**Política de Gestão de Identidades e Acessos (IAM)  
Ambiente Híbrido Microsoft AD**

Subtítulo: Documento Base de Referência para Controlo de Acessos

Data: [preencher]  
Versão: [preencher]  
Responsável: [preencher]

# Índice

1. Objetivos

2. Princípios da Política

3. Matriz de Funções RBAC

4. Matriz de Segregação de Funções (SoD)

5. Salvaguardas Adicionais

# 1. Objetivos

- Garantir o princípio do menor privilégio em ambientes híbridos (AD On-Premises + Azure AD + Microsoft 365).

- Padronizar o controlo de acesso baseado em funções (RBAC).

- Assegurar segregação de funções (SoD) para reduzir riscos internos.

- Implementar auditoria e monitorização em conformidade com normas (SOX, ISO 27001, RGPD, etc.).

# 2. Princípios da Política

- Menor privilégio – cada utilizador tem apenas os acessos mínimos necessários.

- Acesso baseado em função (RBAC) – permissões atribuídas a funções, nunca diretamente a indivíduos.

- Segregação de funções (SoD) – impedir que uma única função tenha controlo total.

- Acesso condicional – MFA, conformidade de dispositivo e restrições geográficas obrigatórias para funções privilegiadas.

- Acesso Just-in-Time (JIT) – ativação temporária de privilégios via Azure AD PIM.

- Auditoria contínua – todos os acessos administrativos devem ser registados e revistos periodicamente.

# 3. Matriz de Funções RBAC

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Função | Âmbito | Permissões | Perfil Típico | Notas |
| Administrador Global (Azure AD) | Tenant Azure AD, M365 | Controlo total (serviços, subscrições, faturação) | 2–4 admins séniores de identidade | Conta “break-glass” com MFA obrigatório e uso apenas emergencial |
| Administrador de Funções Privilegiadas | Azure AD | Gerir atribuições de funções e PIM | Equipa de IAM | Não deve acumular com Global Admin |
| Administrador do Azure AD | Azure AD | Gestão de utilizadores, grupos, licenciamento, acesso condicional | Administradores de identidade | Separado do Global Admin |
| Administrador de Segurança | Azure AD, M365 | Definir políticas e responder a alertas | SecOps / SOC | Trabalha com equipa de cibersegurança |
| Administrador de Conformidade / Proteção de Informação | M365 Compliance Center | eDiscovery, auditorias, políticas de retenção | Equipa de Compliance/Legal | Isolado do Global Admin |
| Administrador de Exchange | Exchange Online | Gestão de caixas de correio, DLs, regras de transporte | Equipa de Mensageria | Limitado ao Exchange |
| Administrador de Teams | Microsoft Teams | Políticas de Teams, reuniões, gestão de utilizadores | Equipa de Colaboração | Apenas Teams |
| Administrador de SharePoint | SharePoint Online | Gestão de coleções de sites, partilhas externas | Equipa de Colaboração | Apenas SharePoint |
| Administrador de Intune | Endpoint Manager | Gestão MDM/MAM, conformidade de dispositivos, apps | Equipa de Endpoints | Essencial para Zero Trust |
| Administrador de AD (On-Premises) | AD DS, DNS, GPO | Gestão de controladores de domínio, OU, GPOs | Equipa de Infraestrutura | Seguir modelo de “Tier 0 Admin” |
| Administrador Delegado de AD (OU/Escopo) | AD On-Premises | Gestão delegada de OU, utilizadores, grupos | IT regional / Service Desk avançado | Evita privilégios excessivos |
| Administrador de Helpdesk | Azure AD / AD On-Premises | Reset de passwords, desbloqueio de contas, licenciamento básico | Service Desk | Função personalizada e limitada |
| Administrador de Aplicações | Azure AD | Registar e gerir apps empresariais | Equipa de Integração | Não necessita de Global Admin |
| Administrador de Rede | Infra Híbrida | VPN, firewall, regras de acesso condicional | Equipa de Rede | Apenas infra |
| Administrador de Auditoria (Read-Only) | Azure AD + M365 + AD | Apenas leitura em logs, auditorias, relatórios | Auditores internos / Compliance | Nunca pode alterar dados |

# 4. Matriz de Segregação de Funções (SoD)

|  |  |
| --- | --- |
| Funções em Conflito | Motivo |
| Administrador Global + Administrador de Segurança | Impede ocultação de atividades maliciosas |
| Administrador de AD + Administrador de Auditoria | Impede manipulação de registos |
| Administrador de Exchange + Administrador de Conformidade | Evita adulteração em investigações |
| Administrador de Intune + Administrador de Segurança | Evita bypass de políticas de dispositivos |
| Administrador de Aplicações + Administrador de Funções Privilegiadas | Evita escalamento de privilégios por apps |

# 5. Salvaguardas Adicionais

- Uso obrigatório de PAW (Privileged Access Workstations) para todas as contas privilegiadas.

- MFA + Acesso Condicional aplicado a todas as funções administrativas.

- Monitorização contínua via Defender for Identity e Azure AD Identity Protection.

- Implementação de JEA (Just Enough Administration) em AD On-Premises.

- Revisões trimestrais de acessos com Azure AD Access Reviews.