eficiencia operativa**.

Al automatizar la supervisión y la respuesta ante incidentes, **se libera al personal de seguridad** de tareas repetitivas, permitiéndoles centrarse en actividades de mayor valor estratégico. A la vez, la experiencia de los usuarios legítimos se optimiza, **reduciendo fricciones innecesarias** y adaptándose de manera inteligente al ritmo de los negocios digitales actuales.

De hecho, según Gartner, **más del 50%** de los proveedores de seguridad **ya utilizan IA basada en machine learning** para mejorar la detección de amenazas avanzadas y reducir los falsos positivos en la gestión de accesos privilegiados. Además, la consultora destaca que **la incorporación de UEBA en el stack de seguridad** permite identificar ataques complejos -incluyendo amenazas internas y movimientos laterales- de forma mucho más eficiente que los sistemas tradicionales.

En definitiva, **la inteligencia artificial transforma la gestión de accesos privilegiados** en una herramienta activa de **detección y respuesta**, capaz de evolucionar al ritmo de las amenazas y de las necesidades del negocio. Así, la gestión inteligente de accesos privilegiados **se convierte en un aliado estratégico** para proteger activos críticos, anticipar amenazas y garantizar la continuidad operativa en **entornos híbridos y multicloud** cada vez más complejos.

05 Hoja de ruta para una estrategia PAM inteligente y sostenible

Adoptar una estrategia avanzada de gestión de accesos privilegiados no se trata únicamente de incorporar nuevas tecnologías, sino de **transformar la forma en que se concibe y gestiona la seguridad** en la organización.

Para que esta evolución sea efectiva y sostenible en el tiempo, **es clave contar con una hoja de ruta clara**, adaptada a las necesidades del negocio y alineada con los principios de ciberseguridad modernos:

PASO 1
Inventario y mapeo de cuentas privilegiadas

Identificar qué cuentas existen, quién las utiliza, a qué recursos tienen acceso y con qué frecuencia es la base para establecer controles eficaces. Este proceso debe incluir no solo usuarios humanos, sino también cuentas de servicio, scripts automatizados y accesos de terceros.

PASO 2
Aplicación del principio de mínimo privilegio

Garantizar que cada usuario —humano o máquina— tenga únicamente los accesos estrictamente necesarios para realizar su trabajo, durante el tiempo imprescindible. Es una de las medidas más eficaces para reducir la superficie de ataque y limitar el alcance de un posible compromiso.

PASO 3
Segmentación de red y controles de acceso contextual

En un entorno multicloud, donde los perímetros son difusos, es fundamental aplicar controles dinámicos que tengan en cuenta el contexto de cada acceso: la localización, el tipo de dispositivo, el horario o el nivel de riesgo asociado.

PASO 4
Integración con ecosistemas de seguridad y cumplimiento

Conexión con plataformas SIEM y SOAR para compartir inteligencia, activar respuestas automáticas y facilitar una visión unificada de los incidentes. La integración con soluciones de cumplimiento normativo ayuda a documentar acciones y demostrar trazabilidad.

PASO 5
Despliegue progresivo y formación continua

Adoptar un enfoque modular y revisiones periódicas. El contexto cambia, las amenazas evolucionan y las organizaciones crecen. Por ello, es clave actualizar políticas, revisar inventarios, ajustar privilegios y formar a los equipos.

Diseñar e implantar una **estrategia PAM inteligente** es una oportunidad para fortalecer la resiliencia digital desde la base. No solo se trata de controlar accesos: se trata de construir una **cultura de seguridad proactiva**, con herramientas inteligentes y procesos bien orquestados, capaces de proteger el núcleo operativo de la organización.

06

IBM Security: visión Zero Trust aplicada a PAM con IA

En un entorno donde la confianza tradicional ha dejado de ser una garantía, la **estrategia Zero Trust** se ha consolidado como el **nuevo estándar de seguridad**. Bajo este enfoque, no se asume que ningún usuario, dispositivo o proceso es confiable por defecto, y cada acceso debe ser verificado, contextualizado y monitorizado en tiempo real. **IBM lleva esta filosofía al siguiente nivel** al integrarla con **capacidades avanzadas de inteligencia artificial** en sus soluciones de gestión de accesos privilegiados.

La propuesta de **IBM Security** combina la madurez de sus tecnologías con un **enfoque modular y escalable**, diseñado para proteger entornos complejos, híbridos y multicloud. Su solución **IBM Security Verify Privilege Vault** es un claro ejemplo de esta evolución.

Va más allá del simple almacenamiento de credenciales, ofreciendo una plataforma integral que permite **gestionar, auditar y automatizar accesos privilegiados** con un alto nivel de contexto y adaptabilidad.

Características:

Detección inteligente de anomalías (UEBA)

Que permite **identificar accesos inusuales** antes de que se conviertan en amenazas reales. Esta **inteligencia contextual** se complementa con flujos de trabajo automatizados que activan respuestas inmediatas, como la revocación de permisos, la solicitud de autenticación reforzada o el aislamiento de sesiones.

Integración nativa con ecosistemas SIEM y SOAR

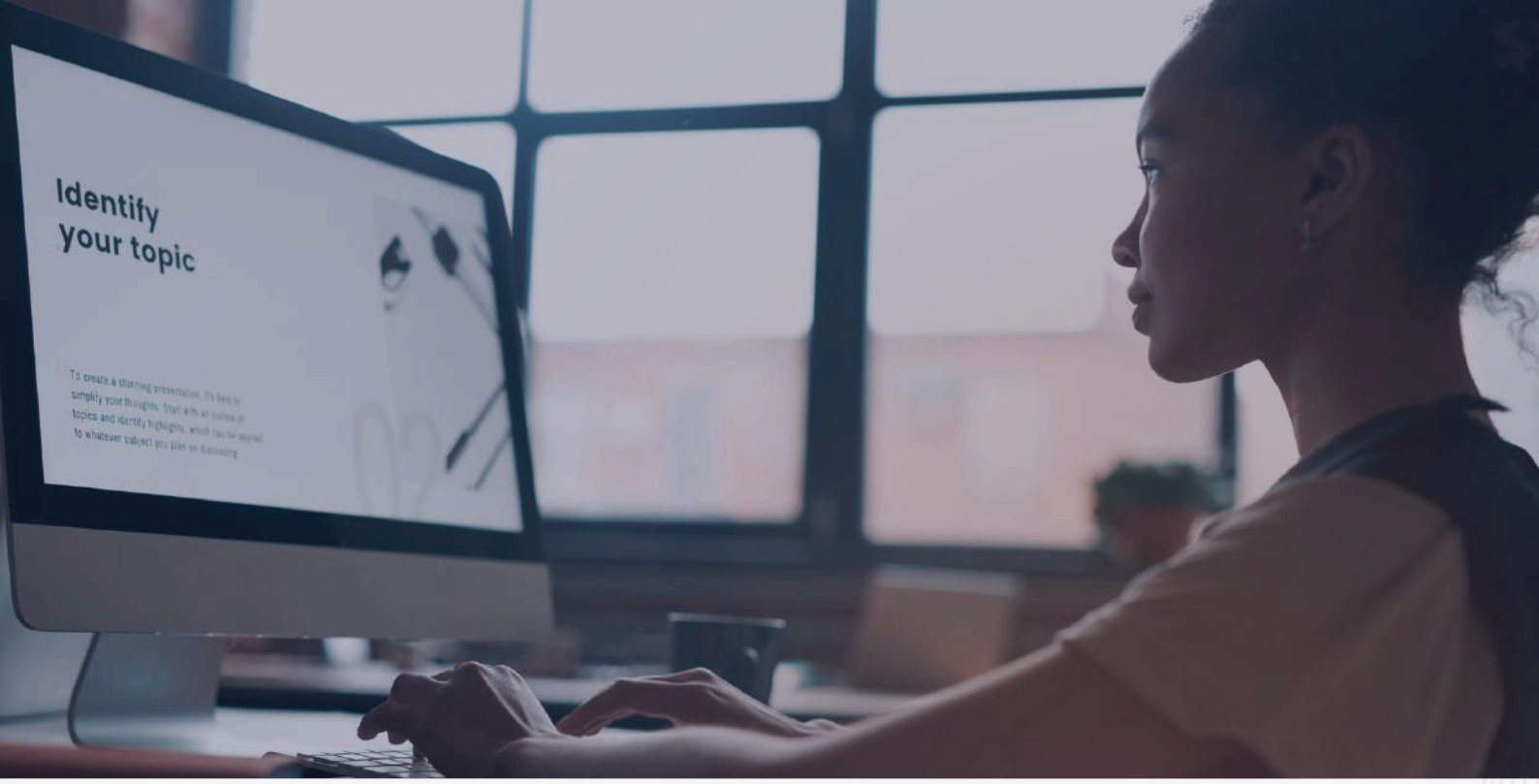
Facilita una **visión unificada de la seguridad y la orquestación** de respuestas automatizadas ante incidentes. Esta integración no solo mejora la eficacia operativa, sino que permite a los equipos de seguridad **actuar con mayor agilidad** y precisión, reduciendo el tiempo medio de detección y respuesta.

Cumplimiento normativo y trazabilidad

Genera **trazabilidad completa sobre los accesos**, el uso de privilegios y las acciones realizadas durante cada sesión. Esto es especialmente relevante para sectores regulados como el financiero, la salud o el e-commerce, donde la **protección de datos sensibles** y la demostración de cumplimiento son imperativos estratégicos.

Adaptabilidad a entornos complejos

La solución está concebida para operar eficazmente **en arquitecturas híbridas y multicloud**, con una arquitectura modular y escalable que permite una **integración fluida** en entornos tecnológicos diversos. Esto resulta fundamental para organizaciones con operaciones distribuidas, estructuras reguladas o sistemas legacy, ya que **garantiza la interoperabilidad** sin afectar la continuidad operativa ni exigir una transformación disruptiva.



Los **casos de uso** de **IBM Security Verify Privilege Vault** van desde la protección de entornos críticos, como bases de datos y sistemas core, hasta la **automatización del ciclo de vida de credenciales privilegiadas** en grandes organizaciones, pasando por la reducción de riesgos internos y la optimización de la experiencia de usuario sin comprometer la seguridad.

En definitiva, la visión de IBM apuesta por una **seguridad centrada en el dato y el usuario**, donde la confianza nunca se da por sentada y cada acceso es validado en función del contexto y el riesgo.

Esta **combinación de Zero Trust e inteligencia artificial** aplicada al control de privilegios supone una respuesta integral a los retos de ciberseguridad actuales. No se trata solo de reforzar perímetros, sino de controlar inteligentemente el acceso a **las joyas de la corona digital:** los recursos más sensibles y valiosos de las organizaciones.

07 Evolutio: habilitando la seguridad inteligente en entornos híbridos

Adoptar una estrategia avanzada de **gestión de accesos privilegiados** requiere más que una solución tecnológica: exige visión, conocimiento del negocio y capacidad de ejecución. En este contexto, **Evolutio** se posiciona como un **aliado estratégico** para aquellas organizaciones que buscan implementar modelos de ciberseguridad sostenibles, **inteligentes y alineados con sus objetivos de transformación digital**.

Con más de 30 años de experiencia en servicios tecnológicos críticos, Evolutio combina la especialización en **ciberseguridad**, **cloud y gestión de identidades** con un enfoque altamente consultivo.

Nuestro modelo de trabajo parte del **entendimiento profundo** de cada entorno y cada cliente, para diseñar e implantar soluciones que no solo funcionan, sino que **evolucionan con la organización**.

La seguridad de accesos privilegiados no es una capa aislada, sino **parte de una visión más amplia** de gobierno del dato y protección del ecosistema digital.

En este sentido, nuestra metodología **Route2Cloud** permite acompañar a las organizaciones en su **transición a arquitecturas híbridas y multicloud** de forma segura, ayudando a definir políticas de control de acceso, segmentación, visibilidad y cumplimiento desde el diseño mismo de la infraestructura.

Desde nuestros **SOCs (Security Operations Centers)**, damos soporte gestionado a organizaciones que requieren capacidades avanzadas de detección, respuesta y correlación de eventos de seguridad. Estos centros operan con **tecnologías de última generación**, integradas con soluciones de **inteligencia artificial y automatización**, para ofrecer una respuesta ágil y contextualizada ante incidentes que involucren accesos privilegiados.

Además, contamos con **oficinas técnicas especializadas y equipos de ingeniería de ciberseguridad** capaces de integrar productos como **IBM Security Verify Privilege Vault** dentro de arquitecturas complejas, garantizando su interoperabilidad con sistemas existentes y alineándolo con las políticas corporativas de seguridad.

Uno de los pilares diferenciales de **Evolutio** es nuestro **Hub de Innovación en Inteligencia Artificial**, desde el cual desarrollamos soluciones propias aplicadas a la mejora continua de la seguridad. Este centro impulsa proyectos que combinan **IA**, **automatización y análisis de comportamiento** para anticipar riesgos, optimizar la gestión de identidades y enriquecer la toma de decisiones en tiempo real.

Gracias a esta combinación de **expertise**, **tecnología y acompañamiento cercano**, ayudamos a nuestros clientes a no solo proteger sus activos más críticos, sino a hacerlo de forma escalable, eficiente y alineada con su crecimiento. Porque en un entorno cada vez más distribuido y cambiante, **la seguridad debe ser tan ágil como el propio negocio**.

08 Conclusiones

La **transformación digital** no solo ha revolucionado la manera en que operan las organizaciones: también **ha redefinido las reglas del juego en ciberseguridad**. En este nuevo entorno, proteger los accesos privilegiados no es una opción: es una prioridad estratégica para garantizar la continuidad, la resiliencia y la confianza en los negocios.

Las amenazas evolucionan **a un ritmo cada vez más acelerado**, y con ellas, las estrategias de protección deben avanzar. Apostar por modelos de gestión de accesos privilegiados inteligentes, basados en **inteligencia artificial**, **automatización** y un **enfoque Zero Trust**, es hoy una necesidad para aquellas organizaciones que quieren anticiparse a los riesgos y proteger sus activos más valiosos.

La combinación de tecnologías líderes, como **IBM Security Verify Privilege Vault**, y la capacidad de **Evolutio** para diseñar, desplegar y gestionar entornos de seguridad inteligentes, ofrece a las organizaciones una **propuesta de valor diferencial:** no solo protegerse mejor, sino hacerlo de forma escalable, eficiente y alineada con sus objetivos de transformación.

Reforzar la resiliencia digital requiere:

- Adoptar un **enfoque proactivo y automatizado** en la gestión de accesos privilegiados.
- Integrar la **inteligencia artificial y el análisis de comportamiento** en los procesos de detección y respuesta.
- Romper con los esquemas tradicionales y evolucionar hacia modelos **contextuales y dinámicos** de control de acceso.
- Apostar por **partners tecnológicos y estratégicos** capaces de acompañar en el diseño, la implantación y la evolución de las soluciones.

Porque hoy, **la IA en ciberseguridad** ya no es opcional, sino crítica.

En **Evolutio**, junto a **IBM**, ponemos nuestra experiencia, tecnología e innovación al servicio de la seguridad de las organizaciones. Acompañamos a nuestros clientes para **diseñar soluciones que protejan** no solo el presente, sino también el futuro de sus negocios.

¿El próximo paso? Transformar la protección de accesos privilegiados en un motor de resiliencia, agilidad y confianza.

Estamos listos para acompañar a su organización en ese camino.

evolutio.com | 91 270 6000 | info@evolutio.com