

2025

seceon

Colombia's Cybersecurity Crisis:

Blind Eagle's Shadow Over Latin America's Digital Transformation

How the Most Active APT in Latin America is Targeting Colombia's Government, Financial Sector, and Critical Infrastructure

Executive Summary

Colombia’s digital transformation journey is being tested by an unprecedented cybersecurity crisis. As Colombia cements its position as a rising regional tech hub-with technology investment, near-shoring, and $25 billion in yearly cryptocurrency circulation, it now faces a relentless campaign from Blind Eagle (APT-C-36), Latin America's most persistent and advanced threat group. With over 1,600 victims during major campaigns in late 2024 and early 2025-including targeted attacks on government, finance, and energy-ncidents like the IFX Networks ransomware wave (affecting 762 organizations across 17 countries) highlight both the opportunity and risk within Colombia’s fast-growing $1.12B cybersecurity market.

Despite notable governmental investments, including the new National Security Operations Center (SOC), Colombia faces an acute 30,000-strong cybersecurity talent gap. This white paper analyzes the threat environment, regulatory trends, and outlines how AI-driven, unified threat management platforms such as Seceon can future-proof Colombia’s economic and digital ambitions while neutralizing the APT threat.

The Escalating Cybersecurity Landscape in Colombia

Threat Scope and Impact

- **Blind Eagle: An Adaptive, Persistent Threat:** Blind Eagle (APT-C-36) has, since 2018, used multi-stage phishing, malware, and infrastructure attacks to systematically target Colombia's government (including judicial and tax authorities), financial sector, and healthcare institutions.
  - In one 4-month campaign (Nov 2024-Mar 2025), over 1,600 Colombian organizations were compromised.
  - Notably, these campaigns harvested thousands of government, finance, and education credentials-including HTML files exposing 8,000+ valid entries and ATM PINs.
- **Major Incidents: IFX Networks Ransomware:** September 2023's IFX Networks attack crippled courts, clinics, and public services, with service outages spreading to 17 LATAM countries. More than 50 state and private Colombian entities, including the judiciary, reported direct operational impact.
- **Market Size and Growth:** Colombia's cybersecurity market reached $1.12B in 2025, growing at 10.95% annually-driven by necessity as much as innovation.

Techniques and Evolving Tactics

- **Rapid Exploit Adaptation:** Blind Eagle is notable for instant exploitation of vulnerabilities-e.g., weaponizing NTLM authentication flaws (CVE-2024-43451) in less than a week after Microsoft patch release.
- **Advanced Payload Delivery and Infrastructure:** Operations include abusing legitimate cloud platforms (GitHub, Google Drive, Dropbox), deploying customizable Dynamic DNS for C2, and layering sophisticated obfuscators (HeartCrypt, PureCrypter).
- **Social Engineering Mastery:** Regionally tailored phishing uses DIAN (tax authority), judiciary, and bank impersonations-crafted with cultural insight and convincing documentation.

Vulnerable Sectors

- **Government:** Repeated attacks on judicial systems and legal databases, tax authorities, and municipal offices impede public services.
- **Finance:** Large-scale bank and fintech credential harvesting; open banking APIs mandated by Decree 1297/2022 create new attack surfaces.
- **Energy:** Distributed, aging grid and legacy SCADA systems are favorite targets amid grid modernization and 5G expansions.
- **Healthcare:** Ransomware campaigns repeatedly disrupt patient data and telemedicine.

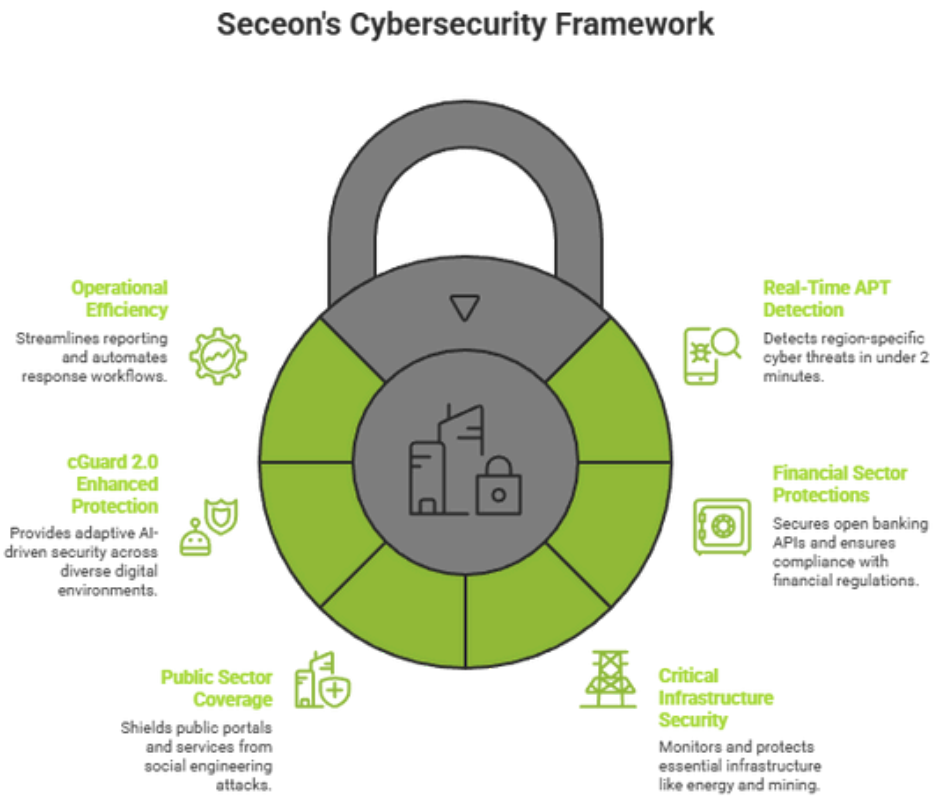
Why Fragmented Security Approaches Fail

- Most Colombian organizations run a patchwork of siloed threat detection, incident response, and compliance tools.
- Manual compliance (for SuperFinanciera, CREG, data protection) is slow and error-prone.
- Elevated operating costs, degraded detection accuracy, and excessive false positives (often exceeding 80%) are the norm.
- Lack of multilingual threat correlation and local threat intelligence means APT campaigns, like those run by Blind Eagle, regularly evade detection for weeks.

Seceon's Unified AI Cybersecurity Platform: Tailored for Colombia

- **Real-Time APT Detection:**
  - Detects region-specific campaigns in under 2 minutes, with built-in Spanish-language and cultural threat intelligence.
- **Financial Sector Protections:**
  - Real-time open banking API security (essentials for Decree 1297/2022).

    - Automated SuperFinanciera compliance workflows, including continuous risk monitoring and incident reporting.
- **Critical Infrastructure Security:**
    - aiSecOT360: Specialized SCADA/ICS/IoT monitoring for Colombia's grid operators, gas, and mining firms.
    - 5G and modernization project visibility.
- **Public Sector Coverage:**
    - Social engineering protection for DIAN, judiciary, and public service portals.
- **CGuard 2.0 Enhanced Protection:** Seceon's CGuard 2.0 is a next-generation cloud-native security platform extending autonomous threat detection and automated mitigation to endpoint, cloud workloads, and IoT/OT environments. It strengthens defense across Colombia's diverse infrastructure by providing adaptive AI-driven protection tightly integrated with the Seceon ecosystem for unified visibility and control.
- **Operational Efficiency:**
    - Unified reporting reduces prep from weeks to minutes; automated response workflows mitigate skill shortages.



Sector-Specific Applications and Outcomes

Government

Key threats: Phishing, malware, impersonations, and ransomware.

Seceon capabilities: Multi-language social engineering detection, instant legal database anomaly alerts.

Impact examples: Enhanced resilience of court services, reduced incident response time, with support from Colombia's National Security Operations Center.

Finance

Key threats: Credential theft, business email compromise (BEC), API fraud.

Seceon capabilities: Real-time transaction and fraud analytics, open banking API protection aligned with regulatory mandates.

Impact examples: Millions prevented in fraudulent losses, faster customer recovery due to advanced fraud detection and regulatory compliance measures.

Energy & Utilities

Key threats: SCADA attacks, ransomware, IoT/5G network risks.

Seceon capabilities: OT/ICS visibility and legacy asset security to protect Colombia's distributed grid and modernize energy infrastructure.

Impact examples: Improved grid uptime and reliability, fewer blackouts through real-time monitoring and proactive threat remediation.

Healthcare

Key threats: Ransomware, patient data breaches.

Seceon capabilities: Endpoint protection and continuous compliance monitoring to safeguard telemedicine and healthcare records.

Impact examples: Fewer operational outages, improved patient data security, and reduced impact from malware and ransomware campaigns.

Private Technology & Near-Shoring Enterprises

Key threats: Supply chain attacks, intellectual property theft.

Seceon capabilities: Cross-border compliance and reporting automation, SIEM tailored for Latin American tech sector needs.

Impact examples: Secures more than $2B in technology sector investments, increases investor confidence and operational continuity for Colombia's growing near-shoring industry.

Real-World Incidents and Case Illustrations

- **IFX Networks Attack (2023):** Hundreds of entities, from the judiciary to city governments, are affected by ransomware. Highlights the urgent need for cross-sector response preparation and automated breach reporting processes.
- **Blind Eagle Exploit Cycle:** Demonstrated ability to weaponize new vulnerabilities in under a week. Only AI-powered, multilingual threat intelligence can keep pace.
- **National SOC Initiative:** New National Security Operations Center aims to support 6,400 public and 300,000 private firms, signaling Colombia's largest-ever public sector cyber investment. Success will depend on platforms with AI, automation, and region-specific intelligence.

Compliance, ROI, and Strategic Value

- **Regulatory Readiness:** Automated compliance for SuperFinanciera banking security rules, Decree 1297/2022, and energy regulation frameworks (CREG).
- **Financial & Operational ROI:** Breach response automation and real-time reporting free talent to focus on high-value tasks, mitigate labor shortages, and reduce time-to-detection from days to minutes.
- **Investor & Public Confidence:** Sustained grid, financial, and public sector trust are foundational for continued near-shoring and international partnership investment.

Key Benefits

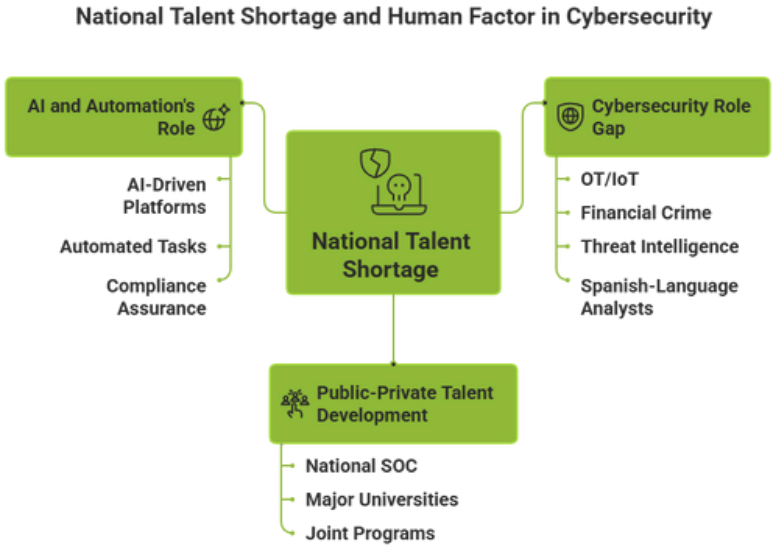
Regulatory Readiness
Automated compliance with banking security rules and energy regulation frameworks.

Financial ROI
Breach response automation frees talent, mitigates shortages, and reduces detection time.

Investor Confidence
Sustained trust is foundational for continued investment and international partnerships.

The National Talent Shortage and the Human Factor

- **30,000 Cybersecurity Role Gap:** Acute need for OT/IoT, financial crime, threat intelligence, and Spanish-language analysts.
- **Public-Private Talent Development:** National SOC and major universities are launching joint programs, but upskilling must scale rapidly.
- **AI and Automation's Role:** AI-driven platforms fill critical skill gaps, automate repetitive tasks, and ensure compliance in the absence of large in-house teams.



Colombia Cybersecurity Intelligence 2025

Critical Infrastructure Security & Seceon Defense Platform

1,600+	762	133%	$25B
Victims in Single Blind Eagle Campaign	Companies Affected by IFX Ransomware	Increase in Ransomware Incidents	Annual Crypto Transactions (5th Globally)

Critical Threats

- **Blind Eagle (APT-C-36)**
  Government targeting, banking phishing, RATs deployment, 8,075 compromised credentials
- **BlackCat/ALPHV Ransomware**
  Sophisticated evasion, multi-platform infections, critical infrastructure targeting
- **Financial Sector Phishing**
  Bancolombia, BBVA, Davivienda impersonation campaigns with ATM PIN harvesting
- **Energy Grid Vulnerabilities**
  SCADA system exploitation, grid stability threats, regulatory compliance gaps
- **Healthcare Sector Targeting**
  EPS Sanitas, Audifarma breaches, patient data exposure, operational disruption
- **Supply Chain Vulnerabilities**
  Third-party service provider compromises, lateral movement, manufacturing disruption

Seceon Platform Performance

✓ **aiSIEM - Intelligent Analytics**
- Blind Eagle APT detection & response
- Banking trojan behavioral analysis
- Cryptocurrency transaction monitoring
- Spanish language threat intelligence

✓ **aiXDR - Extended Detection**
- SCADA/ICS protection protocols
- Cross-border supply chain protection
- Real-time threat correlation
- Automated incident response

✓ **aiSecOT360 - OT/IoT Security**
- Energy grid protection
- Industrial control system security
- IoT device monitoring
- Critical infrastructure defense

Business Impact Analysis

$1.12B	10.95%	30.1%	30,000
Cybersecurity Market Value 2025	Annual Market Growth Rate	Banking Sector Security Investment	Cybersecurity Talent Shortage

For Colombia's toughest cyber threats, Seceon delivers unstoppable protection.

Conclusion: Unified AI Security-A Regional Imperative

Colombia is both a digital pioneer and a cyber target in Latin America. As Blind Eagle and similar groups escalate multi-sector attacks, previous patchwork solutions will fail to address the scope, speed, and cultural specificity of these threats. The future belongs to those who deploy unified, AI-powered cybersecurity platforms combining region-aware threat intelligence, automated compliance, and rapid response at scale.

Colombian institutions-government and private alike must now treat cybersecurity not just as a compliance obligation, but as a core business and national security enabler. Only then can the country's digital transformation yield its full promise, with robust protection for citizens, enterprises, and critical infrastructure.

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, aiXDR, and aiMSSP platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 700 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,000 clients.

References and Citations:

This whitepaper is based on research and data from:

- The Hacker News - Blind Eagle's campaign details
- Darktrace - APT-C-36 tactics
- Check Point Research - Blind Eagle operations
- SC Media - Major incidents in Colombia
- KPMG - LATAM threat intelligence
- Mordor Intelligence - Market size/growth
- Thomas Murray - IFX Networks fallout
- Ventas de Seguridad - National SOC inauguration
- LinkedIn - Colombian fintech/open banking regulation
- INCIBE CERT - IFX ransomware impact
- Internexa - CNO 1960 compliance
- EIN Presswire - Workforce statistics
- Trustwave - APT evolution

About the Author

Anamika Pandey

AI/ML Cybersecurity Engineer, Seceon Inc.



Anamika leverages artificial intelligence, machine learning, and Dynamic Threat Modeling (DTM) to fortify IT, OT, IoT, and cloud infrastructures. Her expertise lies in advancing AI-driven defense strategies that not only ensure compliance and resilience but also deliver measurable ROI. Through Seceon's OTM Platform, she helps organizations anticipate, detect, and mitigate evolving cyber threats, empowering them to stay secure, adaptive, and future-ready.

© 2025 Seceon Inc. All rights reserved. aiSIEM, aiXDR, are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.