ayesa

Cybersecurity 2026

Key Predictions and Trends

ayesa.com

Cybersecurity 2026:

A strategic vision to protect the business in an increasingly complex digital environment

Introduction

Over recent years, cybersecurity has evolved at an accelerated pace. However, 2026 marks a clear inflection point. The combination of artificial intelligence, hyperconnectivity, reliance on complex digital ecosystems, and growing regulatory pressure places organizations in an unprecedented risk landscape—but also one of opportunity

Digital security can no longer be understood as a purely technical or reactive function. Today, it is a **structural pillar of the business**, directly linked to operational continuity, customer and partner trust, and the ability to innovate with confidence. In 2026, organizations that fail to integrate cybersecurity into their business strategy will be assuming an unsustainable level of risk.

At the same time, cybercrime has reached a notable level of maturity and professionalization. Attacks are no longer random or opportunistic. They are **targeted, persistent, and designed to maximize economic, operational, and reputational impact**. Artificial intelligence acts as a force multiplier, enabling attackers to scale, personalize, and automate as never before. Yet this same technology has become a key ally for defensive teams, enhancing their ability to detect, analyze, and respond with greater speed and precision.

This report is driven by a clear objective: **to help our clients—and organizations more broadly—anticipate the cybersecurity landscape that will define 2026**. Its purpose is not only to identify trends, but to provide context, criteria, and practical guidance to support decision-making. The predictions presented here are grounded both in market evolution and in Ayesa's real-world experience supporting organizations in critical sectors as they define and operate their cybersecurity capabilities.

Ultimately, **2026 will mark a turning point for cybersecurity**. The combination of technological innovation, continuous training, and strategic collaboration will determine whether organizations succeed in protecting critical assets and building a safer digital environment. Adapting to this complex and constantly evolving scenario will not be optional—it will be essential to ensure sustainability and competitiveness in a digital world.

In the following pages, we will explore each trend in detail, analyzing its impact, associated risks, and the key recommended courses of action. The goal is to offer a clear, practical vision that helps organizations strengthen their digital resilience and prepare for an increasingly demanding and complex environment.

Cybersecurity 2026:

A strategic vision to protect the business in an increasingly complex digital environment

Executive Summary

Generative artificial intelligence is firmly established as the primary driver of change. In 2026, we will see increasingly autonomous, personalized, and adaptive attacks, countered by AI-enhanced defenses that are reshaping how SOCs and incident response teams operate. AI evolves from a supporting tool into a **structural component of cybersecurity**.

Ransomware enters a new phase of maturity. It evolves toward multi-layered extortion models that combine encryption, data theft, reputational pressure, and supply-chain attacks. **Resilience**, rather than absolute prevention, becomes the true strategic objective.

At the same time, **security of artificial intelligence itself** emerges as a critical new domain. Models, training data, and intelligent agents become high-value assets that must be protected against manipulation, theft, or data leakage, giving rise to the approach commonly known as **MLSecOps**.

The **SOC** undergoes a profound transformation, shifting from a reactive monitoring center to a **decision-making hub**, supported by automation, behavioral analytics, and security processes defined as code. This evolution enables a drastic reduction in detection and response times.

The convergence of **IT, OT, and IoT** extends digital risk into the physical world. In 2026, cyberattacks directly impact production, energy, transportation, and critical services, requiring specialized security approaches that prioritize operational continuity and industrial safety.

Digital identity is confirmed as the new true perimeter. The rise of deepfakes, advanced social engineering, and attacks on multi-factor authentication significantly increases the risk of corporate fraud and account compromise, demanding stronger controls and continuous verification.

From a medium- and long-term perspective, **post-quantum cryptography** gains relevance on the security agenda. While the quantum threat is not yet immediate, the need to protect long-lived data drives organizations to begin planning their transition now.

The **Zero Trust** model reaches maturity and consolidates itself as the reference architecture. Implicit trust disappears, replaced by continuous control, least-privilege access, and microsegmentation across hybrid and distributed environments.

Regulation and reporting requirements reinforce the need to demonstrate—not merely declare—the ability to manage incidents. Cyber resilience becomes a **business KPI**, with direct impact on governance and board-level decision-making.

Finally, **talent and security culture** remain decisive. Artificial intelligence can boost team productivity, but it does not replace human judgment. Continuous training, awareness, and the integration of security across the entire organization will be essential to successfully meet the challenges of 2026.

Generative AI 2.0: When attacks think and defenses learn

Artificial intelligence becomes, in 2026, the **primary catalyst for change in cybersecurity**. We are no longer talking about an emerging technology or a mid-term promise, but about a **structural element** that redefines both how attacks are carried out and how defenses are built. AI ceases to be a point solution and becomes a **permanent actor** within the threat and protection ecosystem.

In recent years, generative AI has demonstrated its ability to produce text, code, images, and voice with striking realism. By 2026, this capability is seamlessly integrated into attack workflows, enabling cybercriminals to automate tasks that previously required time, expertise, and human effort. The result is a **qualitative and quantitative leap** in the scale and sophistication of attacks.

AI-driven attack industrialization

One of the most significant shifts is the **industrialization of reconnaissance and attack preparation**. AI models make it possible to analyze large volumes of public and semi-public information in minutes: organizational charts, professional profiles, technology providers, domains, previous data leaks, or exposed internet-facing technologies. Based on this analysis, AI builds **highly personalized attack maps** for each organization

This leads to far more precise social engineering campaigns. Messages are no longer generic or easily identifiable. They are written in the right tone, in the correct language, with credible internal references, and sent at the time of day when the victim is most likely to engage. Even the writing style can be adapted to mimic that of a spoofed sender, **exponentially increasing success rates**.

AI as an amplifier of attacks... and defenses

The automated generation of malicious code is another key factor. In 2026, we will see **on-demand malware and scripts**, tailored to the victim's environment and capable of modifying their behavior to evade traditional security controls. AI enables rapid iteration: if one attempt fails, the next is adjusted in real time.

Generative AI 2.0: when attacks think and defenses learn

Beyond isolated tools, the use of **autonomous attack agents** begins to consolidate, capable of chaining actions without constant human supervision. These agents can explore a network, test credentials, move laterally, and adjust their strategy based on the responses of the environment.

Augmented defense: AI at the service of the SOC and response

In this scenario, organizations also incorporate AI as a defensive pillar. In 2026, the most advanced SOCs no longer rely solely on static rules or signatures. They use AI models capable of correlating signals, identifying anomalous patterns, and prioritizing incidents based on their real impact on the business.

The main contribution of defensive AI is **noise reduction**. Where thousands of daily alerts were previously generated, now only a few contextualized incidents are presented, with clear information about the affected asset, the possible cause, the scope of the attack, and the recommended actions. This allows analysts to focus their attention on what truly matters.

In addition, AI acts as an assistant in incident response. It can suggest playbooks, execute automated containment actions in low-risk cases, and help generate reports, timelines, and evidence for audits or legal processes. In crisis situations, this capability is key to gaining time and reducing human errors.

The combination of automation and intelligence allows smaller teams to operate more complex environments, something especially relevant in a context of scarcity of specialized talent.

New risks derived from the use of AI

However, the massive adoption of AI also introduces **inherent risks**. The use of public AI tools by employees can cause involuntary leaks of sensitive information. Models may make decisions that are difficult to explain or audit, which creates challenges from a regulatory and governance perspective.

Generative AI 2.0: when attacks think and defenses learn

In addition, excessive reliance on automation can create a false sense of security. AI is only as good as the data and rules that feed it. Without human oversight and without adequate controls, it can amplify errors or overlook critical signals.

In 2026, one of the major challenges will be finding the balance between leveraging the potential of AI and maintaining control, transparency, and accountability in decision-making.

Impact for organizations

The impact of this trend is cross-cutting. It affects how awareness campaigns are designed, how security teams are structured, incident response processes, and organizational culture itself. The question is no longer whether AI should be used in cybersecurity, but **how to do so in a secure and effective way**.

Organizations that integrate AI with a strategic vision, combining technology, processes, and people, will be better prepared to face an increasingly dynamic threat environment. Those that adopt it without governance will assume new risks that may be even more difficult to manage than traditional ones.

KEY POINTS AND RECOMMENDATIONS
Define clear policies for the use of AI within the organization, especially in relation to sensitive data.
Incorporate defensive AI capabilities into SOC and security operations, prioritizing use cases with real impact.
Always maintain human oversight in critical decisions and in the response to high-impact incidents.
Invest in data quality, traceability, and explainability of the models used.
Preparar a los equipos mediante formación específica sobre riesgos y oportunidades de la IA.

Ransomware 4.0: the era of total extortion and systemic blackmail

If there is one threat that symbolizes the maturity of cybercrime in 2026, it is ransomware. Far from being a one-off technique, ransomware has become a highly structured business model, capable of adapting, innovating, and maximizing profits with efficiency comparable to that of many legitimate companies.

In this new stage, which we can call Ransomware 4.0, the objective is no longer solely to encrypt systems. The attacker seeks to **control the narrative, the timing, and the pressure** exerted on the victim, using multiple extortion levers in a coordinated manner.

From encryption to strategic blackmail

In its early years, ransomware was based on a relatively simple scheme: encrypt information and demand a ransom to recover it. In 2026, this approach proves insufficient. Organizations have improved their backup and recovery capabilities, and attackers know it.

> We are witnessing the definitive professionalization of extortion.

As a result, ransomware evolves toward a **multiple extortion model**, where encryption is just one more piece of the machinery. Before executing the visible attack, criminals spend time understanding the victim's environment: which data is most sensitive, which services cannot be stopped, which regulatory obligations exist, and what impact a public data leak would have.

Once inside, the attacker moves stealthily, steals selected information, and only when ready activates the encryption. If the victim does not respond, pressure increases progressively: partial leaks, threats to customers or partners, and even discredit campaigns designed to damage the organization's reputation.

Ransomware 4.0: the era of total extortion and systemic blackmail

The key role of the supply chain

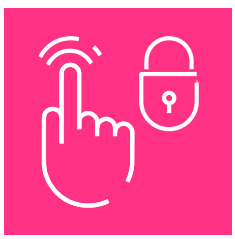
One of the factors gaining the most weight in 2026 is the **attack on the supply chain**. Instead of directly compromising a large organization, attackers seek providers with lower cybersecurity maturity but with privileged access to multiple clients.

A single compromise can open the door to dozens of organizations simultaneously, multiplying the impact of the attack and the potential for extortion. This approach reduces the attacker's effort and increases pressure on victims, who are affected by an incident they did not directly cause.

For many organizations, this type of attack reveals an uncomfortable reality: their level of risk does not depend solely on their own controls, but also on their ecosystem.

Ransomware as a service: total professionalization

In 2026, ransomware operates under fully consolidated **Ransomware-as-a-Service (RaaS)** models. There are malware developers, initial access brokers, negotiation specialists, and infrastructure operators, each with a clearly defined role.



This means that the entry barrier to launching an attack is increasingly low. An actor without deep technical knowledge can acquire compromised access, rent malware, and execute an attack with notable effectiveness. The direct consequence is an increase in the volume of attacks and a greater diversity of actors involved.

In addition, these groups operate with clear metrics: success rate, average negotiation time, average ransom amount. They adjust their strategies based on results, which turns them into increasingly efficient adversaries.

Ransomware 4.0: the era of total extortion and systemic blackmail

Resilience as the main objective

In this context, the key question is no longer whether an organization can avoid all ransomware attacks, but whether it is prepared to **withstand them and recover** with an acceptable impact. Resilience becomes the true strategic objective.

This implies accepting that an attack may occur, but designing the architecture, processes, and response plans to limit its scope. Immutable backups, environment segmentation, privileged access control, and well-rehearsed crisis plans make the difference between a serious incident and an existential crisis.

Impacto para las organizaciones

The impact of ransomware in 2026 goes far beyond the financial ransom. Affected organizations face prolonged outages, high recovery costs, loss of trust from customers and partners, and in many cases, notification obligations that amplify reputational damage.

Even when backups are available, full restoration can take days or weeks. During that time, operations are affected, decision-making slows down, and a huge amount of internal and external resources is consumed.

In addition, the risk of **double victimization** is real. Organizations that pay or that do not address the root causes of the incident may become recurring targets.

KEY POINTS AND RECOMMENDATIONS
Design a robust backup strategy, with immutable copies and periodic restoration tests.
Segment networks and critical systems to limit the propagation of the attack.
Control and monitor privileged access and third-party access.
Prepare and rehearse a ransomware response plan that includes technical, legal, communication, and business aspects.
Continuously assess supply chain risk and require minimum security guarantees.

MLSecOps: protecting the intelligence that drives the business

As artificial intelligence is integrated into critical organizational processes, a new reality emerges: **AI stops being a supporting tool and becomes a strategic asset**. In 2026, machine learning models, decision engines, intelligent assistants, and autonomous agents directly influence areas such as fraud, risk management, operational optimization, customer service, and executive decision-making.

This shift forces security to be rethought from a new perspective. Protecting servers, applications, or networks is no longer sufficient. It is necessary to **protect the models, the data that feeds them, and the processes that make them work**. From this need arises the approach known as MLSecOps.

When AI becomes an attack surface

Unlike traditional systems, AI models present specific attack vectors that are not always evident. A model can be manipulated without the need to compromise a server or exploit a classic vulnerability. It is enough to influence its data, its inputs, or its context.

One of the most relevant risks is **training data poisoning**. Introducing malicious, biased, or manipulated information into datasets can progressively degrade model quality or silently induce erroneous behaviors. The impact is often not immediate, which makes detection difficult and increases risk.

> AI itself becomes a target of attacks.

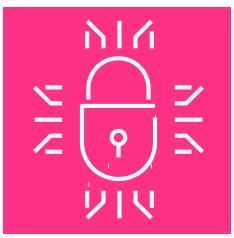
Another critical vector is the manipulation of prompts and inputs, especially in generative models and conversational assistants. Through prompt injection techniques, an attacker can induce the model to ignore restrictions, reveal sensitive information, or execute unintended actions.

Model theft also becomes relevant. Through repeated queries and analysis of responses, an attacker can partially reconstruct the model's logic, appropriate intellectual property, or discover internal patterns that facilitate future attacks.

MLSecOps: protecting the intelligence that drives the business

Invisible risks, very real consequences

The impact of these attacks does not always manifest as an obvious breach. In many cases, the consequences are subtle but profound. A model that makes incorrect risk decisions can generate sustained financial losses. An assistant that leaks sensitive information can cause regulatory non-compliance. A manipulated automated system can erode the trust of customers and partners without the cause being evident at first glance.



In addition, the inherent opacity of many AI models makes traceability difficult. When an automated decision is challenged, it is not always easy to explain why it occurred, with what data, and under what conditions. In an increasingly demanding regulatory environment, this lack of explainability becomes a risk in itself.

The AI lifecycle as a focus of control

The MLSecOps approach proposes applying security, control, and governance principles across the entire AI lifecycle. This implies going beyond the production environment and considering each phase as a potential point of exposure.

From data collection and storage, through model training, validation, and deployment, to the inference and maintenance phase, each stage must have appropriate controls. Environment separation, access management, monitoring of anomalous behavior, and decision logging are fundamental elements.

In 2026, the most mature organizations will no longer treat their models as “black boxes,” but as critical assets with defined owners, assigned risk levels, and specific controls.

MLSecOps: protecting the intelligence that drives the business

Governance and accountability in decision-making

AI security is not just a technical issue. It has direct implications for corporate governance. Who is responsible for a decision made by a model? How is its behavior validated? How is compliance with ethical, legal, and security principles ensured?

These questions become especially relevant in regulated sectors and in use cases that affect people, finances, or critical infrastructures. In 2026, organizations will need to demonstrate not only that they protect their models, but that they **govern their use responsibly**.

Impact for organizations

The advancement of AI makes MLSecOps an essential discipline. Organizations that do not address these risks will face threats that are difficult to detect and even harder to explain. Conversely, those that integrate security into the design and operation of their AI systems will gain trust, resilience, and competitive advantage.

MLSecOps does not slow innovation; it makes it sustainable. It enables scaling the use of AI with control, minimizing risks and responding quickly to anomalous behavior.

KEY POINTS AND RECOMMENDATIONS
Inventory AI models, datasets, and agents used within the organization, identifying their criticality.
Protect training data against manipulation, unauthorized access, and leaks.
Implement controls over prompts, inputs, and outputs of models.
Monitor model behavior to detect deviations or improper use.
Establish clear governance and accountability frameworks for automated decision-making.

The intelligent SOC: from alert center to decision center

For years, Security Operations Centers (SOCs) have been the core of organizations' digital defense. However, they have also carried one of the great paradoxes of modern cybersecurity: the more technology was deployed, the more alerts were generated, and the harder it became to distinguish what was important from what was accessory.

In 2026, this situation changes decisively. The SOC stops being a reactive center, saturated with signals, to become a **decision center**, where intelligence, automation, and context make it possible to act with speed, coherence, and focus on the real impact on the business.

The end of the SOC as an ¨alert factory¨

The volume of security events grows constantly. Endpoints, identities, networks, applications, cloud environments, and OT devices generate continuous telemetry. In traditional models, this abundance of information translates into thousands of daily alerts, many of them of low value.

> The SOC evolves to become a key component of digital resilience.

In 2026, the most advanced SOCs break with this approach. Instead of isolated alerts, they work with correlated incidents, where multiple signals are grouped and analyzed as part of the same behavior. Artificial intelligence and advanced analytics make it possible to identify patterns that, individually, would go unnoticed.

The result is a drastic reduction in noise and a significant improvement in detection quality.

The intelligent SOC: from alert center to decision center

Automation and SecOps as code

One of the major changes of the intelligent SOC is the adoption of **SecOps as code**. Response processes move from static procedures to playbooks that are defined, versioned, and systematically tested. This approach enables:

- Faster and more consistent responses.
- Less dependence on improvised decisions in moments of pressure.
- Greater traceability and ease of auditing.

Automation plays a key role, especially in repetitive and low-risk tasks: endpoint isolation, account blocking, alert enrichment, or evidence collection. In this way, human analysts can focus on advanced investigation and the management of complex incidents.

Behavior and context based detection

In 2026, detection is no longer based solely on signatures or known indicators. Attackers use legitimate credentials, malware-free techniques, and discreet lateral movement. To detect them, it is essential to understand the **normal behavior of users, systems, and processes**.

The intelligent SOC incorporates advanced behavior analysis capabilities (UEBA, NDR) that make it possible to identify subtle deviations: out-of-pattern access, unusual movement between systems, or anomalous use of privileges. These signals, combined with contextual intelligence, make it possible to detect attacks that would otherwise go unnoticed.

Threat intelligence integration with a practical approach

Threat intelligence ceases to be a generic stream of indicators and becomes a contextualized and actionable element. In 2026, the intelligent SOC uses Threat Intelligence adapted to the sector, geography, and risk profile of the organization.

This makes it possible to anticipate active campaigns, prioritize truly exploitable vulnerabilities, and adjust defenses based on real context. Intelligence stops being a static product and becomes an integrated capability within daily operations.

The intelligent SOC: from alert center to decision center

The SOC as an enabler of resilience

Beyond detection and response, the intelligent SOC becomes a key component of **digital resilience**. It is the point where visibility, response capability, and coordination with other areas converge: IT, business, legal, communication, and providers.

In crisis situations, the SOC acts as a nerve center for information, providing a clear and up-to-date view of the incident, facilitating decision-making and reducing uncertainty. This capability is especially relevant in an environment where response times make the difference between a controlled incident and a high-impact crisis.

Impact for organizations

The evolution toward an intelligent SOC allows organizations to manage a more complex threat environment with greater efficiency and predictability. Dependence on large teams is reduced, response quality is improved, and trust from customers, partners, and regulators is strengthened.

In addition, this model facilitates the adoption of hybrid schemes, combining dedicated and multi-tenant resources, without sacrificing control or service quality.

KEY POINTS AND RECOMMENDATIONS
Consolidate security visibility into an integrated platform.
Prioritize behavior-based detection over isolated alerts.
Define and version response playbooks as code.
Automate repetitive tasks while maintaining human control in critical incidents.
Integrate contextualized and action-oriented threat intelligence.

OT, IoT and cyber-physical systems: when the impact is in the real world

In 2026, cybersecurity definitively ceases to be a "screen-based" problem. The convergence between information technologies (IT), operational technologies (OT), and the exponential growth of the Internet of Things (IoT) moves digital risk to the very heart of the business: **production, energy, transport, logistics, healthcare, and essential services**.

The digitalization of industrial processes, massive sensorization, and remote connectivity have delivered enormous benefits in efficiency and control, but they have also opened an attack surface that, for years, was isolated or protected by its own complexity. In 2026, that barrier has disappeared.

IT/OT convergence as a new critical point

Historically, OT environments were designed to be stable, reliable, and long-lasting, not to withstand cyberattacks. Many industrial systems have life cycles of 15, 20, or even 30 years, use specific protocols, and do not allow frequent patching or abrupt changes.

Convergence with IT—driven by the need for centralized monitoring, remote maintenance, and data analytics—has exposed these environments to threats that were not contemplated in their original design. In 2026, this convergence is an irreversible reality.

The result is a scenario in which a cyberattack can cause:

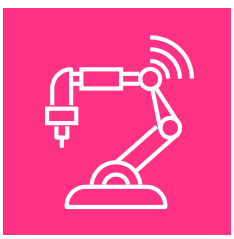
- Production shutdowns.
- Alterations in physical processes.
- Damage to equipment.
- Risks to people's safety.
- Interruptions to critical services.

An "invisible perimeter" that requires specific plans.

OT, IoT and cyber-physical systems: when the impact is in the real world

The rise of IoT and the expansion of the invisible perimeter

Added to this convergence is the growth of industrial and corporate IoT. Sensors, actuators, intelligent devices, and embedded systems are deployed massively to optimize operations, reduce costs, and improve visibility. However, many of these devices:



- Lack secure update mechanisms.
- Use default or weak credentials.
- Are not correctly inventoried.
- Connect to networks without proper segmentation.

In 2026, IoT becomes an **invisible perimeter**, difficult to manage and attractive to attackers as a lateral entry point toward more critical systems.

Targeted attacks and growing motivations

Attackers' interest in OT and IoT environments is not accidental. These systems represent high-impact targets, especially in strategic sectors such as energy, water, transport, industry, and healthcare. Beyond economic benefit, geopolitical, ideological, and sabotage motivations also come into play.

Attacks no longer aim solely at encryption or data theft. In many cases, the objective is to alter processes, degrade service quality, or generate operational uncertainty. In industrial environments, even small alterations can have significant consequences.

Visibility as the first major challenge

Many organizations discover their OT and IoT exposure only after an incident. The lack of an up-to-date inventory and visibility over assets, communications, and dependencies is one of the main risk factors.

Without visibility there is no control, and without control there is no security. Therefore, the first step in most cases is not the deployment of advanced tools, but a real understanding of the environment: which devices exist, how they communicate, and what impact their unavailability would have.

OT, IoT and cyber-physical systems: when the impact is in the real world

The difficulty of responding in cyber-physical environments

One of the major challenges of OT security is incident response. Unlike IT, where isolating a system or shutting down a server is usually feasible, in OT decisions must take into account physical safety, process continuity, and economic impact.

Stopping a plant, isolating a control system, or cutting a communication may be more dangerous than keeping it operational under monitoring. Therefore, OT response requires close coordination between security, operations, engineering, and business.

In 2026, the most mature organizations have **specific response plans for OT**, differentiated from traditional IT plans, and tested through realistic simulations.

Impact for organizations

In 2026, OT and IoT security becomes a strategic priority for any organization with physical processes or critical infrastructures. Risk is no longer theoretical or remote; it is tangible, operational, and potentially dangerous.

Organizations that address this challenge proactively will not only reduce risk, but also improve their ability to operate with confidence in highly digitalized environments. Those that ignore it will assume a level of exposure incompatible with business continuity.

KEY POINTS AND RECOMMENDATIONS
Obtain complete visibility of OT and IoT assets through continuous inventories.
Segment industrial networks and isolate critical environments through zones and conduits.
Implement specialized OT monitoring, adapted to industrial protocols.
Strictly control remote and third-party access.
Develop OT-specific response plans, coordinated with operations and engineering.

Digital identity and advanced fraud: the new perimeter under constant pressure

In 2026, digital identity is consolidated as the **main control point**, and at the same time as the **most exploited attack vector**. In an environment where users access from anywhere, to multiple cloud services, SaaS applications, and internal systems, identity becomes the true security perimeter.

This new scenario presents a clear paradox: the more technical infrastructures are reinforced, the more value credentials, sessions, and authentication mechanisms acquire. For attackers, compromising a legitimate identity is far more effective than attempting to exploit complex technical vulnerabilities.

Social engineering enters a new era

Social engineering has always been a powerful tool, but in 2026 it reaches an unprecedented level of sophistication thanks to the use of artificial intelligence. Voice and video deepfakes enable highly credible impersonations, capable of deceiving even experienced employees.

> The most evident corporate fraud threat in history.

Urgent calls from supposed executives, voice messages that perfectly imitate the tone and manner of speaking of a superior, or fake videos used as proof of legitimacy are now part of the usual arsenal of advanced fraud. These techniques do not only attack systems, but also people's trust and emotional pressure.

The result is a significant increase in corporate fraud, especially in financial processes, bank account changes, exceptional authorizations, and privileged access.

Attacks on multi-factor authentication

Over recent years, multi-factor authentication (MFA) has become established as a security standard. However, in 2026 attackers have learned to bypass and exploit its weaknesses.

Techniques such as MFA fatigue—bombarding users with requests until they accept by mistake—session hijacking, malware on endpoint devices, or social engineering to obtain temporary codes are becoming increasingly common.

Digital identity and advanced fraud: the new perimeter under constant pressure

This does not invalidate the use of MFA, but it does highlight that **not all factors are equal** and that authentication must evolve toward models that are more resistant to phishing and human manipulation.

Privileged identities: the most valuable target

Accounts with elevated privileges continue to be one of the most attractive targets for attackers. A single compromise can enable control of critical systems, the creation of persistence, and lateral movement with very little friction.

In 2026, many serious incidents do not begin with a sophisticated exploit, but with the misuse of valid credentials obtained through fraud, phishing, or poorly managed third-party access.

The management of privileged identities ceases to be a one-off project and becomes a continuous process of control, monitoring, and review.

The importance of context and behavior

In a world where credentials can be stolen, defense can no longer be based solely on "who you are," but also on **how you behave**. Behavioral anomaly detection becomes a key component for identifying fraudulent access that, from a technical point of view, appears legitimate.

Access outside working hours, from unusual locations, with atypical usage patterns, or with anomalous sequences of actions are signals that, when combined, make it possible to detect fraud in progress before it causes major damage.

Toward a resilient identity strategy

In 2026, protecting identity requires a comprehensive approach that combines technology, processes, and people. Implementing MFA is not enough; it is necessary to design secure access flows, limit privileges, continuously verify context, and train employees to recognize sophisticated fraud attempts.

Organizations that understand identity as a critical asset and manage its security proactively will be better prepared to face an environment where impersonation and deception are increasingly credible.

Digital identity and advanced fraud: the new perimeter under constant pressure

Impact on organizations

The impact of identity-based attacks is especially damaging because it breaks one of the fundamental pillars of security: trust. When an incident occurs using legitimate credentials, detection is usually slower and investigation more complex.

In addition, advanced fraud directly affects sensitive business areas such as finance, procurement, human resources, or customer service, extending the impact beyond the purely technological domain.

KEY POINTS AND RECOMMENDATIONS
Adopt phishing-resistant authentication for critical access.
Protect and continuously monitor privileged identities.
Implement context- and behavior-based access controls.
Establish out-of-band verification processes for sensitive operations.
Train employees specifically in the detection of advanced fraud and deepfakes.

Post-quantum cryptography: anticipating today the invisible challenge of tomorrow

At first glance, quantum computing may seem like a distant issue, reserved for research laboratories and major technology headlines. However, in 2026 a reality is consolidating that forces organizations to look beyond the short term: **the data protected today must remain confidential for ten or twenty years.**

This is the true core of the quantum risk. It is not that tomorrow a quantum computer capable of breaking all current encryption systems will exist, but that data stolen today can be stored and decrypted in the future. This strategy, known as "harvest now, decrypt later," is already part of the approach of certain advanced actors.

When time becomes a threat

For decades, classical cryptography has been one of the pillars of digital security. Algorithms such as RSA or ECC have protected communications, identities, transactions, and corporate secrets. However, their security is based on mathematical problems that, in a mature quantum computing scenario, could be solved efficiently.

In 2026, many organizations begin to ask themselves:

What happens to information that must remain confidential for long periods? Strategic contracts, intellectual property, personal data, medical records, industrial secrets, or government information do not lose value over time; on the contrary, in many cases they retain it or even increase it.

This turns post-quantum cryptography into a **long-term risk management issue**, not one of immediate reaction.

A long-term threat that requires planning now.

Post-quantum cryptography: anticipating today the invisible challenge of tomorrow

The hidden complexity of the cryptographic transition

One of the greatest challenges of this trend is its complexity. Cryptography is not an isolated component that can be easily replaced. It is integrated across multiple layers of the architecture: applications, operating systems, network protocols, devices, certificates, public key infrastructures (PKI), and third-party services.

In many cases, organizations do not have a clear view of:

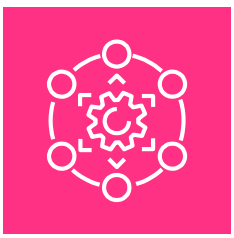
- Which algorithms they actually use.
- Where keys are stored and managed.
- Which systems depend on them.
- Which vendors or legacy applications do not support rapid changes.

In 2026, the first major challenge is not migration, but **understanding the real exposure**.

First steps toward a post-quantum approach

Although the complete transition will take years, in 2026 the first pragmatic strategies begin to take shape. It is not about replacing everything immediately, but about planning and preparing the ground.

Many organizations begin by:



- Conducting cryptographic inventories to identify dependencies.
- Classifying information according to its lifespan and criticality.
- Testing standardized post-quantum algorithms in controlled environments.
- Adopting hybrid encryption approaches, combining classical and post-quantum algorithms.

This gradual approach makes it possible to reduce risk without introducing unnecessary instability into systems.

Post-quantum cryptography: anticipating today the invisible challenge of tomorrow

Regulatory and trust implications

As post-quantum cryptography gains relevance, it also does so from a regulatory and trust perspective. In certain sectors, the ability to demonstrate that sensitive information is protected against future risks may become a differentiating factor.

Clients, partners, and regulators begin to value not only current security, but also a **long-term vision**. In this sense, anticipating quantum risk strengthens the perception of maturity and responsibility in security management.

Impact on organizations

In 2026, post-quantum cryptography is not an operational urgency, but it is an emerging strategic priority. Organizations that ignore this debate may find themselves, in a few years, with technical debt that is difficult to resolve under pressure.

On the contrary, those that start now to understand their exposure, organize their cryptographic architecture, and plan the transition will be better positioned to adapt when the change becomes inevitable.

KEY POINTS AND RECOMMENDATIONS
Identify the information that must remain confidential in the long term.
Carry out an inventory of cryptographic algorithms, keys, and dependencies.
Assess the impact of quantum risk on critical systems and suppliers.
Initiate controlled tests with post-quantum and hybrid algorithms.
Incorporate post-quantum cryptography into the medium- and long-term security roadmap.

Mature Zero Trust: from aspirational concept to real architecture

For years, the Zero Trust model has been cited as the reference approach for modern security. However, in many organizations it has remained a theoretical concept or a set of partial initiatives. In 2026, this situation changes: **Zero Trust ceases to be an aspiration and becomes a real operational architecture**, applied consistently in hybrid, distributed, and highly dynamic environments.

The reason is simple. The traditional perimeter no longer exists. Users working from anywhere, cloud applications, SaaS services, workloads across multiple clouds, third-party access, and unmanaged devices have made the "inside" versus "outside" model unviable. In this context, trusting by default is an unsustainable risk.

The fundamental principle: never trust, always verify

Zero Trust is based on a clear premise: no user, device, or system should be considered trustworthy by default, regardless of location. Every access must be evaluated based on identity, context, and risk.

> Identity management, not only human, under continuous evaluation.

In 2026, this principle translates into continuous and dynamic controls. Authenticating at the start of a session is not enough. The level of trust is constantly evaluated, taking into account factors such as the device used, location, behavior, resource sensitivity, and the security posture of the environment.

This approach drastically reduces the impact of initial compromises. Even if an attacker gains access, their ability to move is limited from the very beginning.

Identity as the central axis of the architecture

In a mature Zero Trust model, identity becomes the primary control point. Users, services, applications, and workloads have their own identities, managed and protected in a consistent manner.

Mature Zero Trust: from aspirational concept to real architecture

Access is no longer granted based on the network, but on the **principle of least privilege**: each identity accesses only what it needs, for the necessary time, and under the appropriate conditions. This approach is especially relevant in cloud and microservices environments, where east–west communications are constant.

In 2026, the most advanced organizations manage identities not only for humans, but also for machines, APIs, and automated processes, expanding the scope of control.

Microsegmentation: limiting the impact of compromise

Microsegmentation is one of the technical pillars of mature Zero Trust. Instead of large network segments with broad levels of implicit trust, **fine-grained logical segments** are created, adapted to applications, services, and specific workflows.

This makes it possible to isolate critical assets and limit lateral movement even within the same network. In practice, an incident is contained within a reduced scope, significantly reducing its impact.

In 2026, microsegmentation is applied both in on-premise environments and in cloud, containers, and OT/IoT platforms, adapting to the specific characteristics of each environment.

Risk-based adaptive Access

One of the elements that differentiates mature Zero Trust from a superficial implementation is the ability to **adapt access based on risk**. Not all accesses require the same level of control, and not all contexts present the same risk.

Mature Zero Trust: from aspirational concept to real architecture

Based on variables such as user behavior, resource criticality, or active threat signals, the system may:

- Require additional authentication.
- Limit functionality.
- Force revalidation.
- Temporarily block access.

This approach makes it possible to balance security and user experience, avoiding unnecessary controls without giving up protection.

Zero Trust as a process, not a product

One of the most common mistakes is treating Zero Trust as a specific technological solution. In 2026, it becomes clear that Zero Trust is an architectural model and a continuous process, not a product that can be bought and installed. Its adoption requires:

- Redesigning access flows.
- Reviewing historical permissions and privileges.
- Integrating multiple capabilities: identity, endpoints, network, applications, monitoring.
- Changing the organizational mindset around access and trust.

Therefore, implementation is usually progressive, prioritizing critical assets and high-impact use cases.

Mature Zero Trust: from aspirational concept to real architecture

Impact on organizations

The adoption of mature Zero Trust enables organizations to operate more securely in complex and distributed environments. It reduces the impact of incidents, improves visibility, and facilitates regulatory compliance.

In addition, it provides a solid foundation for other key initiatives in 2026, such as identity protection, cloud security, intelligent SOC operations, and secure third-party management.

KEY POINTS AND RECOMMENDATIONS
Place identity at the center of the security architecture.
Apply the principle of least privilege systematically.
Implement microsegmentation in critical environments.
Adopt risk-based adaptive access controls.
Address Zero Trust as a progressive and cross-cutting program, not as an isolated project.

Regulation, reporting, and cyber resilience: security becomes a business KPI

In 2026, cybersecurity stops being measured solely in technical terms and becomes a **direct indicator of business health and resilience**. Regulatory pressure, increasing media exposure of incidents, and interdependence between organizations require a shift from statements of intent to the **objective demonstration of capabilities**.

The question is no longer whether an organization "cares" about security, but whether it **can prove that it is prepared to manage a real incident**.

From formal compliance to demonstrable resilience

For years, the regulatory approach has focused on compliance with minimum controls and the existence of documented policies. In 2026, this approach proves insufficient. Regulators, customers, and partners demand practical evidence: detection times, response capabilities, tested plans, and decision traceability.

> The leap from the technical area to the executive committee.

Cyber resilience becomes a central concept. It is not only about preventing incidents, but about **absorbing the impact, maintaining essential services, and restoring operations within acceptable timeframes**. This capability must be integrated into overall corporate risk management.

Incident reporting: speed, clarity, and coordination

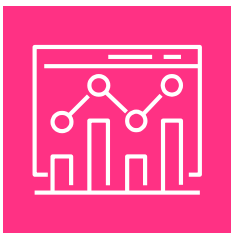
One of the areas where requirements intensify the most is incident reporting. In 2026, many organizations are required to notify relevant incidents within very tight deadlines, often hours or just a few days. This implies:

- The ability to detect and classify incidents quickly.
- Coordination between technical, legal, communications, and executive teams.
- Clear and coherent messaging, even in contexts of high uncertainty.

Improvisation is no longer an option. Organizations must have clear processes, defined roles, and pre-agreed decision flows.

Regulation, reporting, and cyber resilience: security becomes a business KPI

The supply chain under regulatory scrutiny



Security is no longer assessed in isolation. In 2026, regulators and major customers focus on the digital supply chain. Vendors, technology partners, and third parties with access to systems or data become an extension of the organization's own risk.

This requires organizations to:

- Assess the maturity level of their suppliers.
- Require minimum security evidence.
- Establish clear contractual clauses.
- Continuously monitor third-party risk.

An incident involving a critical supplier can generate legal and reputational consequences as severe as an internal incident.

Cybersecurity reaches the executive committee

Another significant change in 2026 is the role of senior management. Cybersecurity stops being an issue delegated exclusively to technical areas and becomes part of the agenda of the executive committee and the board.

This translates into:

- Greater executive oversight.
- Demand for business-understandable metrics.
- Integration of cybersecurity into corporate risk management.

For this dialogue to be effective, it is essential to translate technical risks into business impacts: service disruption, financial loss, reputational damage, or regulatory non-compliance.

Regulation, reporting, and cyber resilience: security becomes a business KPI

KPIs for cyber resilience: measuring what really matters

In 2026, more mature organizations use clear indicators to measure their level of resilience. Beyond the number of incidents or vulnerabilities, they prioritize:

- Mean Time to Detect (MTTD), respond, and recover (MTTR).
- Maximum tolerable impact.
- Percentage of critical assets covered.
- Results of drills and crisis exercises.

These KPIs make it possible to objectively assess the organization's ability to withstand and recover from an attack.

Impact on organizations

The increase in regulatory and reporting requirements forces the professionalization of cybersecurity management. Organizations that are not prepared will face sanctions, loss of trust, and greater impact in the event of an incident.

Conversely, those that integrate digital resilience into their corporate governance will gain credibility, improve their response capability, and strengthen their position with clients and partners.

KEY POINTS AND RECOMMENDATIONS
Integrate cybersecurity into the overall management of business risk.
Define clear incident reporting and notification processes.
Establish cyber resilience metrics that are understandable for senior management.
Continuously assess and manage supply chain risk.
Conduct periodic drills involving both technical and executive teams.

Talent and security culture: the human factor in the age of automation

In a context dominated by artificial intelligence, automation, and increasingly advanced technologies, it might seem that the human factor is losing relevance. However, in 2026 the opposite is true: **people become the decisive element that makes the difference between a resilient organization and a vulnerable one.**

Technology is essential, but not sufficient. Critical decisions, crisis management, context interpretation, and adaptability still depend on human judgment. The cybersecurity of the future is built on well-trained teams, clear processes, and a shared culture.

The transformation of the cybersecurity professional's role

The shortage of specialized talent remains a reality in 2026, but the nature of the work is changing. Automation and artificial intelligence take over repetitive, low-value tasks, freeing time for higher-impact activities. The cybersecurity professional evolves:

People will play a cross-cutting role in security.

- From reactive operator to advanced analyst.
- From alert manager to incident investigator.
- From isolated technical specialist to business interlocutor.

New hybrid profiles emerge, combining cybersecurity with knowledge of data, OT, cloud, or business processes. This cross-functionality is key to understanding the real impact of incidents and correctly prioritizing actions.

AI-augmented teams, not replaced by it

In 2026, AI does not replace security teams; it amplifies them. Analysis copilots, response automation, and investigation assistants enable smaller teams to manage more complex environments.

Talent and security culture: the human factor in the age of automation

However, this dependence on technology requires a high level of maturity. Blindly trusting automated systems can create a false sense of control. Human oversight, decision validation, and the ability to intervene manually remain essential.

The key lies in designing an effective collaboration model between people and technology.

Security culture as a shared responsibility

One of the clearest lessons from recent years is that cybersecurity cannot rest exclusively within a single department. In 2026, the most resilient organizations are those where **security is part of the corporate culture**.

This implies that:

- Employees understand the risks and their role in protecting the organization.
- Business processes incorporate security controls from the design stage.
- Senior management leads by example and supports security initiatives.

Awareness evolves from generic training toward programs tailored to specific roles, with practical and relevant content for each function.

Continuous training and practical learning

The pace of change in threats makes a one-off training approach unviable. In 2026, cybersecurity training is a continuous process, integrated into the life of the organization.

Phishing simulations, incident response exercises, crisis tests, and joint training between technical and executive teams become common practices. These exercises not only improve technical preparedness but also strengthen coordination and trust between teams.

Talent and security culture: the human factor in the age of automation

The role of senior leadership in building a security culture

Leadership involvement is a decisive factor. When cybersecurity is understood as a **strategic priority**, teams gain the backing they need to make difficult decisions in moments of crisis.

By 2026, leaders who truly understand the real-world impact of cyber incidents—and who actively participate in simulations and risk reviews—play a critical role in building more resilient organizations. Security leadership is no longer symbolic; it is visible, hands-on, and accountable.

Impact on organizations

Investing in talent and security culture is not a cost—it is an **investment in resilience**. Organizations with well-prepared, motivated, and aligned teams respond more effectively to incidents, make fewer mistakes, and recover faster.

On the other hand, lack of training, excessive staff turnover, or the absence of a strong security culture can dramatically amplify the impact of any incident—no matter how advanced the deployed technology may be.

KEY POINTS AND RECOMMENDATIONS
Commit to continuous training, tailored to specific roles and responsibilities.
Develop hybrid profiles that bridge cybersecurity expertise and business understanding.
Use AI to augment teams, not to replace them.
Actively involve senior leadership in crisis management and simulation exercises.ght.
Implicar a la alta dirección en la gestión y simulación de escenarios de crisis.

Cybersecurity 2026: Conclusion

In 2026, cybersecurity is more than a technical function: it is a **strategic pillar** that underpins organizational continuity and growth. Security is no longer just a barrier against threats, but a **key enabler of trust, innovation, and resilience**. Organizations that understand this shift and prepare accordingly will not only mitigate risk, but also position themselves as leaders in an increasingly complex and competitive digital environment.

As technologies evolve and attackers become more sophisticated, the only way to stay ahead is through **continuous and proactive adaptation**. The adoption of artificial intelligence, the implementation of Zero Trust, the strengthening of organizational resilience, and the promotion of a strong, transversal security culture are the foundations on which the future of any organization must be built.

At Ayesa, we understand that cybersecurity is not an isolated project, but an ongoing process that must be embedded in the organization's DNA. That is why we do more than deliver cutting-edge technology: we **support our clients in the digital transformation of their security strategy**, ensuring that every step is aligned with business objectives.

We are at a stage where digital risks are not only inevitable, but also **predictable and manageable**. Preparing today for tomorrow's challenges is the true differentiator between organizations that fall behind and those that move forward with confidence toward a more secure, resilient, and innovative future.

Our mission is to be the **trusted partner** that guides our clients along this journey, bringing the experience, knowledge, and technological capabilities needed to ensure that every organization can grow and thrive securely.

Author

Álvaro Fraile
Global Cybersecurity Services Director

Our 360º Cybersecurity Services

INTEGRATION OF IT/OT CYBERSECURITY SOLUTIONS

CiD360

GOVERNANCE, RISK & COMPLIANCE	OFFENSIVE SECURITY SERVICES	SOC MANAGED SECURITY SERVICES	INDUSTRIAL CYBERSECURITY	CYBERSECURITY TRAINING SERVICES
Consulting for adaptation and implementation	Enhancing cyber resilience	Managed Security Services (SOC)	Protection of Industrial Control Systems (ICS)	Tailored specialized training

SDLC-CYBERSEC (SECURE SOFTWARE DEVELOPMENT)

Founded in 1966, Ayesa is a global technology and engineering services company, with 13,200 employees and a direct presence in 24 countries across Europe, America, Africa, Asia, and Oceania. Led by José Luis Manzanares, it exceeds €717 million in revenue, consolidating its position as one of the leading consulting and IT services companies in the Spanish market.

It offers a broad range of advanced Digital Transformation solutions (projects with disruptive technologies and solutions) and core service lines (traditional IT services) to improve competitiveness across all sectors of activity through the application of technology and knowledge.

Industry 4.0, Analytics, Cloud, Hybrid IT, Cybersecurity, Quantum Computing, Blockchain, IoT, AI, RPA, Bimodal IT, Mobility, and Digital Experience are some of the technologies it makes available to its clients to face the new digital era.

It is also among the leading engineering firms, working to build a more efficient and fair world by applying cutting-edge engineering and technology in an integrated manner. It helps companies, institutions, and organizations become what they aspire to be. It works in the space between now and the future, applying the best talent and the most advanced technology.