

Costa Rica. May, 2026

The greatest risk of a cyberattack is within the company itself: human error and lack of investment expose companies

- Grupo EULEN Costa Rica recommends implementing multi-factor authentication, permanent monitoring and internal awareness programs to prevent incidents

In an environment where digital transformation is advancing faster than the technological maturity of many organizations, human error and a lack of sustained investment in cybersecurity continue to be two of the main vulnerabilities that expose companies to incidents capable of completely compromising their operation.

Opening emails of dubious origin, entering unverified websites, downloading external files, or connecting USB devices to corporate computers are seemingly everyday actions that can facilitate unauthorized access, credential theft, malware installation, or ransomware attacks. The growth of hybrid work, accelerated digitalization, and interconnection with external providers have significantly expanded the attack surface of companies, increasing the vulnerabilities from where a cybercriminal can compromise corporate operations.

According to FortiGuard *Labs' 2026 Threat Landscape Report*, Costa Rica registered more than **225.7 million attempted cyberattacks during 2025**, reflecting the growing pressure on public and private digital infrastructures. Globally, threats targeting enterprise networks are on the rise, driven by automated campaigns, artificial intelligence, and advanced social engineering.

Human error: the main attack vector

According to José Ricardo López García, Director of Cybersecurity at Grupo EULEN, although technological platforms have evolved to incorporate multiple layers of protection, human behavior continues to be decisive within the defense strategy. *"The user is not the weakest link; It's the last line of defense when all else fails. But it can only be if the organization has trained it, given it tools, and invested what it takes so that it can stop before it clicks."*

Among the highest-risk practices identified in corporate environments are:

- Interaction with fraudulent emails or phishing campaigns.
- Browsing untrusted or un reputable websites validated by corporate controls. Downloading unauthorized apps or files.
- Use of external devices without device control or DLP policies.
- Share corporate credentials across any channel.

The EULEN Group is a leader in the design of services to companies, with the aim of offering society innovative services that provide useful, quality and more efficient solutions. He specialises in cleaning, security, auxiliary services (logistics, general and telemarketing), FSM (Facility Services & Management), social and health services, comprehensive maintenance, global human resources and employment and environmental solutions. Founded in 1962 in Bilbao, the company is present in 11 countries and has consolidated sales of more than 1,600 million euros, with a global workforce of more than 75,000 people.

The EULEN Group is a member of the Global Compact and firmly committed to society through the development of socially responsible policies: integration of disadvantaged groups into the labour market, reconciliation of family and professional life for its staff

For more information:

Natalia Carvajal Lorenzo Tel. +506 6081-7777
ncarvajal@themapcomm.com
<http://www.themapcomm.com>

The Map Communications

López García warns that these threats are constantly evolving through social engineering techniques powered by artificial intelligence, capable of generating hyper-personalized messages, deepfakes and impersonations that are increasingly difficult to detect.

Lack of investment and continuous monitoring

Beyond individual actions, Grupo EULEN warns of a structural problem: many companies still do not integrate cybersecurity into their strategic or budgetary planning.

"There are still organizations without permanent monitoring, without continuous maintenance of their platforms and without controls over what happens within their corporate networks. In today's digital environment, that is equivalent to operating without visibility," López García said.

Among the main weaknesses detected in organizations are the absence of multi-factor authentication (MFA), outdated systems, and lack of permanent monitoring. Specialists warn that multi-factor authentication should no longer be seen as an advanced measure, but as a basic standard of protection for any corporate environment.

Fernando Gamboa, Security and Operations Manager of Grupo EULEN Costa Rica emphasizes the need for specialized support: "Companies must opt for a comprehensive security strategy where cybersecurity is no longer included as an optional expense, but as a critical component of business continuity. Having specialists allows us to prevent, monitor and respond to threats in real time, significantly reducing the operational and financial impact."

In the face of increasingly sophisticated threats, many organizations are migrating to Zero Trust security models, an approach where no user, device, or connection is considered trusted by default, even within the enterprise network itself.

Specialists agree that cybersecurity must be approached from a comprehensive vision that combines technology, continuous monitoring, risk management and permanent training of employees, especially in a scenario where threats evolve with greater speed and sophistication.

At EULEN Group we accompany organizations in the identification, detection, monitoring and response of cyber incidents.

The EULEN Group is a leader in the design of services to companies, with the aim of offering society innovative services that provide useful, quality and more efficient solutions. He specialises in cleaning, security, auxiliary services (logistics, general and telemarketing), FSM (Facility Services & Management), social and health services, comprehensive maintenance, global human resources and employment and environmental solutions. Founded in 1962 in Bilbao, the company is present in 11 countries and has consolidated sales of more than 1,600 million euros, with a global workforce of more than 75,000 people.

The EULEN Group is a member of the Global Compact and firmly committed to society through the development of socially responsible policies: integration of disadvantaged groups into the labour market, reconciliation of family and professional life for its staff

For more information:

Natalia Carvajal Lorenzo Tel. +506 6081-7777
ncarvajal@themapcomm.com
<http://www.themapcomm.com>

The Map Communications