

CIOReview

THE NAVIGATOR FOR ENTERPRISE SOLUTIONS



LEADING SECURITY TRANSFORMATION THROUGH TECHNOLOGY

Yasel Morales,
Vice President and CIO,
Genesis Security





LEADING SECURITY TRANSFORMATION THROUGH TECHNOLOGY

Yasel Morales, Vice President and CIO, Genesis Security

Yasel Morales is Vice President and CIO of Genesis Security, where she oversees technology strategy, cybersecurity and digital operations across Puerto Rico, the Caribbean and Florida.

Yasel Morales has never treated technology decisions as purely technical ones. As Vice President and CIO of Genesis Security, she weighs every initiative against its effect on the business and on the people who run it. This mindset took root early, during her years as a college student.

While working toward her master degree at the University of Puerto Rico at Mayagüez, she took on several information technology roles. What drew the young graduate in was technology's ability to solve real operational challenges, improve processes and create measurable value for organizations and their clients. Those early experiences also shaped a leadership philosophy centered on continuous learning and understanding an organization from the operational level upward.

Today, Morales brings that perspective to a security business where she combines technical expertise with a business perspective to ensure technology initiatives support employees, strengthen service delivery and contribute to Genesis Security's long-term growth.

That approach is visible in one of the most significant transformations Morales has led at Genesis Security: the evolution from traditional reactive system monitoring to a more proactive and resilient operating model. She introduced integrated AI-assisted video analytics, improved system connectivity and cybersecurity practice and redesigned operational processes around real-time information.

For Morales, however, the project was never simply about deploying novel technology, but about how it became part of the way people worked and made decisions. That required employee engagement, training, clear performance measures, security support and continued improvement.

"Sustainable transformation happens when technology becomes part of organizational culture and everyday decision-making rather than remaining another tool that has been introduced," says Morales.

TURNING AI INTO OPERATIONAL VALUE

Genesis Security has seen a measurable impact from the shift. AI analytics have reduced false alarms by more than 92 percent, allowing monitoring personnel and response teams to focus more of their attention on events that represent genuine threats. The change has improved resource allocation, sharpened response prioritization and reduced alarm fatigue.

AI-assisted video analytics have also improved response time, increased monitoring capacity and provided clients with more actionable information. The technology can detect specific behaviors and identify unusual activity, allowing teams to intervene earlier. It has also helped Genesis Security scale its service without increasing resources at the same rate.

That shift on the operations floor has also changed what clients expect from security technology, giving them more useful information to act on. What used to be simple discussions on security equipment is now a strategic dialogue on intelligence, prediction and measurable outcomes. Clients no longer expect a security system to simply report activity or sound an alert. They expect it to interpret events, tell normal behavior from a genuine threat and support faster, more informed decisions.

The results also revealed an important lesson about implementation. Morales had expected the technology to deliver value, but the level of preparation required before implementation was greater than anticipated. AI, she found, is not a plug-and-play solution. Its effectiveness depends on camera placement, image quality, connectivity, properly defined detection rules and continuous system calibration.

Yasel Morales

"Successful AI implementation requires a combination of strong technology, discipline, process and human expertise," says Morales.

Morales sees the same readiness gap across the wider market. The biggest challenge for mid-market enterprises, she believes, is not access to AI, but the organizational capability to use it well. Many still lack the data quality, system integration, cybersecurity maturity, internal expertise and governance structures needed to turn AI into value.



Much of that gap comes down to how companies think about AI in the first place. Many treat it as a product to purchase rather than a capability to build. An AI-enabled platform does not automatically create value on its own. Organizations need clearly defined use cases, measurable objectives, trained personnel, appropriate policy and real leadership commitment. This requires companies to invest as much in people, process and governance as they invest in technology itself.

BALANCING SCALE AND OPERATIONAL RESILIENCE

As Genesis Security expands across Puerto Rico, the Caribbean and Florida, Morales is focused on maintaining a consistent technology and cybersecurity foundation while tuning itself to each market's regulatory environment.

Genesis Security maintains common standards for system architecture, access control, data protection, documentation, monitoring and cybersecurity across every market it enters

while adapting implementation to the privacy rules, licensing, data retention and local security operations, which are evaluated properly before a solution goes live. Legal, compliance, operational and technical teams work together throughout, keeping the technology environment unified even as regulations differ from one market to the next.

“
Sustainable transformation happens when technology becomes part of organizational culture and everyday decision-making rather than remaining another tool that has been introduced.

As Genesis Security's technology environment continues to evolve across markets, Morales must ensure that upgrades, system integrations and cybersecurity improvements never compromise the availability of monitoring or response operations, which need to run around the clock.

That reality reinforced her focus on safe implementation, redundancy, testing, communication and well-defined contingency planning. It also taught her something broader: operational resilience is not a purely technical issue. It is a business responsibility, and part of her role as CIO is helping the organization move forward while ensuring innovation doesn't introduce unacceptable operational risk.

BUILDING FOR ORGANIZATIONAL ADAPTABILITY

Morales sees organizational adaptability as the defining capability of resilient enterprises over the next five years. She defines it as the ability to identify change, make important decisions and respond quickly without compromising security or operational continuity.

Building that adaptability requires resilient infrastructure, cybersecurity, data governance, system interoperability and workforce development. Just as important, technology and business teams must work together rather than operate on separate tracks.

The most resilient enterprise, Morales believes, will not necessarily be the one with the most technology. It will be the one that can integrate technology into its operations, learn from its data and evolve responsibly. 



CIOReview LATAM
(ISSN 2644-237X)

ValleyMedia, Inc.
600 S ANDREWS AVE STE 405
FT LAUDERDALE, FL 33301

www.cioreview.com