Eleven Paths

Keys to Implementing a 360 Corporate Digital Identity

A challenge not to be delayed

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

Executive Summary

In recent years, in parallel with the accelerated processes of corporate digital transformation, a major issue has been growing steadily in the fundamental structures of all organisations.

We are talking about the drawbacks arising from **inefficient identity access management** which, on the one hand, hinder productivity, and business expansion and, on the other hand, impact significantly on the security of the organisation.

Factors causing identity management issues:

- Non-planned technological evolution based on partial and isolated solutions.
- The inorganic corporate growth and the delay in the integration of identity directories.
- Lack of standard lifecycle management processes and a policy of roles and authorisations.
- Delay in implementing corrective measures as well as a corporate identity strategy.

This paper begins with a description of the issues resulting from inefficient corporate identity management. Then, a model of identity governance based on Gartner's CARTA methodology is detailed. Finally, it provides the characteristics that a comprehensive identity access management solution must have.

01

Challenges in corporate Identity Management

01. Productivity and Business

- **Delays** in the provision of new employees.
- Human resources or IT teams engaged in **repetitive and low-value tasks.**
- Inconsistencies in the organisational chart that imply **delays in the authorisation of access to corporate resources.**
- **Neglect** of significant identity and strategic vision tasks.
- High number of **orphan accounts** resulting in unnecessary licensing costs.
- **Risk of fraud** due to development or testing credentials that are not properly safeguarded.

02. Security

- **Excessive and unnecessary accumulation of privileges** caused by internal staff role changes.
- **Vulnerable privileged access** credentials as passwords are not properly safeguarded.
- **Inability to audit** privileged access.
- There is no **automated offboarding process**, which leads to a significant risk of confidential information theft or sabotage.
- Failure to implement a **strong password policy** facilitates the theft of credentials.
- Theft of **credentials from bots or IoT devices** not included within the identity governance plan.

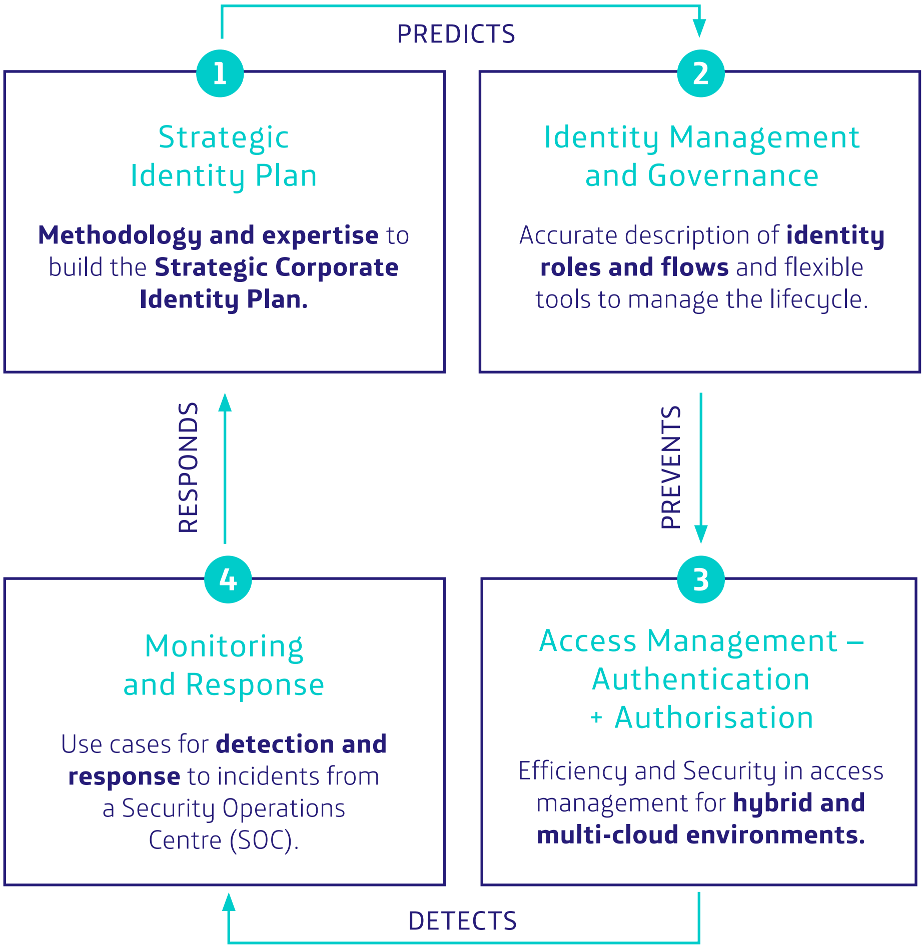
03. Regulatory Risks

- **Access certification to corporate resources** is a very demanding task or impossible to perform.
- Comply with **privacy and data protection regulations**, such as GDPR and LGDP, during access and storage of personal information of employees, collaborators and end users.
- Impossibility of **preventing and detecting leaks of information** from end users.

02 CARTA model for Identity Management

Telefónica proposes an identity management model based on the principles of CARTA (Continuous Adaptive Risk and Trust Assessment)*.

Identity management is a dynamic task that must be manageable enough to extend to a vague, or even non-existent, security perimeter. According to this model, security is based on the principle of zero trust. Therefore, access to resources is subject to contextual parameters (such as the place, the connection mechanism, the device, and the user's behaviour) and based on adaptive processes of continuous authentication coupled with risk engines. Finally, this CARTA model requires permanent monitoring of anomalies to detect potential leaks.



1 Strategic Identity Plan

Methodology and expertise to build the **Strategic Corporate Identity Plan.**

2 Identity Management and Governance

Accurate description of **identity roles and flows** and flexible tools to manage the lifecycle.

3 Access Management – Authentication + Authorisation

Efficiency and Security in access management for **hybrid and multi-cloud environments.**

4 Monitoring and Response

Use cases for **detection and response** to incidents from a Security Operations Centre (SOC).

* In 2017, Gartner introduced a new strategic approach to information security: Continuous Adaptive Risk and Trust Assessment (CARTA). This new principle embraces the current reality of securing a world where digital capabilities of businesses are accessible from anywhere, by any device, and where attackers evolve as quickly as protection strategies.

03 Technological pillars of Identity and Access Management

A comprehensive identity and access management solution requires addressing four categories of use cases by means of an ecosystem of leading technologies, enabling agile deployments and broad integration capabilities.

Identity Governance and Administration

Access Management

Customer Identity and Access Management

Privileged Account Management

A gradual deployment of technologies is required, according to the Strategic Identity Plan, and ideally in full or partial SaaS mode as long as the organisational requirements allow it.

Three factors will be essential when choosing these technologies:

- **Advanced capabilities** in biometric authentication, identity analysis and detection of abnormal behaviour.
- **Flexibility** to make configurations in a fast, intuitive and replicable way.
- **Availability of connectors** to SaaS services or applications, public clouds and legacy applications to easily deploy complex use cases.

Identity use cases

There is a consensus within the market to group identity and access management use cases into the following four technology categories.

Identity Governance and Administration (IGA)

- **Identity consolidation** (synchronisation/ federation).
- Centralised **identity repository.**
- Automated **identity supply.**
- **Periodical reviews.**
- **Access certification.**
- **Management of employees offboarding.**
- **Role Based Access Control** (RBAC).
- Identification **of orphan accounts.**
- Management of **collaborative users**
- **Automated approval** flows.

Access Management

- **Multi-factor authentication.**
- Centralised **authentication.**
- Unified **access portal.**
- **Single Sign-on** (cloud, on-premise, DevOps).
- Continuous **passwordless authentication.**
- **Access management** policies.
- **Zero-Trust Network Access.**

Customer Identity and Access Management

- **Self-service** functions.
- **Single Sign-on** for customers.
- **Social Identity** (BYOI).
- **Consent and privacy** management.
- **Digital onboarding.**
- **Analysis** and reports.
- Progressive **profile registration.**
- **Integration with CRM.**

Privileged Account Management (PAM)

- **Password Vault.**
- Automatic generation of **passwords.**
- Detection of **abnormal account use.**
- **Monitoring** of sessions.
- **Blocking** of sessions.
- **Audit** of privileged accounts.
- Identification of **privileged accounts.**

04 Keys to implementing your strategic plan

01. Analysis and Design

02. Deployment and Configuration

03. Administration and Monitoring

01. Analysis and Design

Expert Consulting helps companies to build their Strategic Identity Plan.

Successful methodology for developing an **identity management and governance model.**

Collaboration between different departments to carry out **coordination tasks** between teams.

Information gathering through interviews with key actors.

Alignment with **corporate security policies.**

Risk and priority assessment.

Definition and monitoring of indicators (KPIs) to ensure successful implementation.

Design of **processes and roles** within the organization.

Coordination with business teams for **end-user identity management.**

Architecture design and technology selection.

02. Deployment and Configuration

Thanks to teams of certified technologists, you will be able to tackle the implementation of those technologies selected in your strategic plan.

Deploy technology in the ecosystem most appropriate for your organisation, **public cloud, private cloud or on-premise.**

Configure or develop **connectors** to your services and applications.

Implement the **process and role model.**

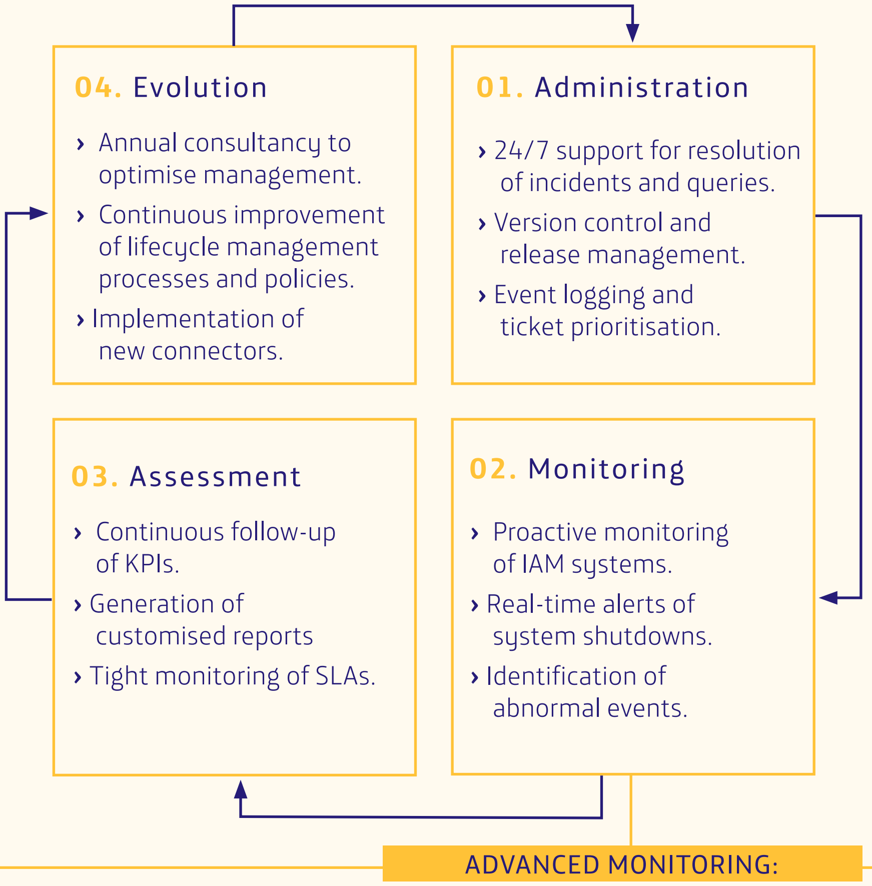
Manage the project using agile, short iteration methodologies with realistic objectives.

Design a custom **training and certification plan** for each department.

Ensure **cross-functional knowledge.**

03. Administration and Monitoring

Integrate identity and access management into your corporate security management model and manage it from your SOC.



04. Evolution

- Annual consultancy to optimise management.
- Continuous improvement of lifecycle management processes and policies.
- Implementation of new connectors.

01. Administration

- 24/7 support for resolution of incidents and queries.
- Version control and release management.
- Event logging and ticket prioritisation.

03. Assessment

- Continuous follow-up of KPIs.
- Generation of customised reports
- Tight monitoring of SLAs.

02. Monitoring

- Proactive monitoring of IAM systems.
- Real-time alerts of system shutdowns.
- Identification of abnormal events.

ADVANCED MONITORING:

Prioritise alerts and organize automated remediation actions based on predefined workflows and policies.

Review user risk activity such as failed logins or new authentication factors to detect threats before they occur.

Automatic enrichment of security alerts including identity context information.

Identify anomalies based on the development of entity behaviour patterns:

- Unusual login patterns.
- Sudden, unusual or rare activity involving files, systems or processes.
- User impersonation for accessing files and drives.
- Brute force access.
- Internal identification.
- Low and slow user data leaks to external or connected storage.
- Bot activity.
- Machine performance-related issues.
- Misconfigured service accounts.

Identity and access management is a major challenge that requires a technological foundation and expert knowledge, as well as strategic but realistic leadership.

At ElevenPaths, we know these issues and have adapted our solutions to this complex scenario of diffuse ecosystems. Our solutions combine cutting-edge technology with certified and highly experienced professional services.

Let us help you to face this challenge and build with you the solution tailored to your organisation to make identity management your competitive advantage.

About ElevenPaths

At ElevenPaths, Telefónica's Cybersecurity Company, we believe in the idea of challenging the current state of security, an attribute that must always be present in technology. We are always redefining the relationship between security and people, with the aim of creating innovative security products which can transform the concept of security, thus keeping us one step ahead of attackers, who are increasingly present in our digital life.

We combine the freshness and energy of a start-up with the power, experience, and robustness of Telefónica to provide solutions that enable prevention, detection, and response against everyday threats in our digital world.

We build strategic alliances to provide a strengthened security to our clients. Moreover, we work jointly with organizations and entities such as the European Commission, Cyber Threat Alliance, ECSO, EuroPol, Incibe, and the Organization of American States (OAS).

More information:
elevenpaths.com | @ElevenPaths | blog.elevenpaths