MICROSOFT ENTRA PROOF OF CONCEPT

IDENTITY FOUNDATION

MOVING BUSINESS THROUGH TECHNOLOGY

ENTRA SUITE SERVICES

PROOF OF CONCEPT

Designed to demonstrate the feasibility and potential benefits of Microsoft Entra Suite within a controlled environment.

IMPLEMENTATION SERVICES

Focuses on the full-scale deployment of Microsoft Entra Suite across the organization

IDENTITY FOUNDATION	IDENTITY GOVERNANCE	ADVANCED IDENTITY	IDENTITY GOVERNANCE AND REMOTE ACCESS	PRIVATE ACCESS
› Microsoft Entra ID P2	› Microsoft Entra ID Governane	› Microsoft Entra Suite › MDI	› Microsoft Entra Suite	› Microsoft Entra Private Access

Mod. IT 09 02

IDENTITY FOUNDATION PROOF OF CONCEPT

Microsoft Entra emphasizes identity and access management, ensuring that user access and privileges are managed efficiently and securely.

This advanced identity tool focuses on applications, networks, identities, and infrastructures, providing a seamless user authentication experience.

Within the scope of this engagement, we include the activation and configuration of Microsoft Entra **for a limited number of users**, which will achieve the following objectives:

› Provisioning of a central repository with all identities of the client to enable effective access management to the organization's applications, including both cloud and on-premises applications.

› Identity governance that will provide the client with governance policies, such as role-based access management, enforcement of access attestation policies for applications, access segregation, and ensuring that the right people have access to the designated applications.

› Availability of automated workflows for access assignment based on predefined rules.

Mod. IT.09.02

IDENTITY FOUNDATION PROOF OF CONCEPT - SCOPE

IDENTITY FOUNDATION	ACCESS GOVERNANCE

IDENTITY FOUNDATION

› **HR Integration**:
  › API Inbound HR Integration;
    › CSV Inbound provisioning mapping
    › Implement workflows from HR employees (account generation)
    › Automate HR Synchronization with Entra ID and Active Directory
  › Other Users Types Integration - External Users Provisioning;
  › User Lifecycle Governance- CRUD Policies implementation (internal and external users)

› **Users Attestation - Identity advanced Security**:
  › Privileged identity management (PIM)
  › Create Risk-based Conditional Access policies (sign-in risk, user risk)
  › Create all device and application filters for Conditional Access
  › Identify Risky accounts and vulnerabilities

› **Base Accesses Management**:
  › Users License activation (from base kit of accesses);
  › Base Security groups initial accesses activation.

ACCESS GOVERNANCE

› **Entitlement Management**:
  › **2 Applications Access Manual Profiles** definition and creation
  › Administration Roles Profiles definition and creation
  › Catalogues creation and configuration

› **Self Service Access Governance**:
  › Application Delegation Governance;

› **Enterprise App Registration**
  › Application Governance Policies Creation & Applications provisioning;
  › **Non-AD connected applications** - Up to 1 on premises applications integration with automate provisioning and accesses processes;
  › **Non-Entra ID connected applications**: Up to 1 application integration with SCIM integration implementation with automate provisioning policies creation and accesses provisioning.

Mod. IT_09.02

ARMISGROUP.COM

PT Porto, Lisbon | **BR** São Paulo, São José dos Campos | **UAE** Dubai | **USA** Miami, New York