HONNE SENSE

LEADERSHIP AND INNOVATION THAT INSPIRES,
TECHNOLOGY THAT CONNECTS

VOL.7 SEPTEMBER - OCTOBER 2025

CONTENTS

EDITORIAL

A year ago, we published the first issue of Honne Sense. It was born as a way to share what we learn every day while working with technology, innovation, and digital transformation. Today, twelve months later, this publication has evolved into a space to connect with the community of leaders who are shaping the technological future of Mexico and Latin America.

This anniversary gives us the opportunity to look back—but, more importantly, to look ahead. In this issue, dedicated to 2025–2026 technology trends, we bring together the perspectives of several CIOs who are setting the course for their organizations and for the country. Interestingly, they all agree on one key point: technology is no longer a support area, but a strategic pillar of business.

From virtual machines to invisible infrastructure; from security as an added layer to intelligent monitoring within the cloud; and from chats as isolated tools to true orchestration centers—Santiago Vanegas, Iván Maldonado, and Andrik de la Cruz share different angles of this evolution. In the end, however, they all speak of the same thing: a new stage where technology simply works, integrates seamlessly, and enables companies to grow with speed and confidence.

At Honne Sense, we want to keep contributing to that conversation—not from theory, but from the practice and experience we live every day alongside our clients and partners. We thank everyone who has read, shared, and contributed ideas throughout this first year; this project exists because there is a community that believes knowledge multiplies its value when shared.

We move forward—learning, exploring, and building—because the best part of this journey is that it's only just beginning.

Carlos Lerma
CEO
Honne

CIO PERSPECTIVES MEXICO 2025–2026: BETWEEN INNOVATION AND DIGITAL RESILIENCE

EXECUTIVE SUMMARY

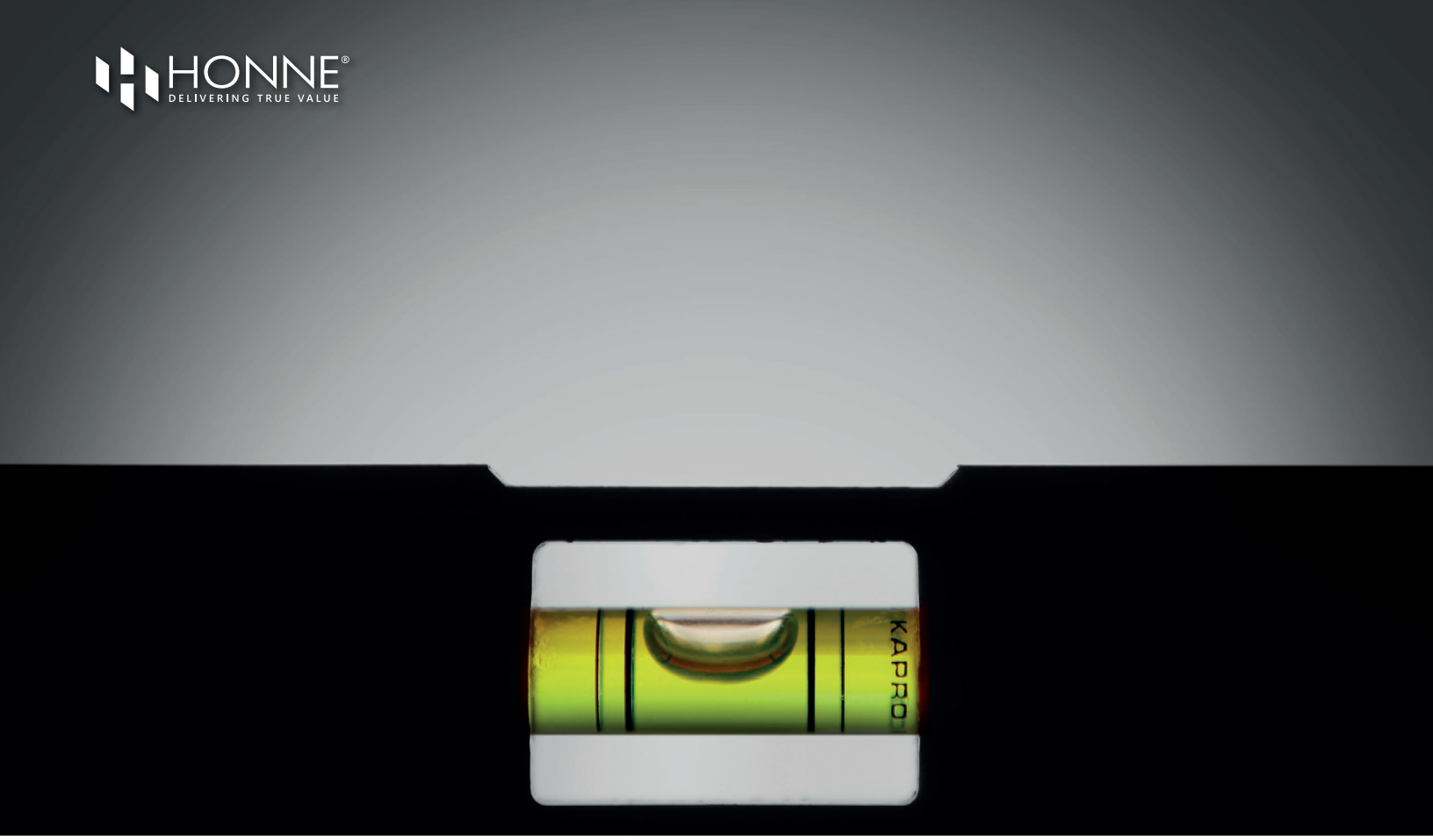
The research conducted with leading CIOs, CTOs, and innovation executives in Mexico offers a clear view of the priorities, challenges, and opportunities that will shape the technological landscape through 2026. The results reflect a balance between the urgency to ensure resilience, the need to enhance digital maturity, and the vision of innovation as a driver of growth.

CIOs agree that technology is no longer just a support function but a strategic pillar of business. Their perspectives reveal a future where financial discipline, digital culture, and the adoption of emerging technologies will converge to sustain the competitiveness of Mexican organizations.

Key topics addressed in the report:

1. Digital maturity: on the way, but with remaining gaps.
2. Cloud strategies: hybrid and diversified.
3. Business continuity: a plan not always tested.
4. Security: the most challenging front.
5. Investment priorities: from cost savings to value creation.
6. Emerging technologies: generative AI leading the way.
7. Budgets: moderate optimism.
8. The human side: between SUVs and superheroes.
9. Conclusion: innovating with resilience.

This analysis not only reveals where technology investment in Mexico is heading but also how CIOs are redefining the meaning of **resilience, innovation, and digital culture** within their organizations.



The voice of CIOs is increasingly becoming the compass that defines the direction of organizations. In a context where digital transformation never stops, listening to them allows us to anticipate trends, identify challenges, and envision Mexico's technological future.

With this goal in mind, Honne conducted research with leading CIOs, CTOs, and innovation executives in Mexico to understand their priorities, concerns, and strategic bets toward 2026. The findings reveal a landscape full of contrasts: organizations striving for digital maturity, cautiously growing budgets, increasingly complex security risks, and a strong interest in emerging technologies such as generative artificial intelligence.

What's clear is that the next two years will be decisive: Mexican companies must balance **innovation and resilience** if they want to remain competitive.

1. Digital Maturity: In Progress, But Still with Gaps

One of the most revealing findings of the research is the level of digital maturity within organizations. **62% of surveyed CIOs admitted to being at an intermediate stage**—with partially digitalized processes, limited tool integration, and a conscious effort to modernize.

Only 18% identified as being at an advanced stage, with full system integration, consolidated data analytics, and intensive use of artificial intelligence. In contrast, **20% remain in early stages,** where digitalization is concentrated in isolated areas and lacks a cross-functional strategy.

These numbers confirm that digital transformation is not a destination achieved, but an ongoing and evolving process. Mexican organizations are making solid progress but still face **critical gaps:** lack of end-to-end integration, difficulty scaling innovation pilots, cultural resistance to change, and limitations in managing digital talent.

In this context, Honne helps companies accelerate their digital maturity through four main pillars:

1. **Advisory**: defining a business-aligned technology roadmap, with maturity diagnostics and prioritization of high-impact initiatives.

2. **Build:** implementing modern cloud architectures, with data analytics, artificial intelligence, and automation as key enablers.

3. **Run:** providing managed services that ensure continuity, efficiency, and world-class operations—freeing IT teams from operational tasks.

4. **Transformation:** supporting the adoption of emerging technologies such as GenAI and Data Analytics, using proven methodologies to move from pilots to scalable solutions.

With this approach, Honne becomes a **strategic ally** that not only drives digitalization but transforms it into a systematic engine for innovation and sustainable growth.

2. Cloud Strategies: Hybrid and Diversified

The cloud has become the core of technological operations for organizations in Mexico. 71% of CIOs reported operating under a hybrid model, combining public cloud with on-premise systems. This trend reflects a clear reality: not all processes can migrate

immediately, but there is a growing preference for models that leverage the best of both worlds.

In the provider ecosystem, leaders agree that the market is dominated by the major **hyperscalers**, although there are also specific alternatives tailored for **regulated industries** or organizations with particular requirements.

A relevant finding is that **more than half of executives** indicated that **external managed services** are rapidly gaining ground—especially in infrastructure, operations, and security. For many, this practice has become a **natural path to free internal resources** and maintain focus on business strategy.

In this regard, **Honne offers managed cloud services** that ensure continuity, efficiency, and protection while simplifying technology management. Through this model, organizations not only reduce operational workloads but also **strengthen their ability to innovate and respond agilely to market challenges.**

3. Investment Priorities: From Cost Savings to Value Creation

When analyzing t**echnology investment goals for 2026**, CIOs' priorities are clear: **58% highlighted improving customer experience** as their main goal, closely followed by **product and service innovation (52%).** Although operational efficiency and cost reduction remain important, they are no longer the primary drivers of technology agendas.

This shift reflects a profound **change in mindset.** Technology is no longer seen merely as a means to optimize processes or control expenses—it has become an **enabler of new value propositions.** Investments are increasingly directed toward digital platforms that enable personalized experiences, the agile launch of services, and the exploration of more dynamic and profitable business models.

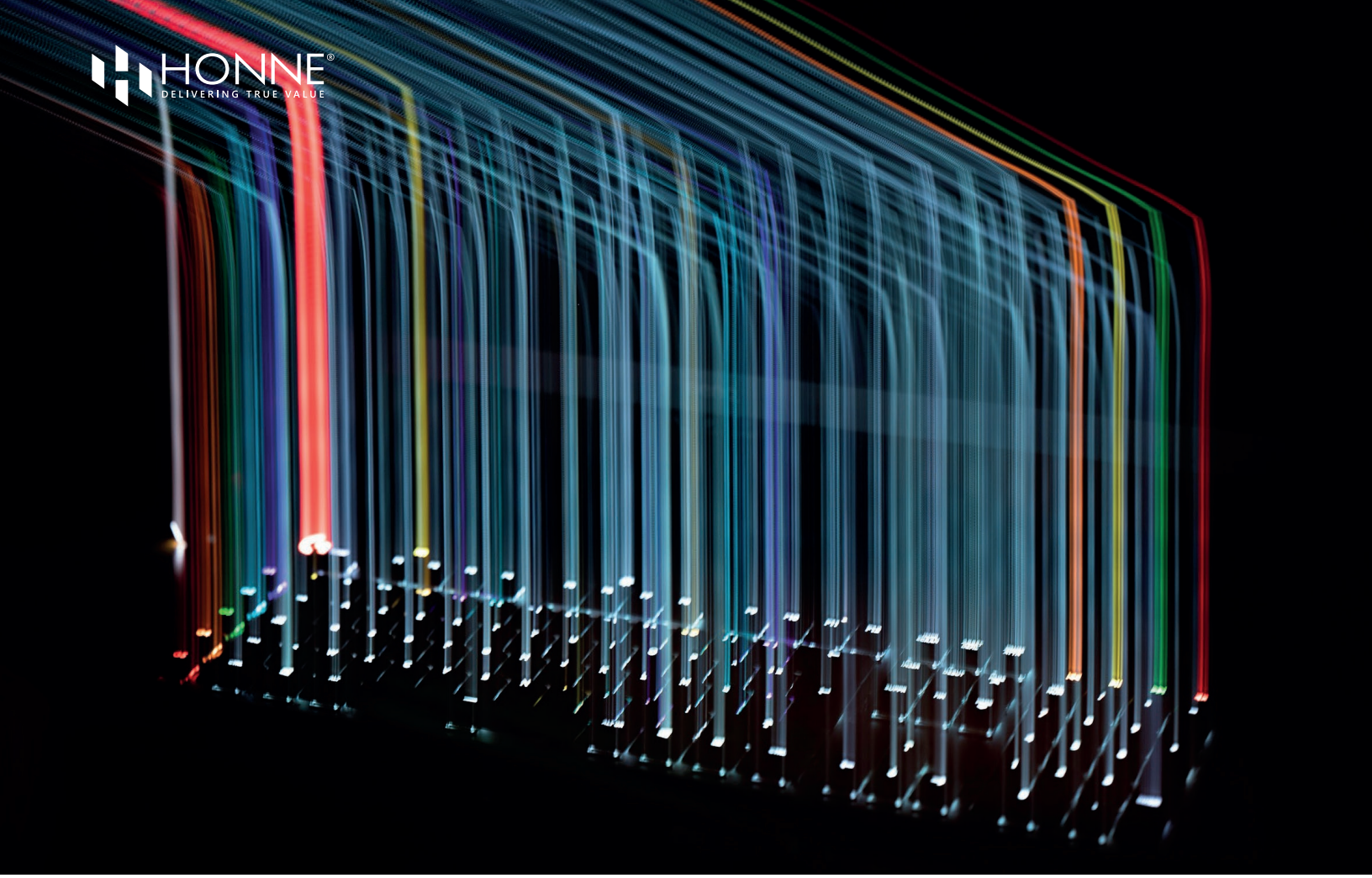
The conclusion is clear: **IT no longer plays a support role—it stands as a strategic pillar of business growth.** This change in perspective marks a turning point for Mexican organizations, which now view technology not just as a tool for efficiency but as a **lever for differentiation, competitiveness, and sustainable innovation.**

The real challenge for CIOs lies not only in **deciding how much to invest,** but in ensuring that **every peso translates into real business growth**. This is where Honne **becomes a key ally**—helping organizations ensure that technology goes beyond cost savings to become a **constant source of value, innovation, and competitive differentiation.**

4. Business Continuity: A Plan Not Always Tested

Resilience has become a key word on the CIO agenda. 72% of leaders stated that they have a formal **Business Continuity or Disaster Recovery Plan (DRP); however, only 34%** test it regularly. An additional **28%** acknowledged that their plan is still in the design or implementation phase, leaving a **significant gap in real preparedness** for potential incidents.

The risk is clear. In an environment where **cyberattacks, infrastructure failures, and service outages** are inevitable, a DRP that only exists on paper is simply not enough. Leaders agree that the real challenge heading into 2026 will be **moving from planning to prac-**



tice—ensuring not only that the documents exist, but that organizations have the **proven capability to recover quickly** and minimize the impact of any incident.

A **continuity plan without testing is like an insurance policy without real coverage**—it creates a false sense of security. For this reason, more and more CIOs recognize the need for **regular simulation exercises, risk audits, and dynamic updates** to keep the DRP alive and relevant amid the rapid pace of technological change and evolving threats.

Honne helps organizations strengthen their resilience through **managed services and continuity strategies** that go beyond documentation: we design, test, and operate recovery plans so that, in the face of any contingency, companies can respond swiftly and maintain the trust of their customers and partners.

5. Security: The Most Challenging Front

When discussing the main security risks, CIOs identified three primary concerns:

1. **Internal data leaks**
2. **External cyberattacks**
3. **Lack of security training**

The combination of **external threats and internal vulnerabilities** illustrates the complexity of today's digital landscape. Security can no longer rely solely on firewalls or specialized software; it requires a **comprehensive strategy** that integrates people, processes, and technology—where **prevention and preparedness** are just as critical as incident response.

CIOs agree that the real challenge is not only to invest in tools but to build a culture of **digital awareness.** Training employees, establishing clear protocols, and maintaining constant oversight are essential steps to reduce exposure. **Security should not be seen as a one-time solution but as a continuous cycle of anticipation, monitoring, and resilience**.

As one CIO put it:

"The best investment in security isn't always the most expensive—it's the one that makes the entire organization think and act with digital responsibility."

In this context, having a **specialized partner like Honne** is key to strengthening cybersecurity posture. The combination of **proactive monitoring, ongoing testing, and awareness programs** is crucial for ensuring that security stops being a barrier and becomes an **enabler of trust, continuity, and sustainable growth.**

6. Emerging Technologies: Generative AI Leads the Way

The enthusiasm for innovation is unmistakable. **68% of CIOs** plan to explore Generative **Artificial Intelligence (GenAI)** over the next two years, while **42%** mentioned **Advanced Internet of Things (IoT)** as one of their top priorities.

GenAI leads the list not only as a trend but as a **strategic lever** to reimagine processes, products, and experiences. Technology leaders emphasize its potential to **accelerate content creation, enable virtual assistants, automate workflows, and personalize interactions** with customers and employees. For many, **generative AI represents the defining bet of this decade.**

Meanwhile, **IoT** is emerging as a critical component in industries where **connectivity and real-time analytics** create competitive advantages. In manufacturing, retail, and logistics, the ability to monitor operations minute by minute promises to transform efficiency and decision-making.

Both trends confirm that organizations are not merely seeking tools, but **intelligent ecosystems** that integrate analytics, automation, and connectivity to deliver sustainable value.

In this evolution, **Honne partners with CIOs** to turn exploration into measurable results. We design pilots that validate the value of GenAI and IoT in real-world environments, integrate these technologies with existing infrastructure, and ensure they **scale securely and reliably.** In doing so, **innovation stops being a promise and becomes a tangible engine of efficiency, differentiation, and growth.**

7. Budgets: Cautious Optimism

Looking toward 2026, most CIOs expect their IT **budgets to grow moderately**, while a smaller group anticipates significant increases.

This reflects a **measured optimism:** organizations understand that investment is essential to remain competitive, but they will do so with financial discipline and by **prioritizing high-impact initiatives.**

8. The Human Side: Between SUVs and Superheroes

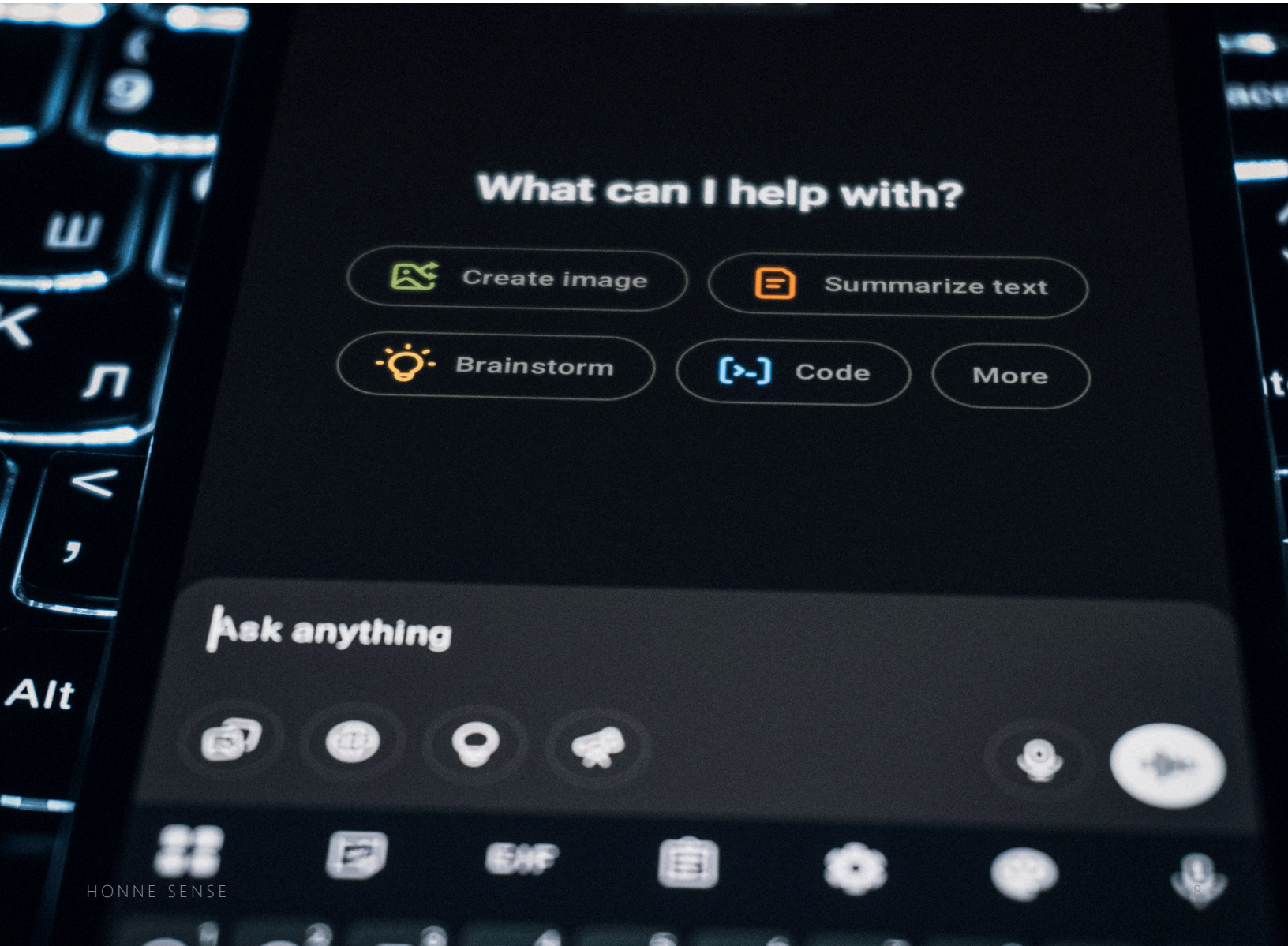
Beyond the data, the survey invited CIOs to describe their IT departments through **creative metaphors:**

- Like a **reliable SUV**, robust and ready for any road.
- Like an **executive sedan**, efficient and professional.
- Like **Iron Man**, innovative, full of gadgets, and always ready to impress.
- Like **Scooby-Doo**, solving mysteries through teamwork.

These insights show that behind every technology strategy there are **teams with identity, culture, and pride**—and they remind us that **digital transformation is not only technical but deeply human.**

9. Conclusion: Innovating with Resilience

The results of the **CIO Mexico 2026 research** deliver a clear message. 64% of leaders place **innovation** as their top priority, **53%** highlight **resilience** as the most urgent challenge, and **47%** acknowledge that **advancing digital maturity** is the inevitable path forward.



This balance—**innovating, enduring, and evolving digitally**—will define the success of Mexican organizations in the coming years. The CIOs' agenda makes it clear **that investing in technology is not enough**; it must be done with **vision, financial discipline,** and the proven ability to **test resilience in real-world conditions.**

At **Honne**, we believe the key lies in combining **strategic vision with disciplined execution**: choosing the right technologies wisely, validating continuity plans through testing, building skilled teams, and fostering a **digital culture that transcends generations.**

Because **the future isn't something to wait for—it's something to design, build, and execute with clarity.** And as Mexico's CIOs chart the course ahead, **Honne will be there every step of the way**, helping transform their strategies into **tangible and sustainable results.**

FROM VIRTUAL MACHINES TO INVISIBLE INFRASTRUCTURE: A PERSONAL JOURNEY

By Santiago Vanegas, Azure Architecture Lead and Cloud Architect at Honne.

When I started working in systems back in 2010, the big topic was virtual machines. I remember the fascination of seeing how we could consolidate on a single physical server multiple environments that used to take up entire racks. For those of us who had spent years dealing with hardware, it was almost magical: fewer machines, more efficiency, more control. But it also came with its own challenges—expensive licenses, wasted resources, and endless maintenance nights. It was a time when success was measured by the ability to keep the datacenter running and ensure service continuity, even at the cost of countless hours of support.

Over the years, I discovered containers. At first, I confess they seemed like a lab toy—something that might work well for startups but was hard to imagine in the "serious" corporate world. Until I started using them and realized how lightweight and practical they were. What used to take hours to deploy could now be up and running in seconds. Gartner isn't exaggerating when it says that over 90% of large enterprises will use container management tools in hybrid environments by 2027—I've experienced it firsthand, and the difference is dramatic. The mindset shifted too: we went from planning how many VMs a project needed to simply defining images, pods, and deployments that could scale up or down within minutes. The change in thinking was as profound as the technological one.

Later, I came across serverless. And this time, the feeling was different—not just greater efficiency, but the ability to forget about the infrastructure itself. I remember a pilot project where we tested Azure Functions. Going from planning servers and capacity to simply deploying functions and paying only for what actually runs felt like lifting a huge weight off my shoulders. Companies like Coca-Cola prove it with numbers (they reduced nearly 65% of their costs by migrating part of their backend to Functions), but for me, the real impact was the speed: moving from "Where are we going to run this?" to "It's already running" in just minutes. Beyond the numbers, it was a reminder that infrastructure shouldn't be a bottleneck—it should be a direct enabler of business outcomes.

Today, in 2025, I'm witnessing how intelligent automation is transforming not only the where, but the how of IT operations. AIOps, algorithms that detect anomalies before they become issues, self-configuring infrastructures, and observability tools enhanced with AI that predict failures before they happen. We're no longer looking for needles in a haystack—we have a magnet that places them in our hands. I've seen projects where early detection cut incident resolution times by two-thirds, and believe me, that's life-changing: fewer outages, fewer 3 a.m. emails, and more time to focus on innovation.

Looking back, what began with the excitement of virtual machines has led us toward increasingly invisible and autonomous infrastructure. One where technical leaders no longer measure success by the number of servers they manage, but by how quickly they can deliver value to the business. And that's the real challenge: adaptation. Because what's coming isn't just more technology—it's a pace of change that waits for no one. Adoption speed has accelerated so much that what used to take decades to evolve now happens in just a few years.

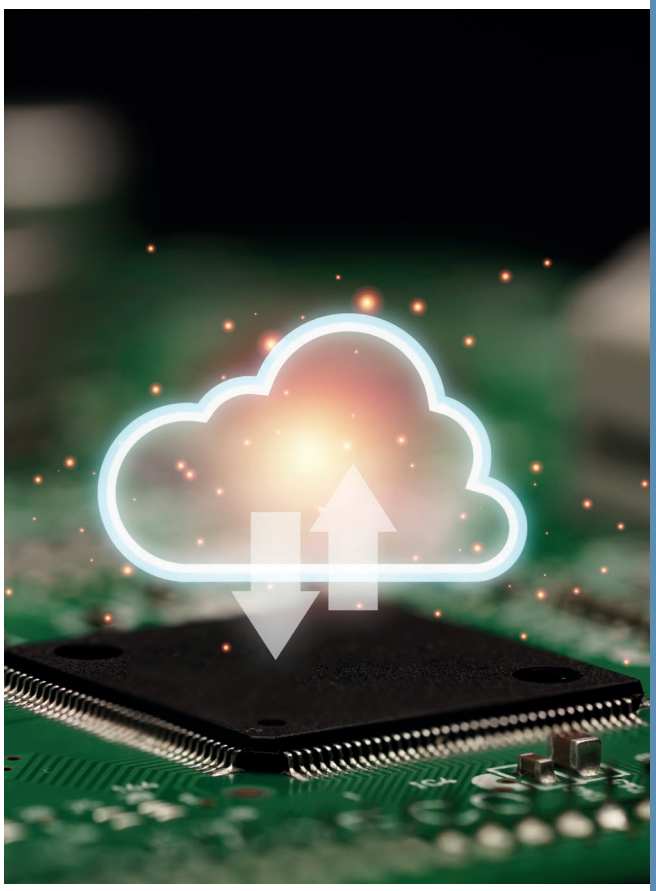
The transition from virtual machines to containers, then to serverless and intelligent automation, reflects not only a technological shift but a deep cultural one. In the past, the challenge was to manage hardware; later it was mastering hypervisors, then learning orchestration with Kubernetes; and now, the goal is to increasingly abstract ourselves from the infrastructure to focus on enabling business outcomes. It's not just about learning new tools—it's about understanding how each advance redefines the role of IT professionals. We've moved from "hardware administrators" to "platform architects," and increasingly, to "value strategists."

This journey also brings new risks and responsibilities. Serverless and container-based environments offer agility but demand greater maturity in security, monitoring, and governance. Companies that fail to adapt their compliance, observability, and cost management processes to this new reality risk losing control. I've seen cases where the promised savings from migrating to serverless functions turned into unexpected cost overruns due to poor consumption management. Likewise, dependency on specific cloud providers in serverless architectures raises portability and resilience challenges that can't be ignored. Every technology brings benefits—but also new challenges we must learn to manage so innovation doesn't become a headache.

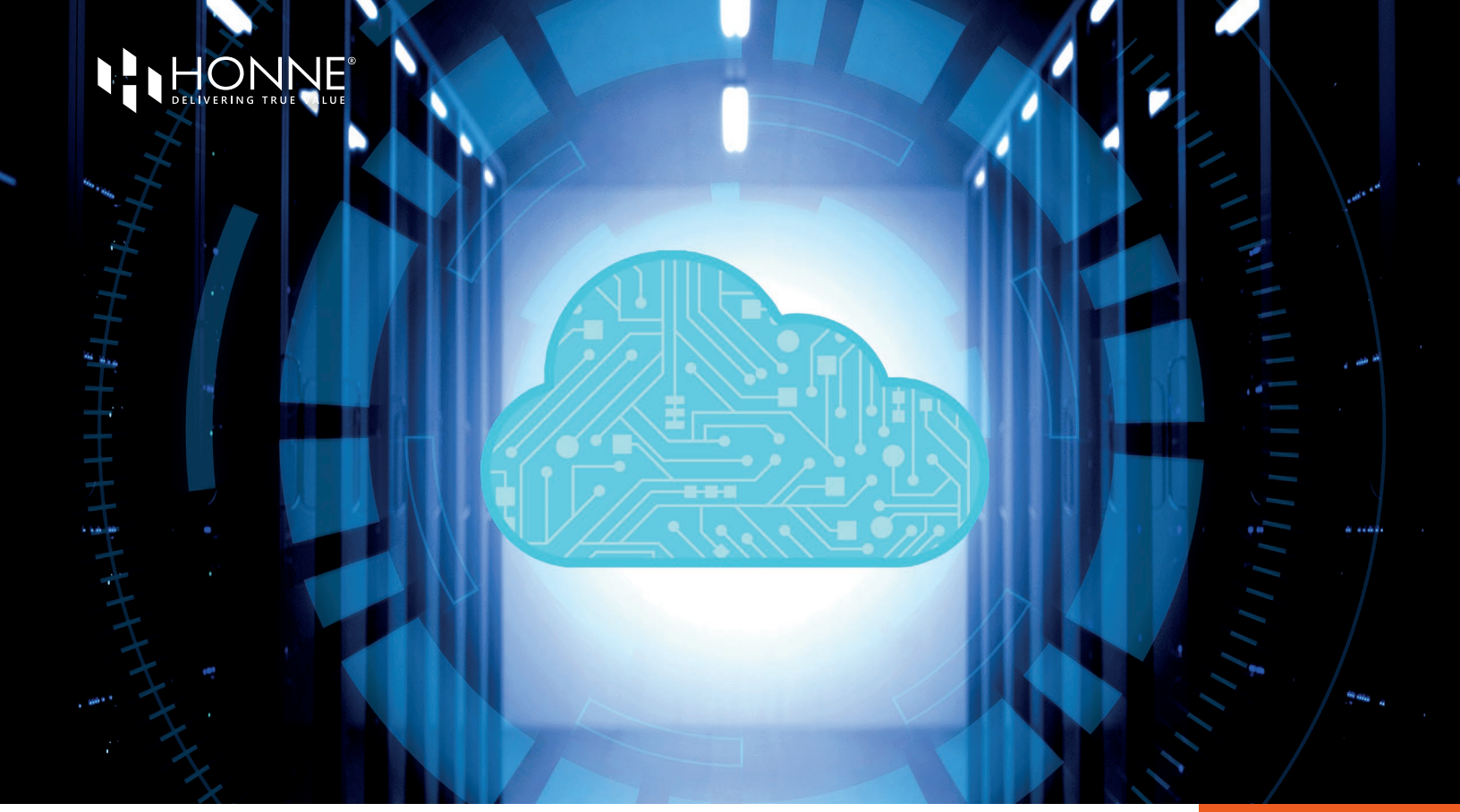
And as all this unfolds, artificial intelligence and machine learning are becoming the great catalysts of the future. Today we already see platforms capable of self-diagnosis, auto-scaling, and self-healing without human intervention. Infrastructure, once visible and tangible in server rooms, is now evolving into a digital fabric that operates almost invisibly—but directly impacts business competitiveness. The promise of autonomous infrastructure is no longer science fiction; it's a real, accelerating trend that challenges us to think bigger and stay ahead.

In conclusion, virtual machines won't disappear overnight—they'll remain relevant for legacy, highly regulated, or specialized workloads. However, their prominence is quickly fading in favor of models that prioritize speed, efficiency, and automation. For those of us working in this ecosystem, the challenge is twofold: to preserve the experience gained from VMs while preparing to lead in a future where infrastructure becomes increasingly invisible and autonomous.

Because ultimately, the real transformation isn't just technological—it's about our ability to adapt and deliver value in a world where change is measured not in decades, but in ever-shorter cycles. The question we should be asking isn't whether virtual machines will come to an end, but whether we, as professionals, have the resilience to evolve at the same pace as technology.



Santiago Vanegas is a technology enthusiast with 14 years of experience in the industry. As an Azure Architecture Lead and Cloud Architect for the past seven years, he has played a key role in digital transformation projects and the adoption of emerging technologies. His greatest satisfaction comes from helping organizations transition to the cloud seamlessly and objectively, fostering innovative processes that drive growth and modernization.



COMPREHENSIVE MONITORING FOR SUSTAINABLE CYBERSECURITY IN THE AWS CLOUD

By Ivan Guadalupe Maldonado Zuñiga, Amazon Web Services (AWS) Services Specialist at Honne.

Early Detection and Emerging Threats

Effective cybersecurity goes beyond traditional antivirus solutions. Organizations now face increasingly complex threats such as ransomware and phishing. Enhanced monitoring enables the early detection of these attacks through the implementation of AWS solutions that go beyond basic protection.

Amazon GuardDuty

This AWS service leverages threat intelligence, machine learning, and anomaly detection to continuously monitor AWS accounts and network activity for malicious behavior. It identifies unusual patterns, such as API access from unusual geographic locations or API calls that may indicate credential compromise.

Amazon Macie

Amazon Macie uses machine learning to discover, classify, and protect sensitive data stored in Amazon S3 buckets, such as personally identifiable information (PII) or financial data. It monitors access and data movement, alerting administrators to any anomalous behavior.

User and Entity Behavior Analytics (UEBA)

By integrating Amazon Detective, organizations can analyze and visualize security events from GuardDuty, Macie, and AWS Security Hub. This helps identify the root cause of threats—such as zero-day attacks or lateral **movement—by correlating network activity, GuardDuty findings, and AWS CloudTrail logs.**

Implementation Examples: Early Detection

TOOL	CASE	SOLUTION
Amazon GuardDut	An attacker compromises an EC2 instance to mine cryptocurrency, causing a CPU spike and unexpected costs.	GuardDuty detects the finding "Bitcoin-Tool:EC2/Bitcoin Mining." An automated AWS Lambda function isolates the instance for further investigation, mitigating both financial and security impact.
Amazon Macie	A developer configures an S3 bucket with public access, accidentally exposing customers' personally identifiable information (PII).	Macie, when scanning the bucket, identifies the PII and alerts the security team about the public access policy. The team immediately corrects the policy, preventing a potential data breach.
Amazon Detective	A security analyst observes multiple low-severity alerts from GuardDuty. A coordinated attack is suspected, but the root cause remains unclear.	Detective correlates the findings with network traffic and CloudTrail logs, creating a behavior graph that reveals a chained attack: credential compromise, resource enumeration, and lateral movement—enabling a targeted response.

Privacy Management and Data Protection

Protecting data is critical, especially as "double extortion" attacks increase—where attackers not only encrypt data but also steal it and threaten to publish it. Integrated monitoring helps safeguard sensitive information, and it is important to implement controls to prevent data loss (DLP).

AWS Key Management Service (KMS)
Provides the ability to create and manage encryption keys used to secure your data in AWS services such as Amazon S3, Amazon EBS, and Amazon RDS. Monitoring key usage via AWS CloudTrail is crucial to audit and detect unauthorized access to keys.

Monitoring Anomalous Transfers
Amazon CloudWatch and AWS CloudTrail are essential tools. CloudTrail logs all API activity in your AWS account, allowing you to review the usage of services like S3. By configuring CloudWatch alarms, you can detect unusually large data transfers, which may indicate information leakage.

AWS WAF (Web Application Firewall)
Acts as a frontline barrier against common attacks, such as SQL injection, cross-site scripting (XSS), and phishing attempts, protecting your web applications and APIs. It serves as a proactive preventive layer that strengthens your overall security posture.

HONNE®
DELIVERING TRUE VALUE

Implementation Examples: Privacy Management

TOOL	CASE	SOLUTION
AWS KMS y CloudTrail	A former employee attempts to use credentials from a compromised account to access and decrypt a production database.	A CloudWatch alarm is configured to monitor the DecryptAPI event in CloudTrail. The alarm triggers on the attempt, allowing credentials to be revoked and preventing data leakage.
Monitoring Transfers	A compromised cred ential begins downloading gigabytes of data from an S3 bucket.	A CloudWatch alarm set to detect massive data transfers (e.g., >10 GB) is triggered. The security team stops the activity, limiting the impact of the exfiltration.
AWS WAF	An e-commerce website is targeted by multiple SQL injection attacks.	AWS WAF is deployed to protect the website, using rules that automatically identify and block SQL injection patterns, safeguarding the customer database from compromise.

Continuous Visibility and Corrective Actions

Protecting data is critical, but simply introducing security controls is not enough if their effectiveness is not verified. Continuous vulnerability analysis is essential to achieve full visibility and prioritize corrective actions according to business impact.

AWS Security Hub
This service provides a centralized view of your security alerts and status. It consolidates security findings from multiple AWS services (such as GuardDuty, Inspector, and Macie), as well as AWS partner solutions, making it easier to identify trends and automate response actions.

Amazon Inspector
This service continuously scans your workloads to identify software vulnerabilities and deviations from security best practices.

Simulations and Penetration Testing
To evaluate organizational resilience, attack simulations and penetration tests should be part of a continuous program that mimics realistic scenarios, such as credential compromise and data exfiltration. AWS enables this disciplined management approach to combine detection, measurement, and ongoing improvements to protect the organization's critical assets.

AWS Incident Response
This is a set of tools and guides that allows you to plan and respond effectively to security events. Proactive monitoring enables early detection of incidents, allowing for faster reactions to minimize impact.

Implementation Examples: Visibility and Remediation

TOOL	CASE	SOLUTION
AWS Security Hub	A security team reviews multiple consoles (GuardDuty, Inspector, Macie) to get a complete picture of their security posture, losing time and visibility in the process.	The team centralizes findings in Security Hub. From a single dashboard, they can view all prioritized findings, apply compliance filters, and automate incident responses.
Amazon Inspector	A DevOps team launches an EC2 instance without a security assessment, leaving the operating system unpatched with critical vulnerabilities.	Inspector scans the new instance and detects vulnerabilities. The finding is sent to Security Hub, where a ticket is automatically created in Jira for the DevOps team to apply the necessary patches.
AWS Incident Response	A GuardDuty alert indicates compromised IAM credentials, requiring immediate response to prevent further damage.	The team follows a predefined response plan. They use AWS Systems Manager Automation to revoke credentials and isolate the affected instance within seconds, minimizing the impact.

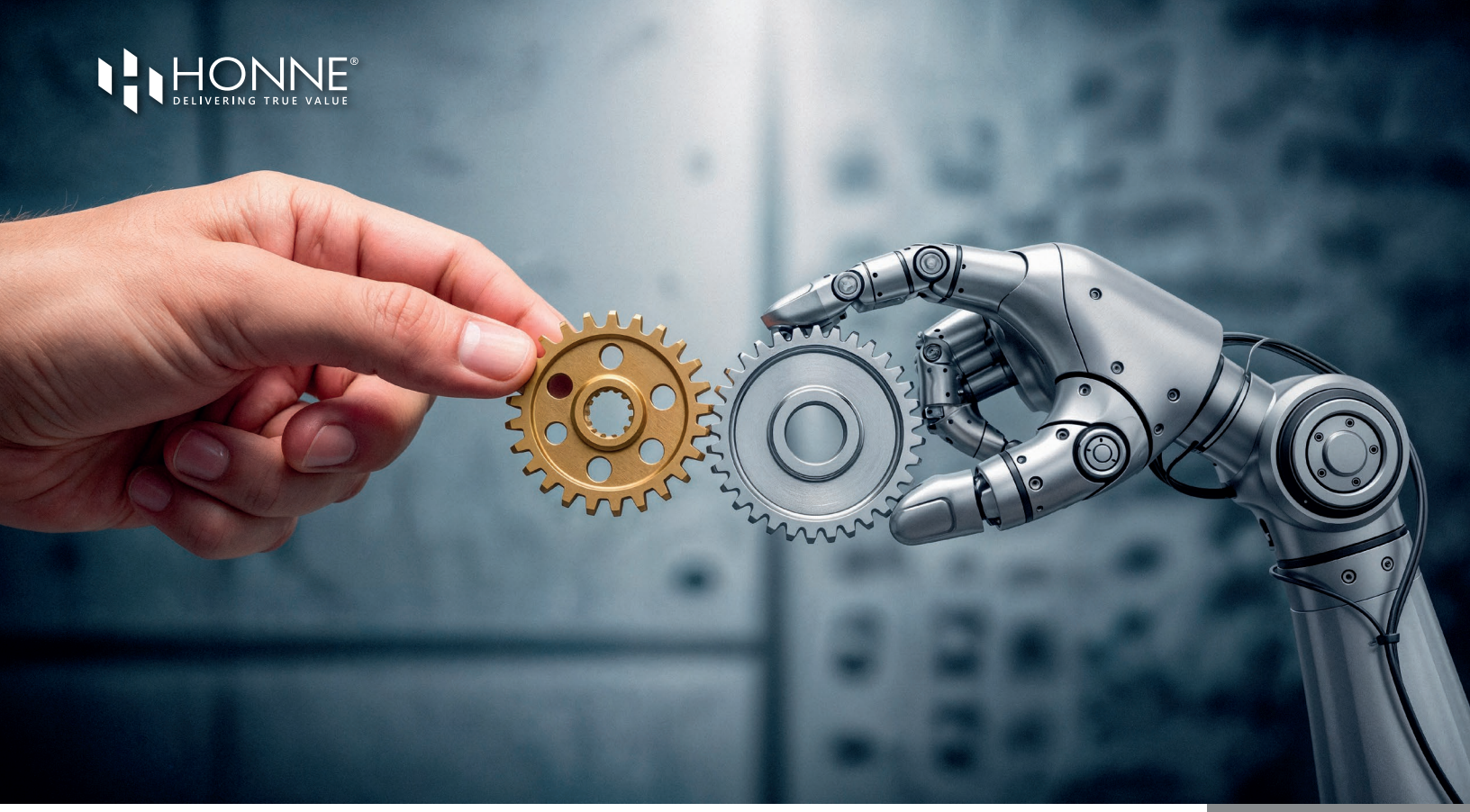
Monitoring as a Pillar of Resilience

In the era of digital transformation, cybersecurity is no longer a cost center but a strategic investment that enables innovation.

Comprehensive monitoring, powered by AWS's robust ecosystem of services, transforms security from a reactive approach to a proactive and preventive one.
This continuous oversight, combined with automation, fosters a security culture that not only protects assets and data but also builds a foundation of resilience, allowing businesses to operate confidently in a constantly evolving threat landscape.

True security is not about being perfectly safe—it is about being continuously resilient.

Ivan Guadalupe Maldonado Zúñiga is a specialist in Amazon Web Services (AWS).
With a strong background in data analysis, Ivan not only manages key AWS services (such as EC2, S3, RDS, and more) but also applies his expertise to keep applications secure and fully operational. His experience focuses on the implementation and support of cloud-based solutions, with a particular emphasis on resource optimization and the continuous improvement of infrastructures.



ORCHESTRATION OF MULTIPLE TOOLS USING MCP: BEYOND A SIMPLE CHAT

By Andrik Martínez, Full Stack Developer in the Digital Innovation Area at Honne.

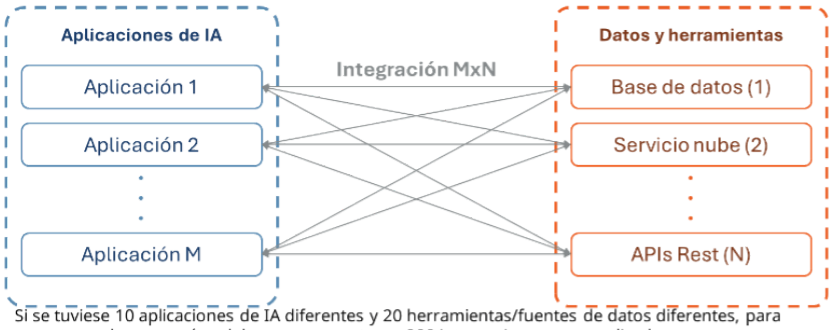
In the May–June 2025 edition of Honne Sense, we discussed the selection and implementation of use cases leveraging Artificial Intelligence (AI). In this section, we focus on addressing one of the challenges that arise after implementing AI solutions, specifically those that use one or more agents.

The Challenge

Unlike a chatbot, an agent has a higher level of autonomy, capable of performing complex actions and tasks independently on behalf of a user or another system. Agents can use external tools, access systems, execute scripts, search for information, and carry out many other activities.

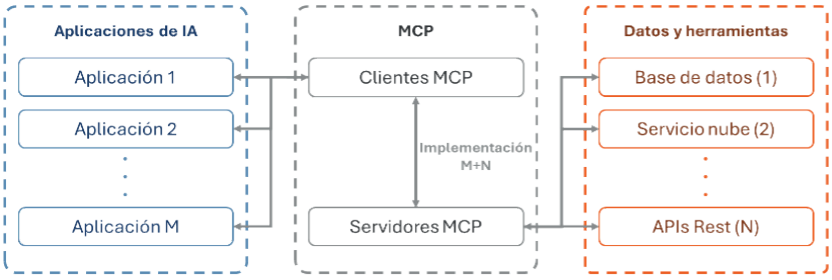
When an organization deploys multiple applications that use AI agents, each requiring connections to various data sources, tools, and/or services, the necessary integration between these components can lead to the M×N integration problem. This problem occurs when multiple AI applications (M applications) need to integrate with multiple tools, systems, and/or data sources (N tools, systems, and/or data sources). Creating a high number of specific integrations.

As more applications, data sources, systems, and tools are added, the number of integrations to maintain becomes unmanageable.



Si se tuviese 10 aplicaciones de IA diferentes y 20 herramientas/fuentes de datos diferentes, para conectar todas entre sí se debe crear y mantener 200 integraciones personalizadas.

An architecture that properly employs MCP reduces integration complexity, transforming the M×N problem into a simpler M+N equation. With MCP, M clients and N servers are built, requiring only M+N implementations.
Furthermore, for projects that require a solution leveraging the benefits of AI agents, capable of connecting to multiple data sources, and whose components can evolve independently and be reusable, a good approach would be to opt foran architecture that employs the Model Context Protocol (MCP). In the remainder of this



Si se tuviese 10 aplicaciones de IA diferentes y 20 herramientas/fuentes de datos diferentes, para conectar todas entre sí se debe crear y mantener 30 implementaciones personalizadas.

section, we will focus on the use of MCP.

Model Context Protocol (MCP)

As its name suggests, MCP is a recently released (late 2024) open-source standard that creates a universal language for AI systems to communicate with data sources, tools, and other systems.
MCP is not an agent framework; it is a standardized integration layer that allows agents to access tools. Additionally, MCP does not decide when a tool is called or for what purpose.

MCP enables Large Language Models (LLMs) to communicate efficiently with external services by establishing a standard. It also allows the use of "plug-and-play" tools instead of writing custom integration code for each tool, complementing agent orchestration frameworks.

Architecture with MCP

An architecture implementing MCP behaves similarly to a client-server architecture. MCP architectures have three main components:

1. MCP Host: An AI application that coordinates and manages one or more MCP Clients. Examples of MCP Hosts include IDEs and development tools such as Visual Studio Code, AI assistants like Claude Desktop, or any

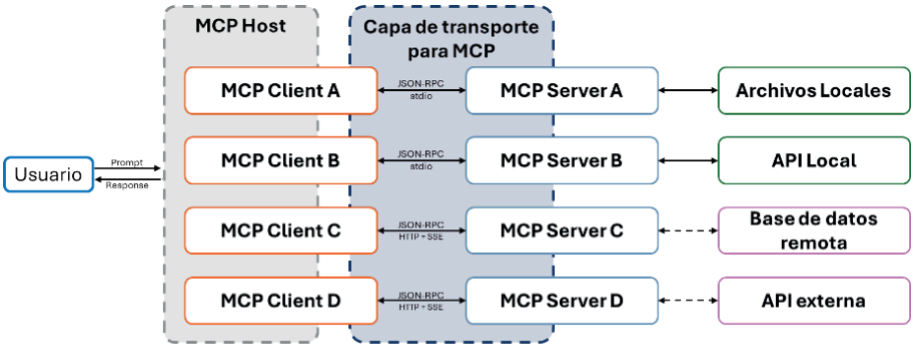
server hosting the AI agent and MCP Client.

2. MCP Client: The program, software, or code snippet that implements the MCP protocol and connects to MCP Servers. It retrieves context from the MCP Server for the MCP Host to use; it runs within the MCP Host. There can be multiple MCP Clients in an MCP Host, but each MCP Client has a 1:1 relationship with an MCP Server. Examples of MCP Clients include connectors in Claude.ai and Microsoft Copilot Studio ((not fully... an LLM or AI agent is not considered an MCP Client).

3. MCP Server: This is the program that provides context to the MCP Client. It enables connections to tools, resources, and data outside the AI ecosystem; the idea is that each MCP Server focuses on a specific integration (tool, database, API). Examples of MCP Servers include integrations with tools such as Slack, GitHub, Git, Docker, databases, and public clouds.

We can understand this architecture using a restaurant analogy: the restaurant represents the MCP Host, the waiters and coordinator represent the MCP Clients, and the meat and vegetable suppliers represent the MCP Servers. Here, an LLM and AI personnel could be the chef, who understands and prepares dishes using the ingredients provided to fulfill customer orders.

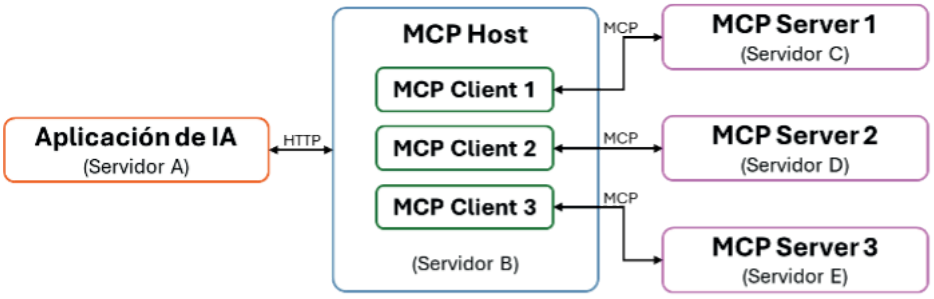
A real-world example of an architecture using MCP would be a web application (acting as the MCP Host) whose interface includes a chat where users can make requests to an agent (if there are multiple agents, the request



is directed to the orchestrating agent). The agent uses an LLM to understand natural human language; once the requirement is understood, the agent (via the MCP Client) sends requests to the necessary MCP Servers to complete the assigned task.

Each MCP Server queries native APIs to execute the received requests and then returns a response.
When the system, tool, or data source to be accessed is external to the organization, the owner must create and expose their MCP Server. Currently, several companies have already implemented MCP Servers in their tools (such as Jira, Confluent, Visual Studio Code, and Slack), so connecting to these tools does not require developing an MCP Server—only configuring the connection.

MCP vs REST API
Despite the similarities, there are significant differences between an API and MCP:
The use of MCP is recommended over APIs when a solution involves AI agents with multiple tool integrations, prioritizing interoperability among AI providers.



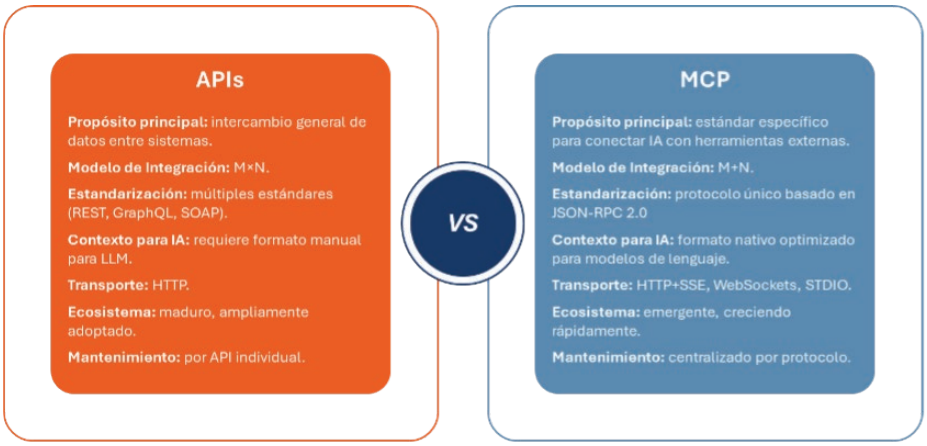
Use Case

The use of architectures employing MCP is not limited to the following use case.

Project Management

We can develop a task management system using an MCP-based architecture and leveraging AI. For this example, assume a company has a TI development team using several tools to receive incident reports and manage new implementations: Slack, GitHub, Jira, and Drive.

The general proposed architecture is as follows:
With this architecture, multiple workflows can be executed, such as the following:



Workflow 1: Sprint Status Report

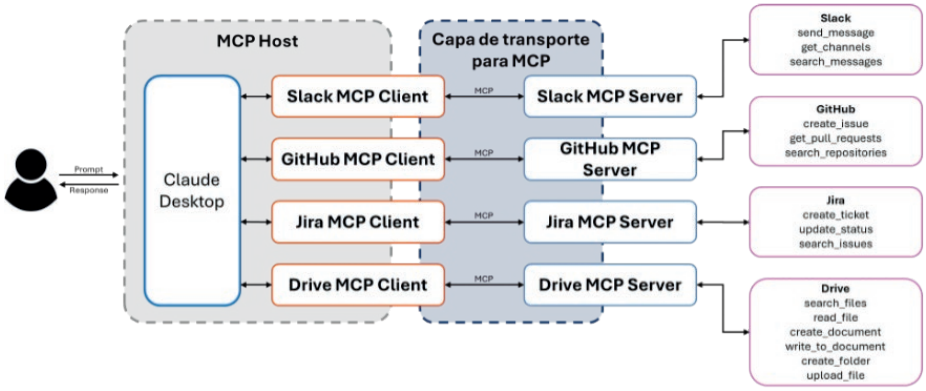
1. Jira Server: Retrieve tickets for the current sprint.
2. GitHub Server: Fetch related pull requests.
3. Slack Server: Review messages.
4. Drive Server: Save the generated report.

Workflow 2: Incident Management

1. Jira Server: Create a ticket.
2. GitHub Server: Create a branch for the hotfix.
3. Slack Server: Notify the DevOps team.
4. Drive Server: Document the incident.

Workflow 3: Automated Code Review

1. GitHub Server: Retrieve pull request details.
2. Jira Server: Find the related ticket.
3. Slack Server: Request a review from the development team.



4. Drive Server: Generate a review checklist.

It is important to mention that the agent determines which tool to use and the order of actions based on the decisions of the LLM, which reviews the context and available tools. However, specific workflows can be defined, or prompts can guide the sequence of actions, while the LLM maintains flexibility to adapt the flow according to the needs of each situation.

Considerations

Before implementing an MCP-based architecture, it is necessary to evaluate whether your AI solution presents the N×M problem. On the other hand, even if an architecture has integrations with N×M complexity, in most cases it will still be cost-effective (ROI calculations are required for this). MCP implementation becomes cost-effective when multiple AI applications need to interact with multiple systems.

Another important aspect is that MCP is a very recent standard, so there is limited trained personnel for implementing and supporting an MCP infrastructure. Therefore, for successful adoption, your organization will likely need to invest in developing technical capabilities to manage and implement MCP solutions.

Although organizations that adopt MCP early may gain a competitive advantage, it is necessary to balance innovation with the stability of a protocol still in evolution. It is also important to consider the added latency—the cumulative sum of delays generated at each step of the MCP communication chain. Additionally, MCP is stateful at the protocol level, although MCP Servers have the flexibility to be stateless or stateful depending on their specific needs.

Benefits

Among the benefits of adopting an MCP-based architecture are reduced complexity when integrating new applications or systems, making MCP a good alternative to solve the M×N problem.

Applications built with MCP can be more context-aware, understanding the user's current situation and accessing the information needed to provide relevant assistance.

MCP can also provide flexibility to switch between different LLM providers without losing access to data sources, as the protocol is model-agnostic.

Conclusion

The Model Context Protocol represents a fundamental shift that transforms the costly M×N integration problem into a more manageable M+N equation, enabling a new generation of context-aware AI applications that can dynamically adapt to business needs.

Although its adoption requires careful strategic evaluation, investment in technical capabilities, and a balance between innovation and stability, organizations that implement MCP in a planned manner will not only solve their current integration challenges but also build the infrastructure needed to compete in a future where technological agility and intelligent collaboration between systems will be key to business success.

Andrik Martínez is a full stack developer in the Digital Innovation Area at Honne. He has participated in artificial intelligence projects and the development of digital solutions that drive innovation in organizations across various sectors.

HONNE®
DELIVERING TRUE VALUE

ABOUT HONNE

Honne is a leading company that, through its consulting services, implements advanced technological solutions that automate processes, optimize operations, and reduce costs. It provides world-class support and operations through its Cloud Centers of Excellence (CCoE), which operate 24/7/365. Its comprehensive and personalized approach ensures that each client receives solutions tailored to their specific needs, thus boosting their efficiency and com petitiveness in the market. With a constant commitment to innovation, Honne is dedicated to transforming the way organizations operate and grow in the digital era.

www.honne.com

https://mx.linkedin.com/company/honne

LOCATIONS

Av. Juárez 1102 Pabellón M, Floor 33, Col. Centro, Monterrey, N.L, Mexico, 64000.
Corporative Office

Av. Insurgentes Sur 730 Floor 2, Col. del Valle, Benito Juárez, Mexico City, Mexico, 03100.
CDMX Office

Science and Technology Park, TecnoTam, Victoria City, Tamps., Mexico, 87020.
CcoE (Cloud Center of Excellence)

Cl. 81 #11-08 Chapinero, Bogotá, Colombia.
Colombian Office

Agustinas 833, 8320199, Santiago, Chile.
Chile Office

2700 Post Oak Blvd, Houston, Tx, USA, 77056.
USA Office

33 Rue La Fayette 75009, Paris, France.
France Office

REFERENCES

Gutowska, A. (s. f.). Model Context Protocol (MCP). IBM. Recuperado 25 de septiembre de 2025, de https://www.ibm.com/think/topics/model-context-protocol?utm_source=ibm_developer&utm_content=in_content_link&utm_id=tutorials_mcp-watsonx&cm_sp=ibmdev-_-developer-tutorials-_-ibmcom

Building AI applications with Model Context Protocol (MCP). (2025, 23 julio). IBM Developer. Recuperado 25 de septiembre de 2025, de https://developer.ibm.com/tutorials/mcp-watsonx/

Unlocking the power of Model Context Protocol (MCP) on AWS. (2025, 3 junio). Amazon Web Services. Recuperado 25 de septiembre de 2025, de https://aws.amazon.com/es/blogs/machine-learning/unlocking-the-power-of-model-context-protocol-mcp-on-aws/

Architecture overview. (s. f.). Model Context Protocol. Recuperado 25 de septiembre de 2025, de https://modelcontextprotocol.io/docs/learn/architecture

Connect your AI applications to the world. (s. f.). Model Context Protocol. Recuperado 26 de septiembre de 2025, de https://modelcontextprotocol.io/about

World Economic Forum. (2025). Global Cybersecurity Outlook 2025. Recuperado 20 de septiembre de 2025, de https://www.weforum.org/reports/global-cybersecurity-outlook-2025

IDC. (2025). Worldwide Digital Transformation Spending Guide. Recuperado 22 de septiembre de 2025, de https://www.idc.com/promo/dx/spending

Gartner. (2025). Top Strategic Technology Trends 2025. Recuperado 23 de septiembre de 2025, de https://www.gartner.com/en/information-technology/insights/top-tech-trends