5

HACKERS DO BEM_

Módulo 05

Gerenciamento de Identidades e Contas

Aula 01

Tipos de Contas e Identidades _

Softex SENAI RNP MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Aula 01

Tipos de Contas e Identidades

Tipos de Contas e Identidades

TIPOS DE CONTAS E IDENTIDADES

- Fundamental para a implementação de um sistema robusto de gestão de identidade e acesso.
- Garante a proteção dos ativos de informação e a conformidade com os requisitos regulatórios aplicáveis.

Aula 01

Tipos de Contas e Identidades

Controles de Gerenciamento de Identidade

CONTROLES DE GERENCIAMENTO DE IDENTIDADE

- Rede Privada:
  - A conta do usuário representa sua identidade digital;
  - O Administrador de rede gerencia o servidor que hospeda as contas visando manter sua integridade;
- Rede Pública:
  - O usuário pode fazer uso de identificação criptográfica.
  - Maior segurança ao processo de autenticação e autorização.

CERTIFICADOS E SMART CAR

- Certificados digitais são documentos eletrônicos emitidos pelas Autoridades Certificadoras (ACs).
- São confiáveis dentro de uma infraestrutura de chaves públicas (PKI).
- Vinculam uma chave pública a uma identidade específica (pessoa, organização ou dispositivo) devidamente identificada e validada.
- O armazenamento pode ser em um cartão inteligente ou em uma chave USB.

Fonte: Wm Certificadora.
Disponível em: https://wmcertificadora.com.br/categoria-produto/acessorios/
Acesso em: 18 mar. 2024.

Fonte: Medium.
Disponível em: <https://medium.com/@saurav.agg19/session-vs-token-based-authentication-5bc3b5942cc1>
Acesso em: 18 mar. 2024.

TOKENS

- Em um sistema de autenticação único, o usuário autentica-se em um provedor de identidade (IdP).
- O usuário recebe um token criptográfico para acesso às aplicações compatíveis;
- O uso de tokens pode trazer risco de segurança: um ator malicioso pode reproduzir o token, obtendo acesso não autorizado às aplicações.

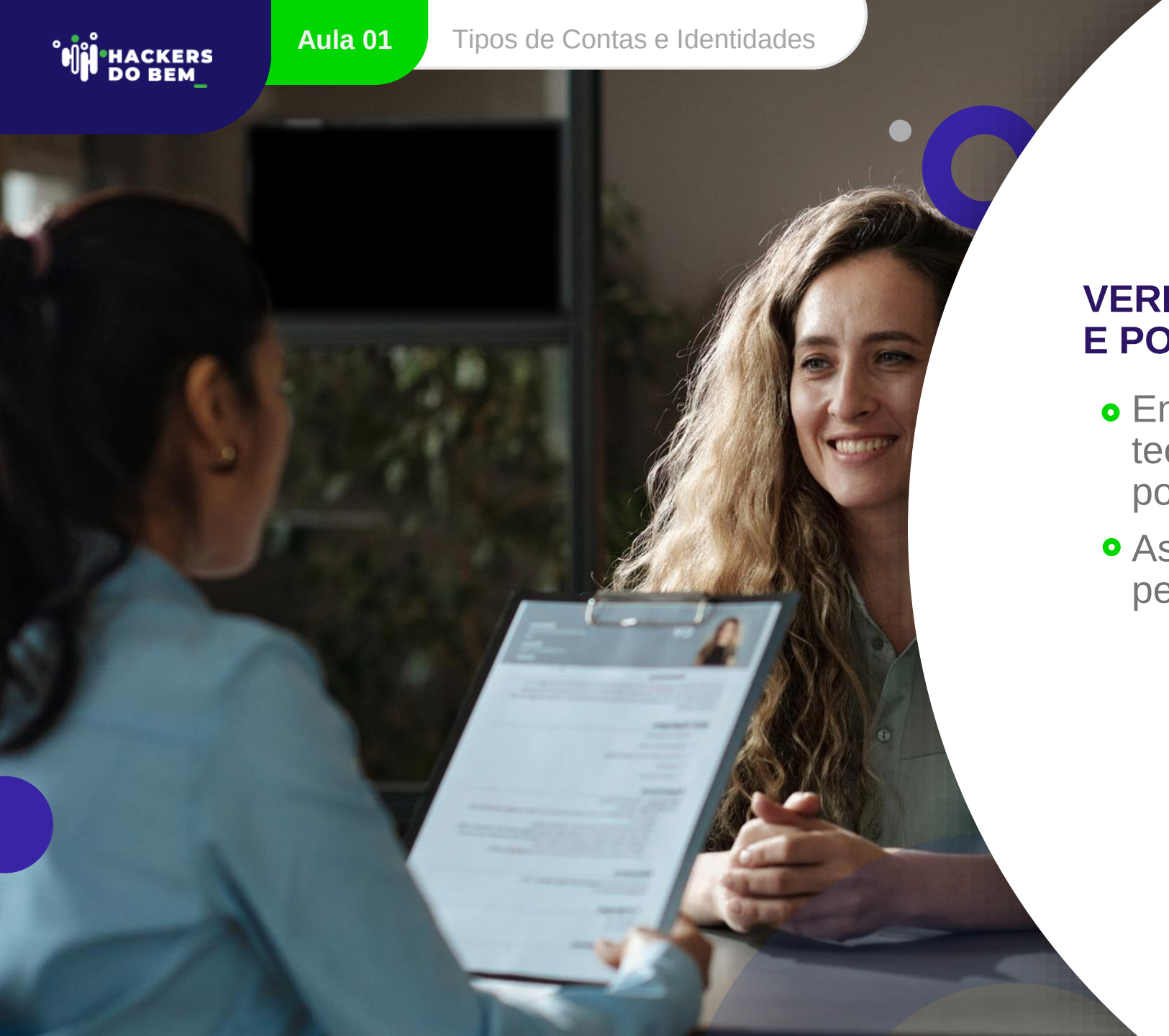
PROVEDORES DE IDENTIDADE

- Serviços responsáveis pelo fornecimento de contas de usuário e pelo processamento de solicitações de autenticação;
- Após autenticar-se em um provedor de identidade confiável, o usuário pode utilizar essa identidade em diferentes sites ou serviços.
- O usuário não precisa criar contas separadas para cada um deles.

Aula 01

Tipos de Contas e Identidades

Verificação de Antecedentes e Políticas de Integração



VERIFICAÇÃO DE ANTECEDENTES E POLÍTICAS DE INTEGRAÇÃO

- Envolve tanto procedimentos e tecnologias de TI/segurança quanto políticas de Recursos Humanos (RH).
- As políticas de gerenciamento de pessoal são aplicadas em três fases:
  - Recrutamento (contratação);
  - Operação (trabalho);
  - Término ou separação (demissão ou aposentadoria.

VERIFICAÇÃO DE ANTECEDENTES

- Avalia se uma pessoa é realmente quem ela diz ser.
- Também se ela não está ocultando atividades criminais, falência ou conexões que a tornem inadequada para o cargo.
- Em ambientes de alta confidencialidade ou com acesso a transações de alto valor e cargos federais são realizadas verificações de antecedentes.

PROCESSO DE INTEGRAÇÃO (*ONBOARDING*)

- Consiste em receber um novo colaborador, fornecedor ou contratado.
- As áreas de TI e RH se unem para: criar conta de acesso, atribuir permissões e garantir que as credenciais da conta sejam conhecidas apenas pelo usuário.
- Outros aspectos e processos envolvidos no *onboarding*:
  - Transmissão segura de credenciais;
  - Alocação de ativos;
  - Treinamento.

ACORDO DE CONFIDENCIALIDADE (NDA)

- Estabelece os termos e condições em relação à confidencialidade das informações.
- É uma medida de proteção importante para garantir que informações sensíveis e estratégicas da empresa sejam mantidas em sigilo.

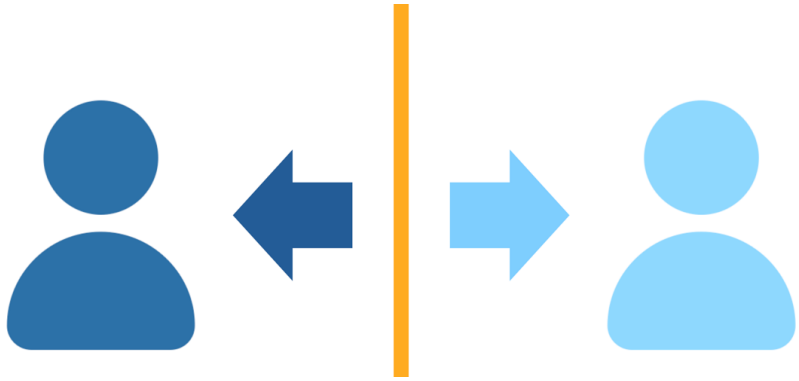
Aula 01

Tipos de Contas e Identidades

Políticas de Pessoal para Gerenciamento de Privilégios

POLÍTICAS DE PESSOAL PARA GERENCIAMENTO DE PRIVILÉGIOS

- Definem como os privilégios de acesso a sistemas, dados e recursos são atribuídos aos funcionários;
- Fatores considerados: suas responsabilidades, cargos e necessidades específicas para realizar suas atividades de trabalho;
- Estabelecem diretrizes claras para a revogação ou alteração de privilégios.



Fonte: Akf Partners[1].

[1]Disponível em: https://akfpartners.com/growth-blog/separation-of-duties-in-an-agile-environment> Acesso em: 05 abr. 2024.

SEPARAÇÃO DE FUNÇÕES

- As funções e responsabilidades devem ser divididas entre os indivíduos para evitar conflitos éticos ou abuso de poder;
- Procedimentos operacionais padrão (SOPs);
- Autoridade compartilhada;
- Nenhum indivíduo deve ter controle absoluto sobre uma função crítica, diminuindo os riscos de abuso, erros ou fraudes.

MENOR PRIVILÉGIO

- Significa que um usuário recebe apenas os direitos necessários para desempenhar sua função, sem privilégios extras.
- É essencial restringir o acesso aos recursos e informações essenciais para o desempenho das atividades do usuário.
- Realizar auditorias periódicas a fim de identificar não conformidades.

POLÍTICAS DE *OFFBOARDING*

- É o processo de garantir que um funcionário, contratado ou terceiro deixe a empresa de forma adequada e organizada.
- Etapas para o *Offboarding*:

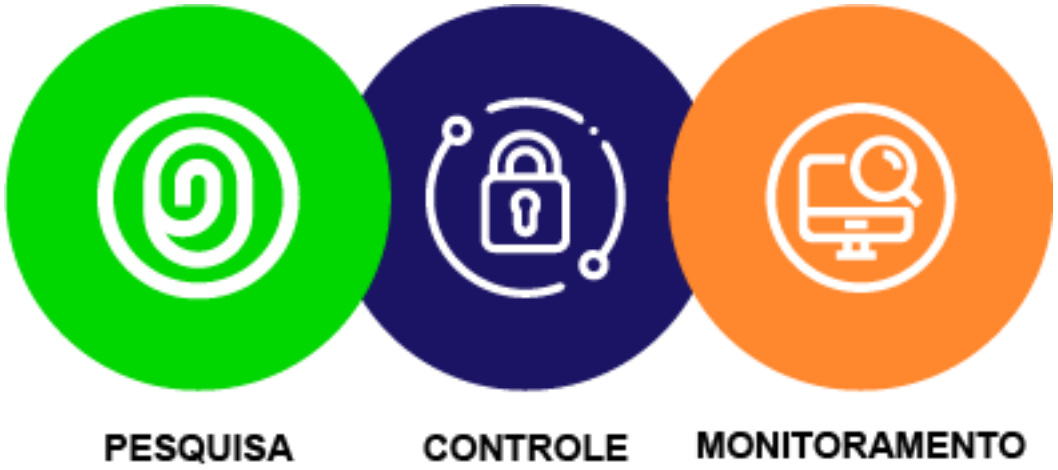
  Gerenciamento de contas;

  Ativos da empresa;

  Ativos pessoais.

SEGURANÇA EM TIPOS DE CONTAS

- Nos sistemas operacionais, dispositivos de rede e produtos de diretório de rede, são utilizados diferentes tipos de contas:
  - Usuário Padrão;
  - Usuário Administrativo;
  - Contas de Grupos de Segurança;
  - Contas de Serviço.



Fonte: Microfocus.
Disponível em: <https://www.microfocus.com/pt-br/cyberres/identity-access-management/privilege-management>
Acesso em: 18 mar. 2024.

GESTÃO DE CREDENCIAIS

- É o processo de administrar e controlar as identidades digitais e as formas de autenticação utilizadas por usuários em sistemas e redes.
- Atividades de gestão de credenciais:
  - Criação de contas de usuário e atribuição de privilégios;
  - Atualização regular de senhas e monitoramento de atividades suspeitas;
  - Revogação de credenciais e implementação de medidas de segurança para proteger as credenciais armazenadas.

CONTAS DE CONVIDADOS

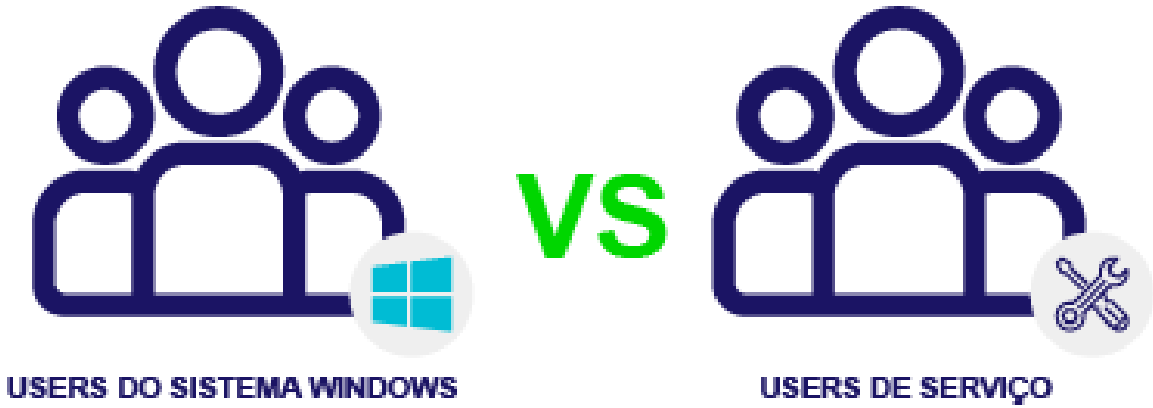
- São contas de usuário com acesso limitado e controlado.
- Criadas para permitir que usuários temporários ou externos acessem recursos específicos sem terem uma conta permanente:
  - Atender necessidades de visitantes ou fornecedores;
  - Possuem restrições de acesso, privilégios e permissões;
  - Podem ter um período de validade definido;
  - Devem ser monitoradas e auditadas.

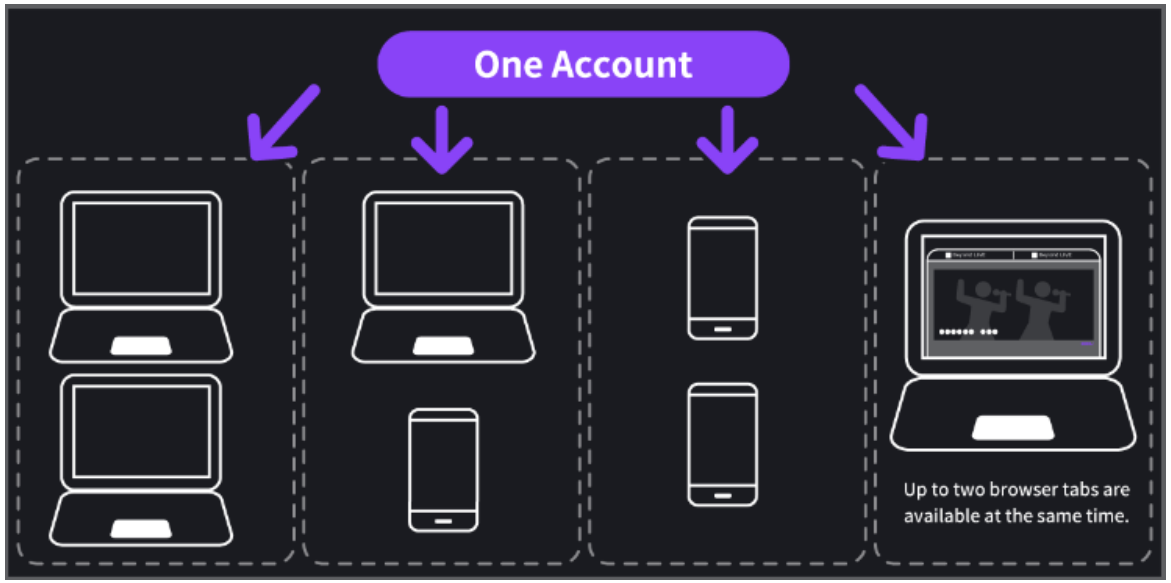
CONTAS DE ADMINISTRADOR OU ROOT

- São contas de usuário que possuem os mais altos privilégios em um sistema de computador ou rede. Características:
  - Controle total sobre o sistema – Root no Unix e Administrador no MS-Windows;
  - Criada durante a instalação;
  - Realiza alterações críticas e executa tarefas avançadas;
  - Devem ser monitoradas e auditadas.

SERVIÇOS DE CONTA

- São tipos de contas de usuário usadas no contexto de sistemas operacionais Windows para executar serviços e processos:
  - Conta de Sistema (System Account): executa tarefas do Gerenciador de Controle de Serviços e o subsistema do Windows;
  - Conta de Serviço Local (Local Service Account): executa serviços localmente;
  - Conta de Serviço de Rede (Network Service Account): executa serviços que precisam acessar recursos de rede como compartilhamento.





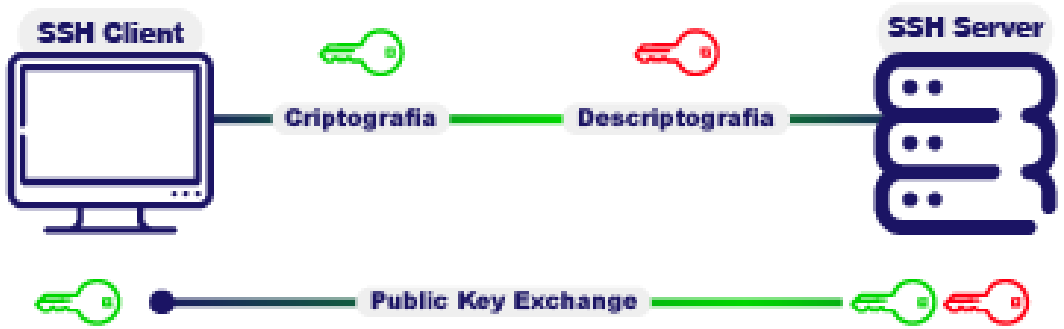
Fonte: Beyondlive.
Disponível em: <https://beyondlive.com/faq/29>
Acesso em: 18 mar. 2024.

CONTAS E CREDENCIAIS COMPARTILHADAS, GENÉRICAS E DE EQUIPAMENTO

- São tipos de identificações de acesso utilizadas para permitir o compartilhamento de recursos ou a execução de processos específicos:
  - Contas e Credenciais Compartilhadas);
  - Contas Genéricas;
  - Contas de Equipamento (Device Accounts).

CHAVES DO SSH

- Chaves do Protocolo Secure Shell (SSH), são um método de autenticação e criptografia utilizado para estabelecer conexões seguras.
- Consistem em pares de chaves criptográficas: uma chave privada e uma chave pública, principal vantagem em relação às senhas convencionais.
- São mais difíceis de serem comprometidas por ataques de força bruta e menos suscetível a ataques de *phishing*.



Fonte: Medium.
Disponível em: https://medium.com/@aqeelabbas3972/introduction-to-ssh-secure-shell-0d07e18d3149
Acesso em: 18 mar. 2024.

5

HACKERS DO BEM_

Módulo 05

Gerenciamento de Identidades e Contas

Aula 02

Políticas de Contas_

Softex SENAI RNP MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Introdução

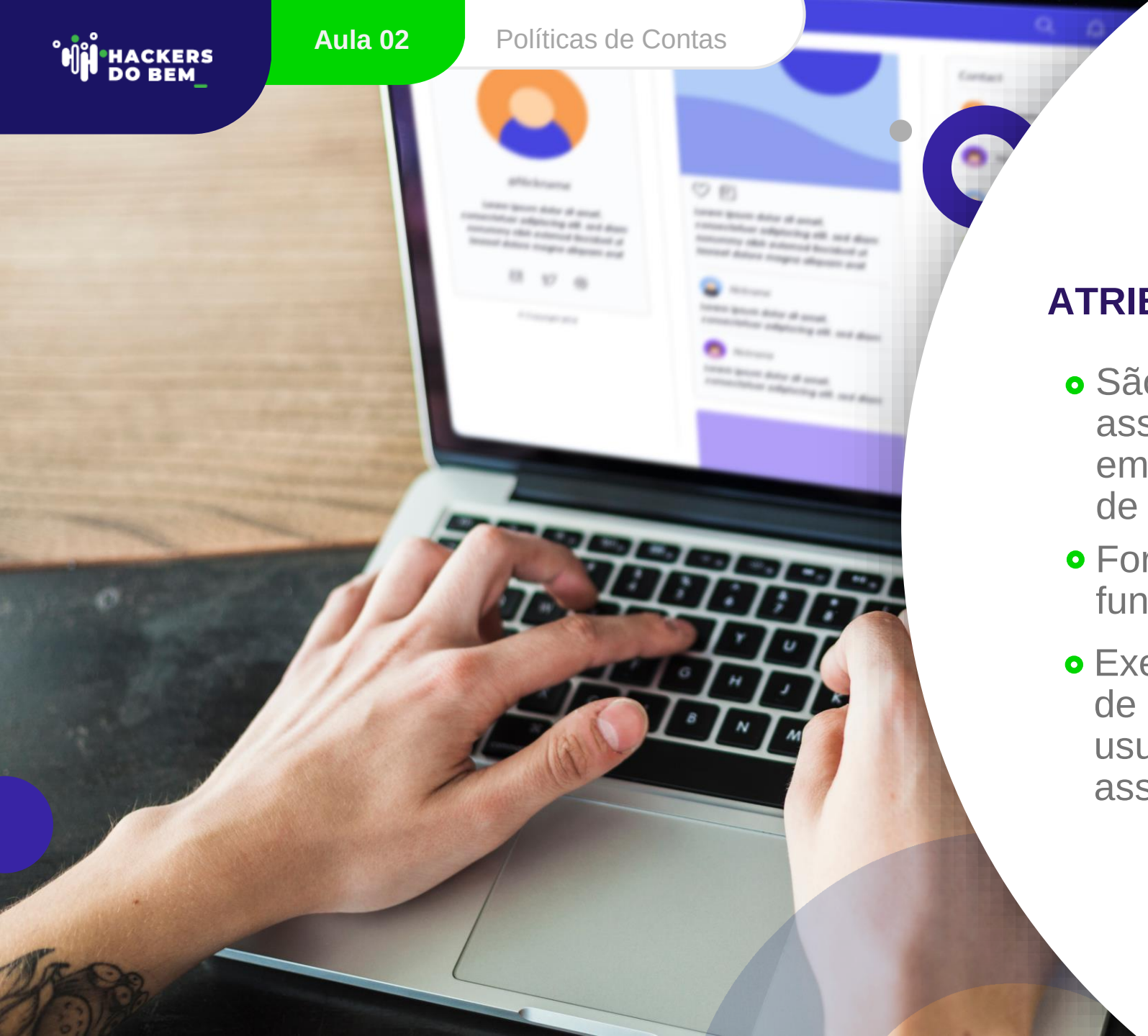
Nesta aula, você conhecerá os seguintes assuntos:

- Políticas relacionadas ao ciclo de vida das contas de usuário em ambiente computacional.
- As políticas de contas como diretrizes para controlar o acesso e o uso de contas de usuário.
- A definição de regras e restrições sobre quem tem acesso a quais recursos e em quais condições.
- Definição de políticas de senha de conta, restrições e definição de atributos de conta.

Aula 02

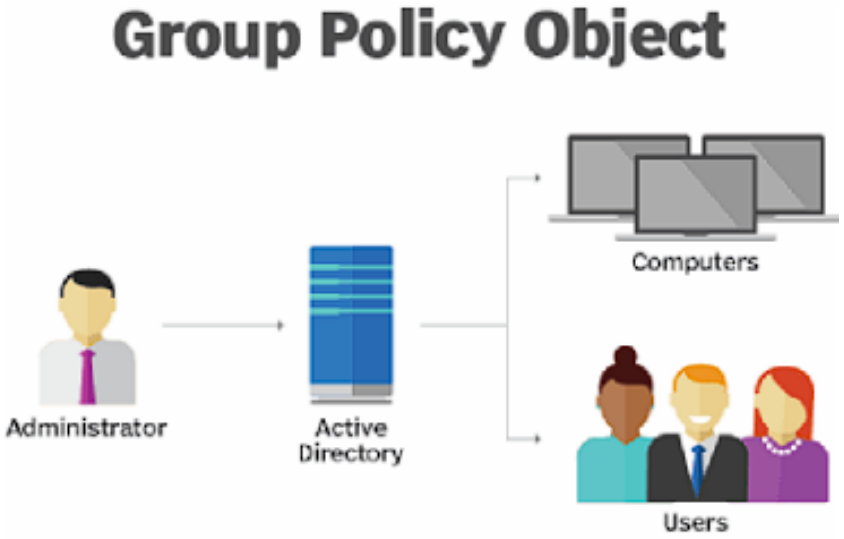
Políticas de contas

Contas_



ATRIBUTOS DE CONTAS

- São informações específicas associadas a uma conta de usuário em um sistema de gerenciamento de contas.
- Fornecem detalhes sobre a identidade, função e características do usuário.
- Exemplos de atributos: nome, endereço de e-mail, telefone e departamento do usuário, nível de acesso, permissões associadas, etc.



Fonte: Eventos.
Disponível em> https://eventos.ifmt.edu.br/cursos/home/
Acesso em: 18 mar. 2024.

POLÍTICA DE CONFIGURAÇÕES DE SENHAS DE CONTA

- Contêm as regras e diretrizes que determinam quem tem permissão para acessar recursos ou informações em que condições e com quais privilégios.
- Podem abordar aspectos como: autenticação, autorização, criptografia, restrições, segregação de funções e controle de acesso baseado em papéis.
- Uma forma de implementação são os GPOs (objetos de política de grupo) configurados em uma rede Windows Active Directory.

POLÍTICAS DE ACESSO

- É um conjunto de diretrizes e regras que determinam os requisitos e as restrições relacionadas às senhas utilizadas pelas contas de usuário.
- Visa promover senhas fortes e seguras.
- Aspectos da política de configurações de senhas de conta:
  - Comprimento mínimo da senha;
  - Complexidade da senha;

POLÍTICAS DE ACESSO

- Exigência de alteração periódica;
- Restrições de reutilização de senhas;
- Bloqueio após várias tentativas falhas;
- Proibição de senhas comuns.

RESTRIÇÕES DE CONTAS

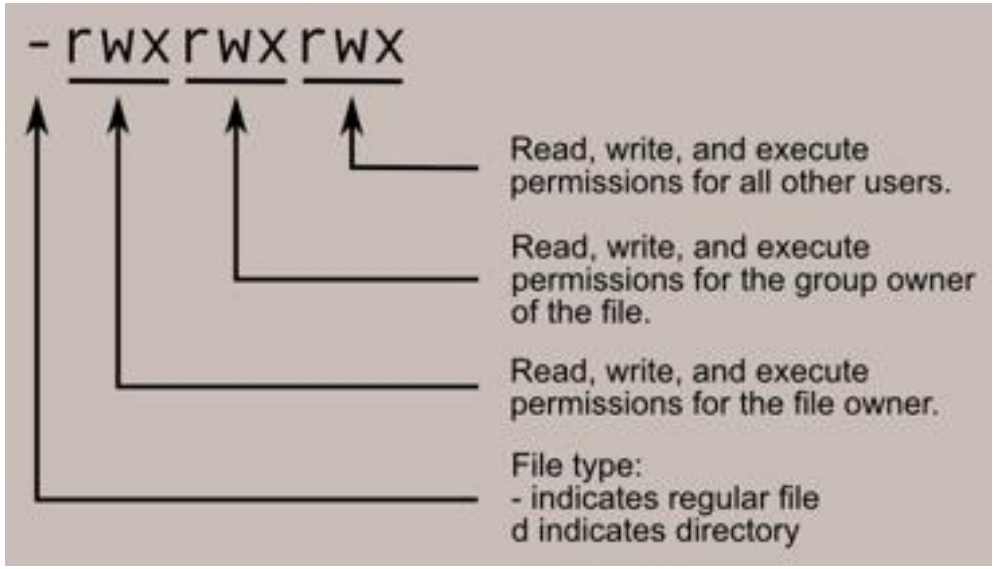
- São mecanismos utilizados para limitar e controlar o acesso e o uso de contas de usuário com base em diferentes critérios.
- Podem ser:
  - Políticas baseadas em localização;
  - *Geofencing* – tecnologia que delimita espaços geográficos utilizando dispositivos móveis ou geolocalização.
  - Restrições baseadas em horário.

AUDITORIA DE CONTAS

- É um processo que envolve a revisão e análise sistemática das atividades e eventos relacionados às contas de usuário.
- Pode abordar diferentes aspectos como:
  - Conformidade;
  - Monitoramento de atividades;
  - Detecção de violações de segurança;
  - Investigação forense.

PERMISSÕES DE CONTAS

- Referem-se aos direitos e privilégios atribuídos a uma conta de usuário. Determinam o que um usuário pode ou não pode fazer.
- Tipos de permissões:
  - Leitura;
  - Gravação;
  - Execução;
  - Exclusão;
  - Administração.



Fonte: Blog Apiki.
Disponível em: <https://blog.apiki.com/permissao-de-arquivos-e-pastas-do-wordpress/>.
Acesso em: 18 mar. 2024.

BLOQUEIO E DESABILITAÇÃO DE CONTAS

- O bloqueio refere-se a uma medida temporária em que o acesso a uma conta é negado por um determinado período de tempo.
- Geralmente aplicado quando ocorrem várias tentativas de *login* malsucedidas.

BLOQUEIO E DESABILITAÇÃO DE CONTAS

- A desabilitação é uma ação permanente em que a conta de usuário é desativada ou removida completamente do sistema.
- Acontece:
  - Quando um usuário deixa a organização;
  - Quando uma conta está associada a atividades fraudulentas.
  - Quando há uma violação significativa da política de segurança.

5

HACKERS DO BEM_

Módulo 05

Gerenciamento de Identidades e Contas

Aula 03

Soluções de Autorização

Softex SENAI RNP MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Introdução

Nesta aula, você conhecerá os seguintes assuntos:

- Sistemas de controle de acesso – Discretionary Access Control (DAC) e Role-Based Access Control (RBAC);
- Sistemas avançados – Mandatory Access Control (MAC) e Attribute-Based Access Control (ABAC);
- Permissões de *read*, *write* e *execute* para sistemas de arquivos;
- Privileged Access Management (PAM), Directory Services usando o Lightweight Directory Access Protocol (LDAP);
- Identificação federada;
- Protocolos de segurança.

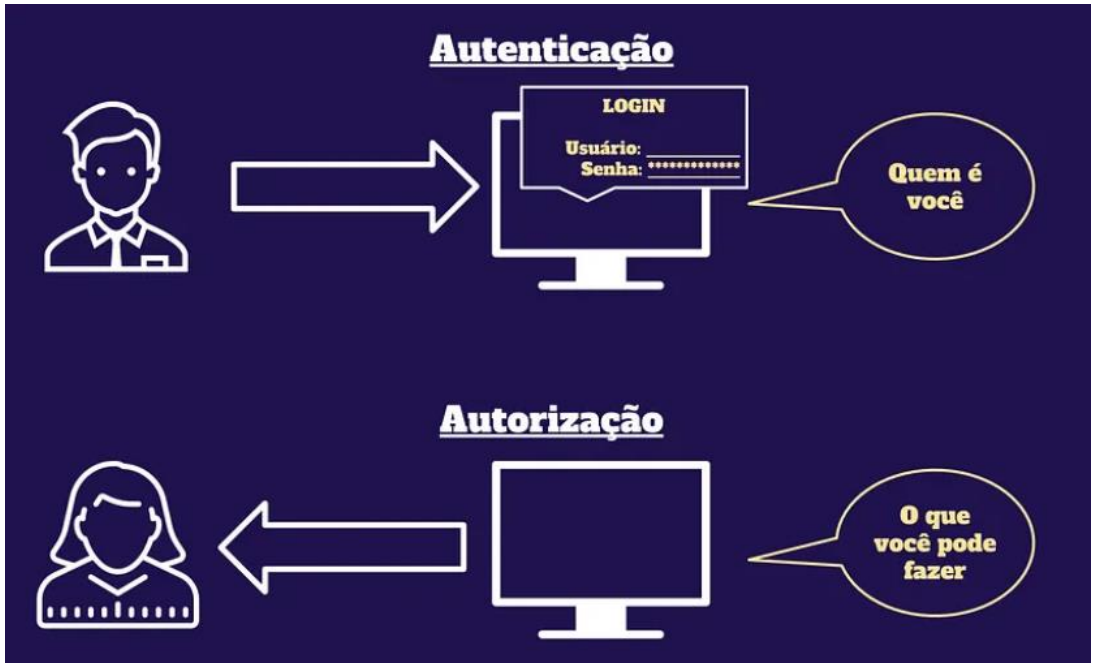
Aula 03

Soluções de Autorização

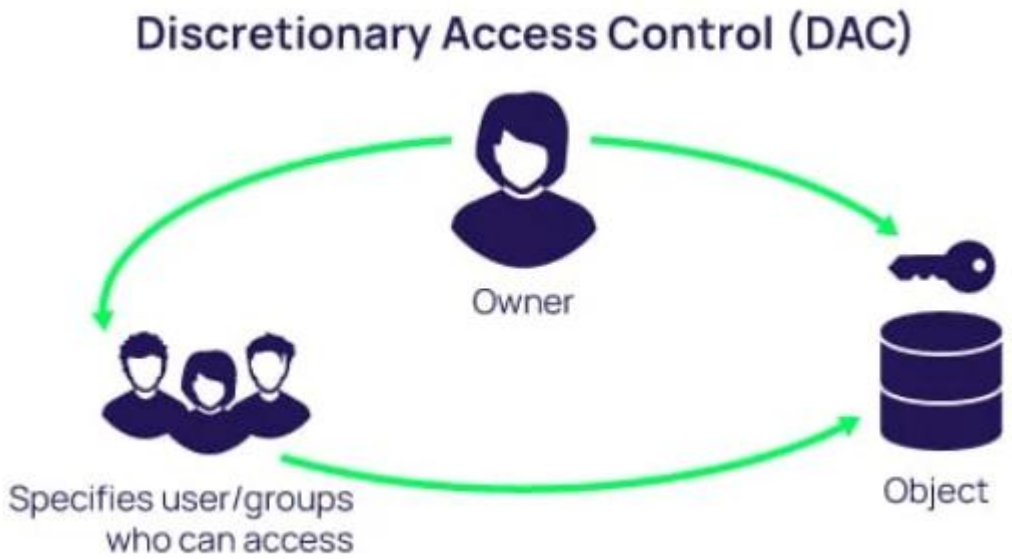
Controle de Acesso

CONTROLE DE ACESSO

- É um conjunto de políticas, procedimentos e tecnologias visando garantir que apenas pessoas autorizadas possam acessar determinados recursos.
- Envolve um processo de autenticação e autorização.
- O objetivo maior é proteger informações sensíveis e recursos críticos.



Fonte: Medium.
Disponível em: <https://medium.com/@andressaabrantes/seguran%C3%A7a-em-web-apis-378404337ac7>
Acesso em: 18 mar. 2024.



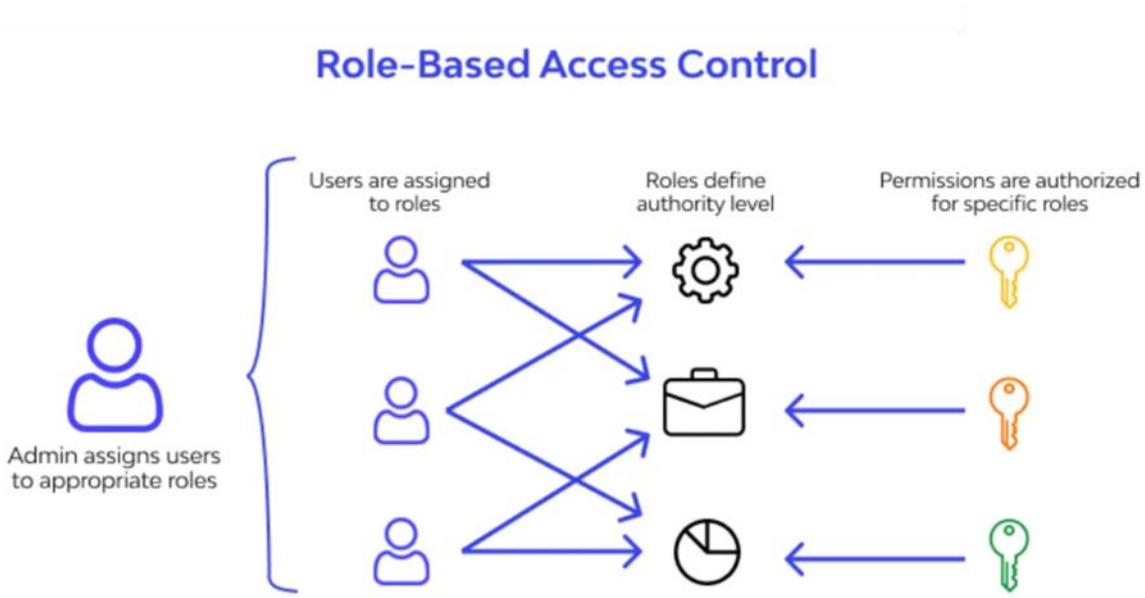
Fonte: Delinea.
Disponível em: <https://delinea.com/blog/access-control-models-methods>
Acesso em: 18 mar. 2024.

CONTROLE DE ACESSO DISCRICIONÁRIO - DISCRETIONARY ACCESS CONTROL (DAC)

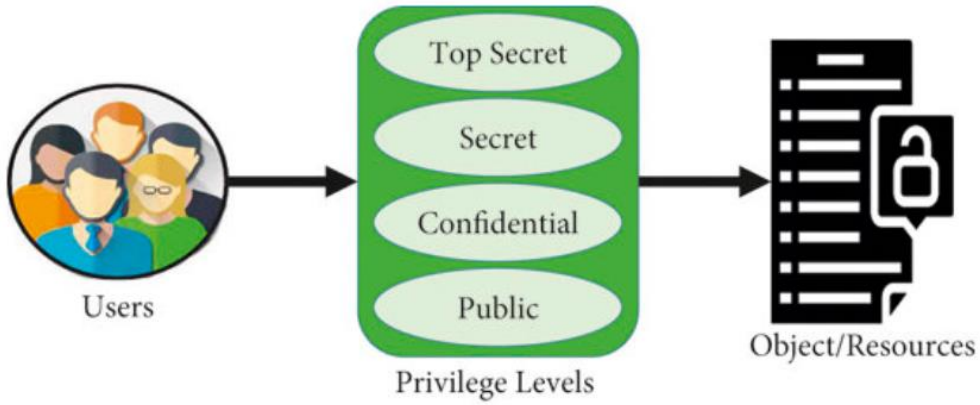
- É um modelo de controle de acesso onde os proprietários determinam quais as operações que podem ser realizadas sobre os recursos.
- Passos para um DAC:
  - Proprietários e respectivos recursos;
  - Permissões de acesso para cada recurso;
  - Lista de Controle de Acesso associada a cada recurso;
  - Proprietário e controle.

CONTROLE DE ACESSO BASEADO EM FUNÇÃO – ROLE-BASED ACCESS CONTROL (RBAC)

- É um modelo de controle de acesso onde as permissões estão baseadas na atribuição de funções específicas dos usuários.
- Funcionamento do RBAC:
  - Funções baseadas nas responsabilidades e cargos ;
  - Usuários recebem uma ou mais funções;
  - Permissões associadas às funções;
  - Recursos recebem permissões.



Fonte: Micoope.
Disponível em: <https://www.micoope.com.gt/?o=an-enhancement-of-the-role-based-access-control-model-nn-LAw9YjhQ>.
Acesso em: 18 mar. 2024.



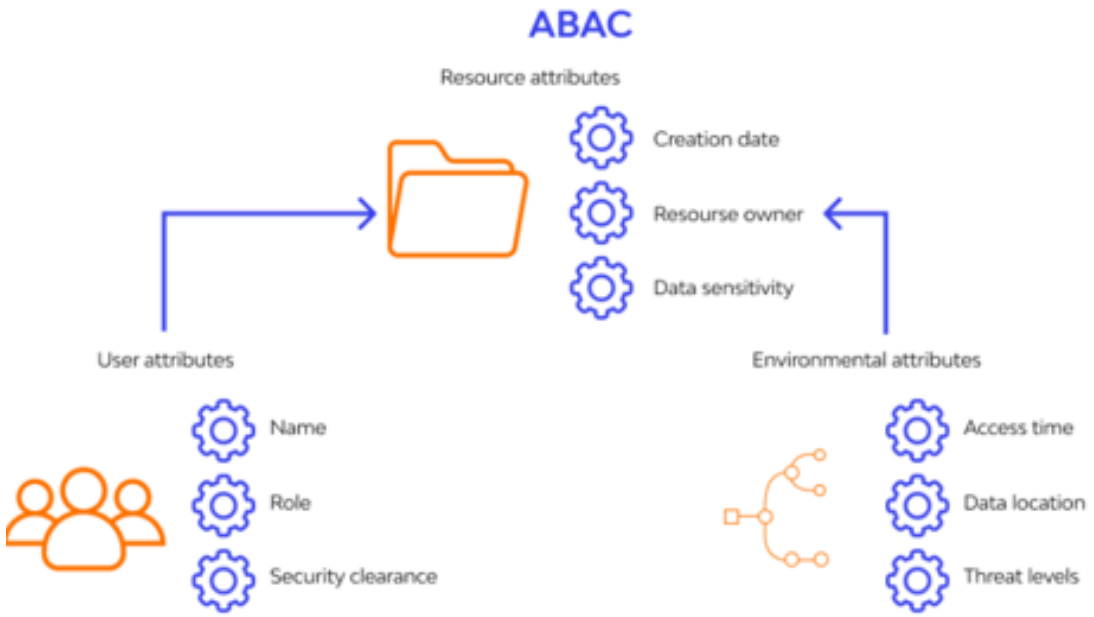
Fonte: Research Gate.
Disponível em: <https://www.researchgate.net/figure/view-of-mandatory-access-control-MAC_fig4_358430862>.
Acesso em: 18 mar. 2024.

CONTROLE DE ACESSO OBRIGATÓRIO – MANDATORY ACCESS CONTROL (MAC)

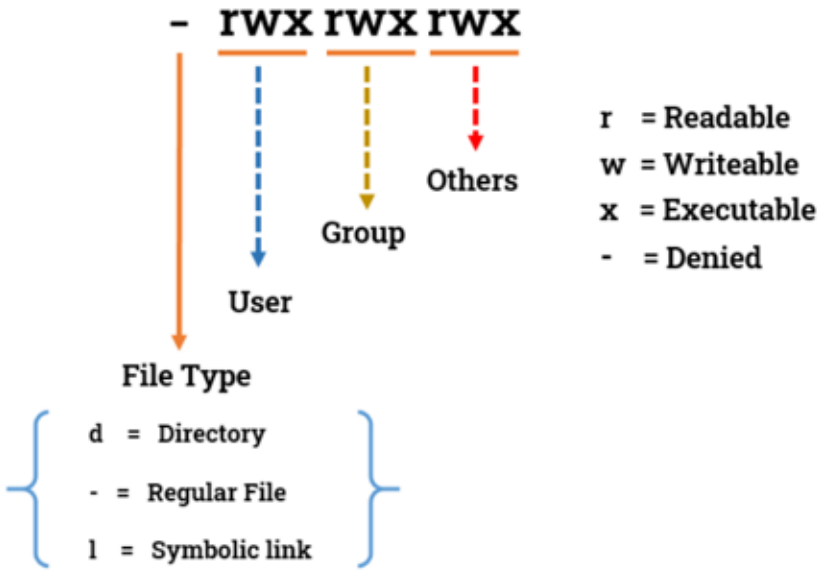
- É um modelo de controle de acesso onde as permissões estão baseadas em políticas definidas pelo sistema.
- Funcionamento do MAC:
  - Políticas de segurança da organização;
  - Rótulos de segurança "Alto", "Médio" e "Baixo;
  - Regras de acesso definem as permissões;
  - Aplicação das políticas.

CONTROLE DE ACESSO BASEADO EM ATRIBUTOS – ATTRIBUTE-BASED ACCESS CONTROL (ABAC)

- É um modelo de controle de acesso onde as permissões estão baseadas em atributos de entidades, recursos e condições.
- Funcionamento do ABAC:
  - Atributos;
  - Entidades;
  - Recursos;
  - Políticas de autorização.



Fonte: Python.
Disponível em: <https://python.plainenglish.io/policy-based-access-control-pbac-what-it-is-and-why-you-need-it-in-your-modern-data-lakehouse-672e869c2082>.
Acesso em: 18 mar. 2024.



Fonte: Medium.
Disponível em: <https://medium.com/@dhanashrisaner.30/enhancing-security-with-linux-file-permissions-and-access-control-lists-ed6eb53679a5>.
Acesso em: 18 mar. 2024.

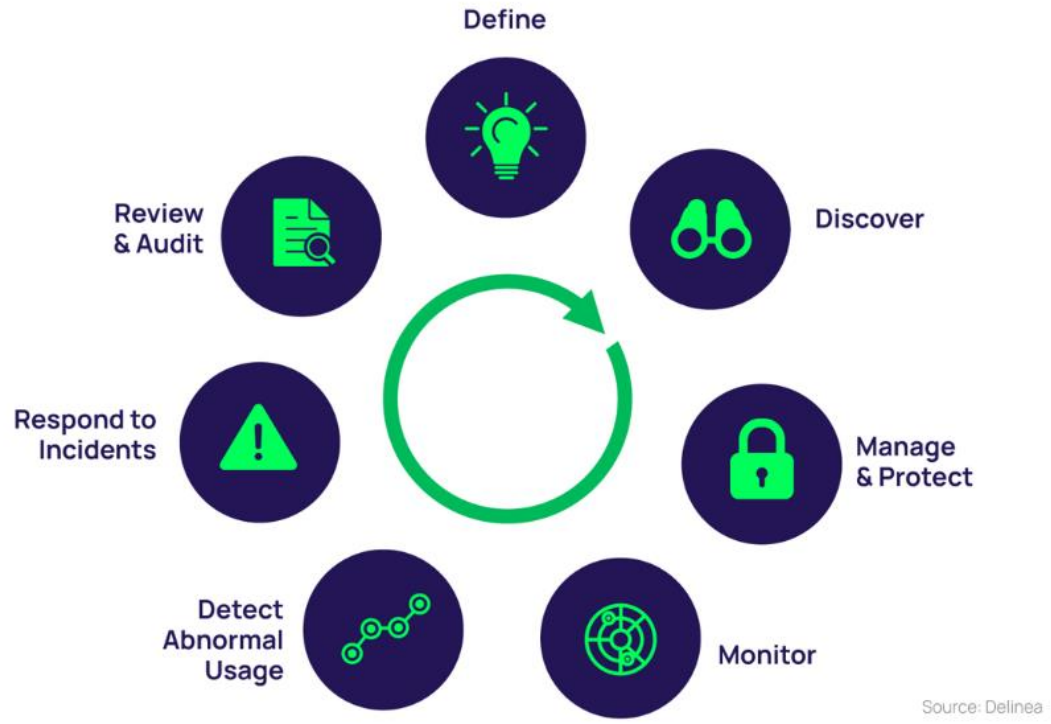
PERMISSÕES DO SISTEMA DE ARQUIVOS

- São as permissões que determinam quais ações os usuários podem realizar em um arquivo ou diretório.
- Funcionamento das permissões:
  - Leitura (*Read* –r);
  - Escrita (*Write* –w);
  - Execução (*Execute* –x);
  - Comando chmod;
  - Comando chown.

GERENCIAMENTO DE ACESSO PRIVILEGIADO - PRIVILEGED ACCESS MANAGEMENT (PAM)

- É um procedimento que se concentra em proteger e gerenciar o acesso a contas e recursos privilegiados.
- Implementação do PAM:

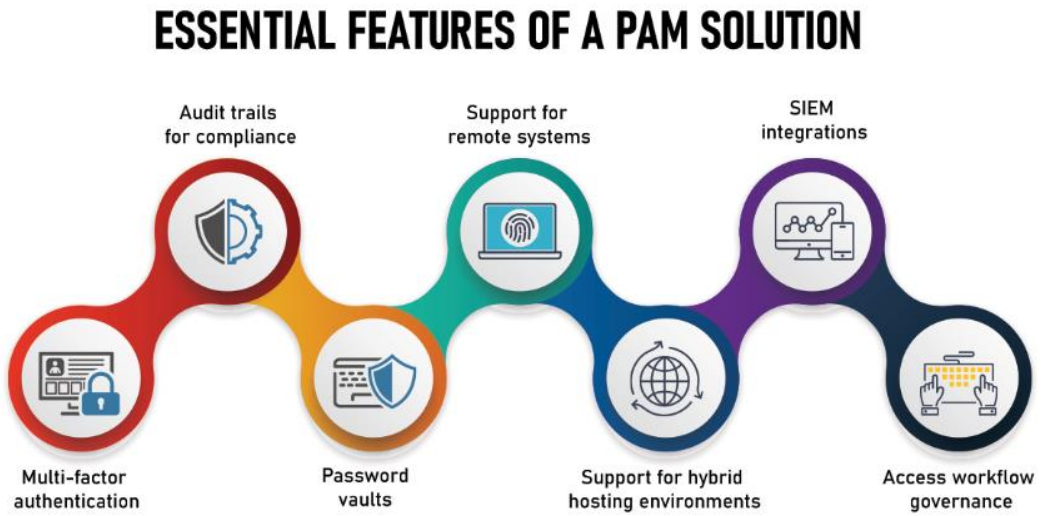
1. Identificação de contas privilegiadas;
2. Políticas de acesso;
3. Gerenciamento de credenciais;



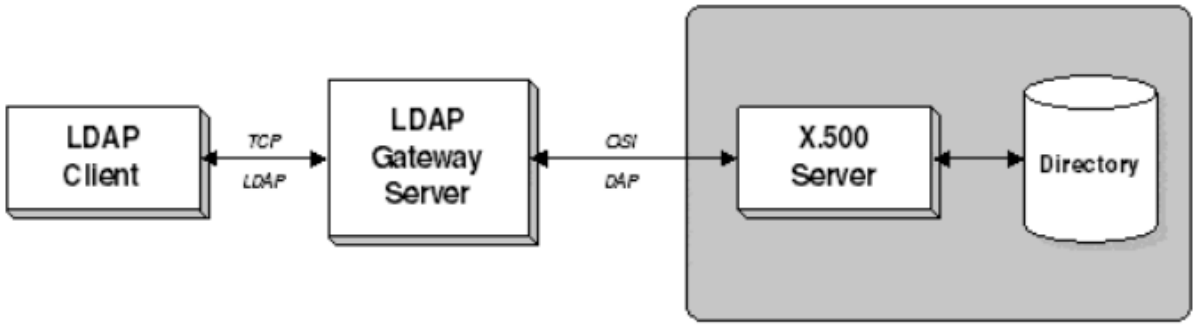
Fonte: Delinea
Disponível em: <https://delinea.com/blog/privileged-access-management-lifecycle-path-to-maturity>.
Acesso em: 18 mar. 2024.

GERENCIAMENTO DE ACESSO PRIVILEGIADO - PRIVILEGED ACCESS MANAGEMENT (PAM)

4. Autenticação multifator (MFA);
5. Monitoramento de atividades;
6. Rotação de senhas;
7. Controle de sessões;
8. Aprovação e revisão.



Fonte: Spice Works.
Disponível em: <https://www.spiceworks.com/it-security/identity-access-management/articles/top-10-privileged-access-management-solutions/>.
Acesso em: 18 mar. 2024.



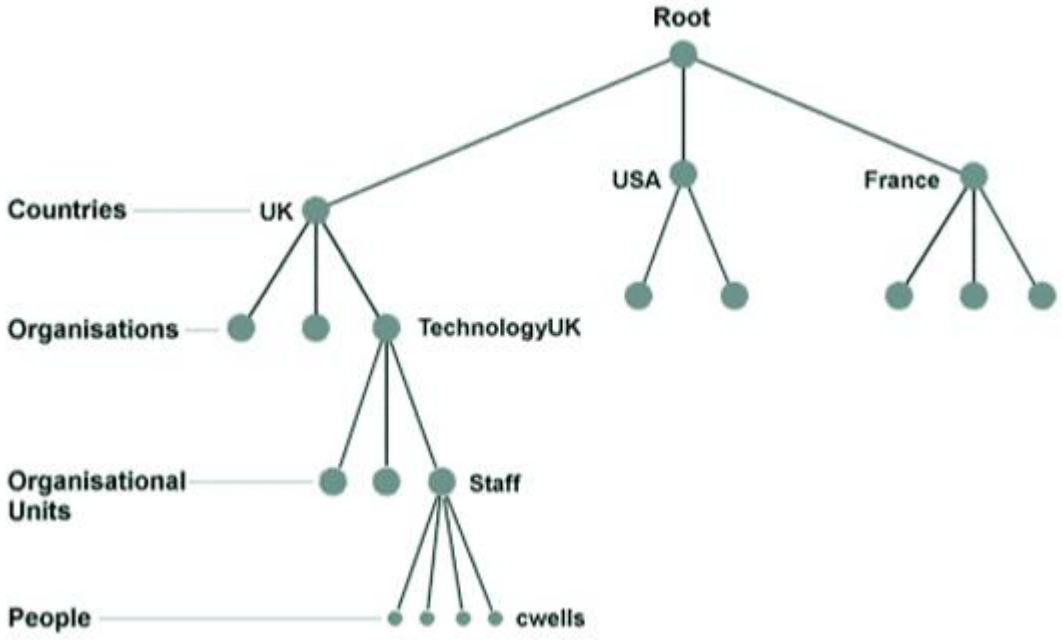
Fonte: Netwokency.
Disponível em: <https://networkencyclopedia.com/lightweight-directory-access-protocol-ldap/>.
Acesso em: 18 mar. 2024.

SERVIÇOS DE DIRETÓRIO

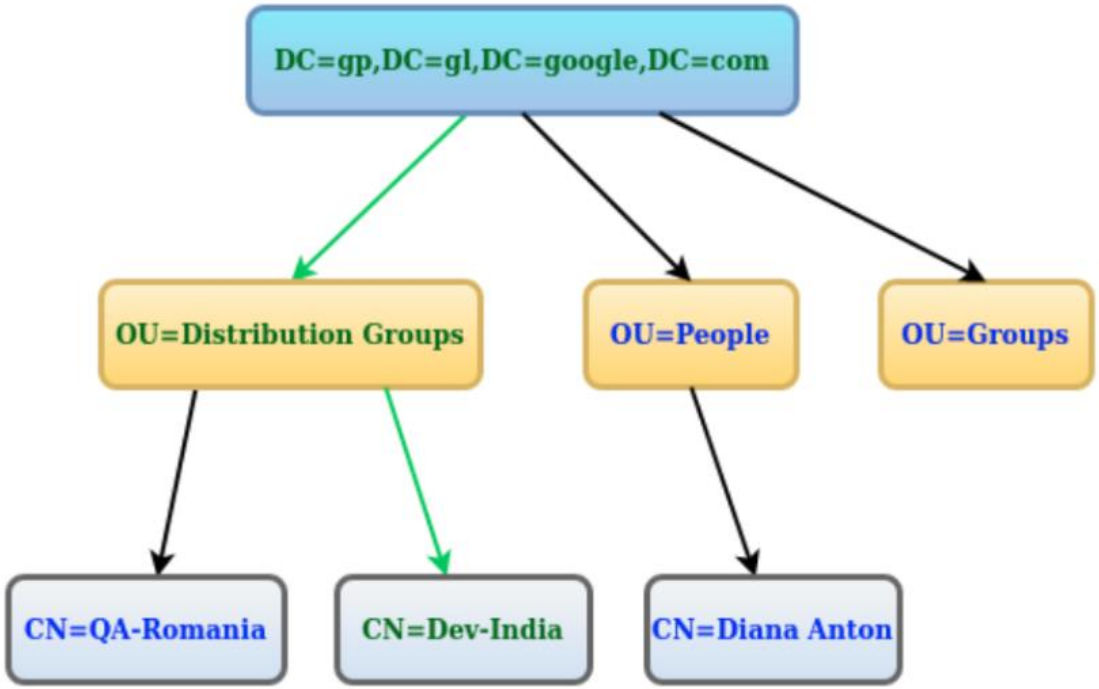
- São sistemas que permitem armazenar, organizar e recuperar informações de forma hierárquica.
- Tipos: Lightweight Directory Access Protocol (LDAP) e diretórios formato X.500.
- Funcionamento dos serviços de diretório:
  - LDAP – versão simplificada do padrão X.500;
  - Diretórios X.500 – segue o padrão X.500;

SERVIÇOS DE DIRETÓRIO

- Hierarquia – entradas de diretório pai e filho;
- Distinguished Name (DN) - identificação única para cada entrada no diretório;
- Árvore de diretórios;
- LDAP como Interface;
- Consultas LDAP;
- Autenticação.



Fonte: Keith brooks.
Disponível em: <https://keithbrooks.com/download/Collabsphere2021_ADSync.pdf>. Acesso em: 18 mar. 2024.



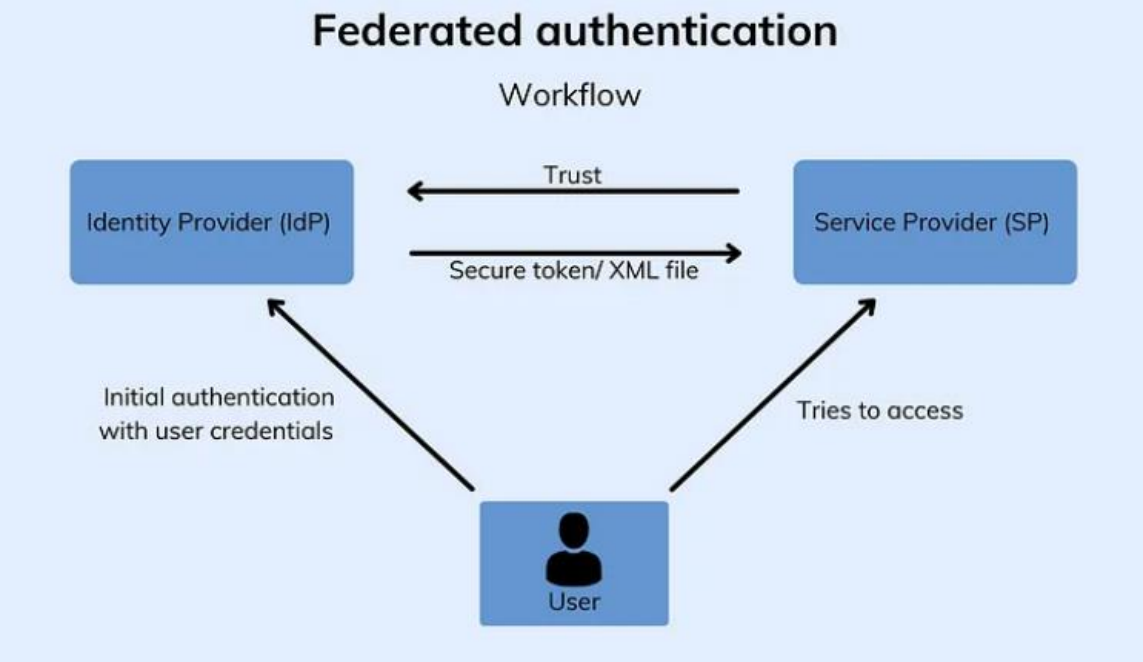
Fonte: Stack Over Flow.
Disponível em: <https://stackoverflow.com/questions/18756688/what-are-cn-ou-dc-in-an-ldap-Search>.
Acesso em: 18 mar. 2024.

ELEMENTOS EM SISTEMAS DE GERENCIAMENTO DE DIRETÓRIOS

- São elementos usados LDAP e nos diretórios X.500 para identificar, classificar e organizar informações.
- Elementos utilizados:
  - Common Name (CN);
  - Organizational Unit (OU);
  - Organization (O);
  - Country (C);
  - Domain Component (DC).

FEDERAÇÃO

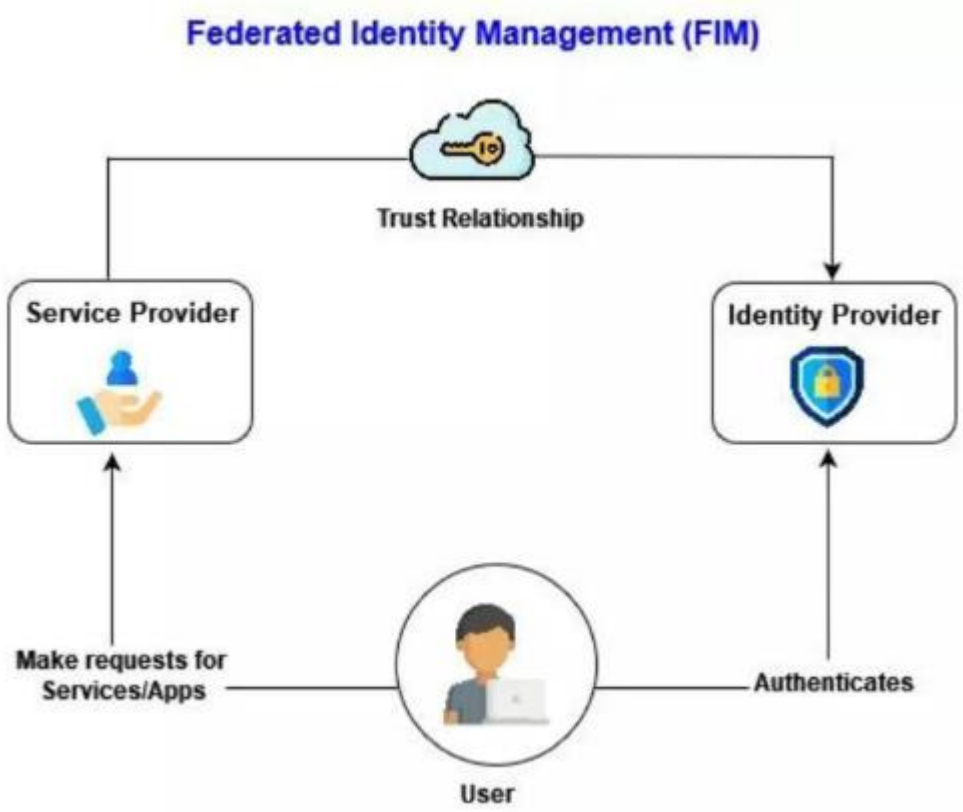
- Trata-se de um modelo onde diversas organizações ou serviços concordam em compartilhar informações de autenticação e autorização.
- Funcionamento:
  - Identidades e atributos;
  - Provedores de Identidade (IdPs);
  - Provedores de Serviços (SPs);



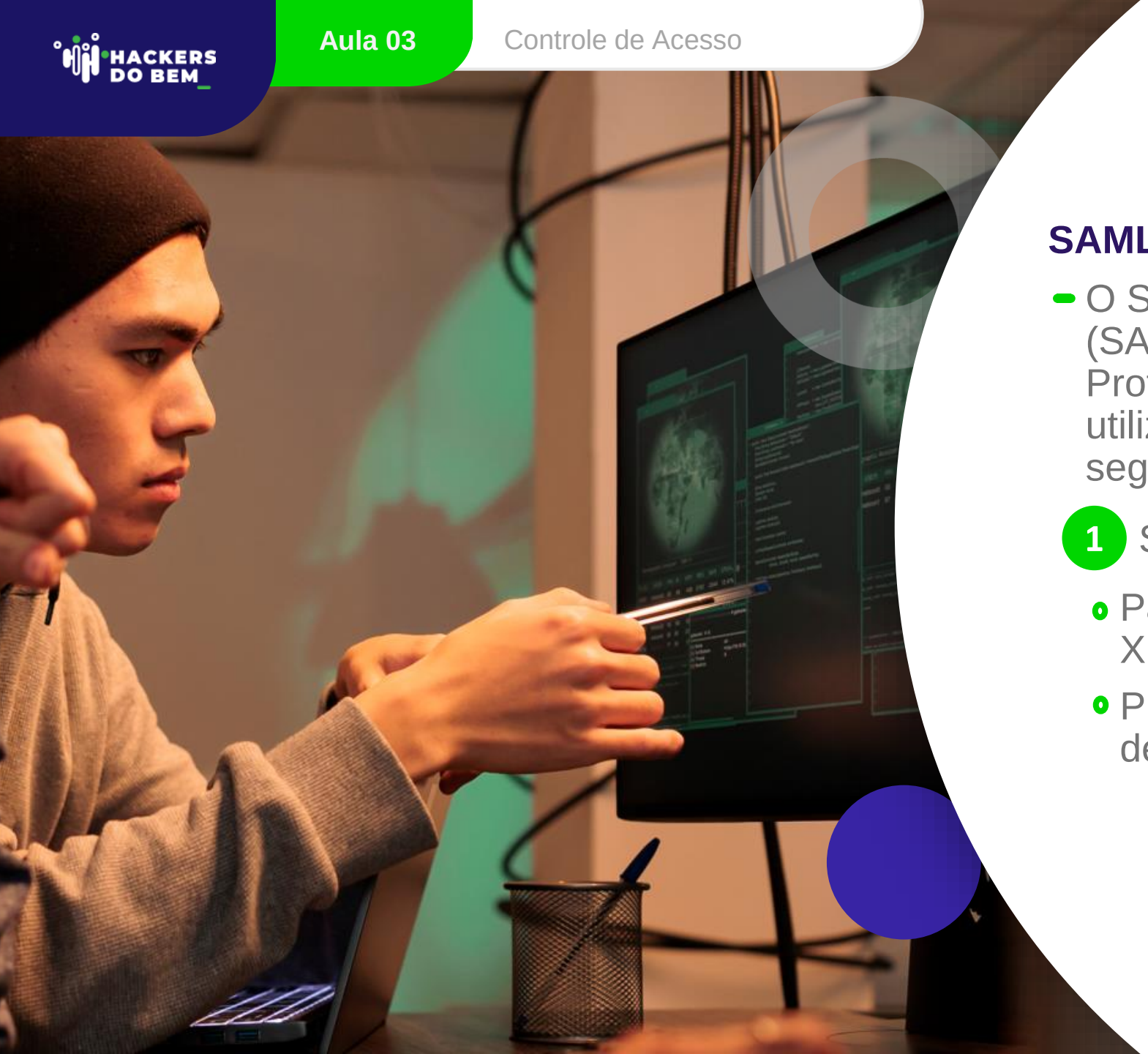
Fonte: Link springer.
Disponível em: <https://link.springer.com/chapter/10.1007/978-1-4842-8936-5_2>.
Acesso em: 18 mar. 2024.

FEDERAÇÃO

- Federação;
- Security Assertion Markup Language (SAML);
- Processo de autenticação e autorização;
- Benefícios da Federação;
- Controle de acesso granular.



Fonte: Link springer.
Disponível em: <https://www.miniorange.com/blog/federated-identity-management-fim/>.
Acesso em: 18 mar. 2024.



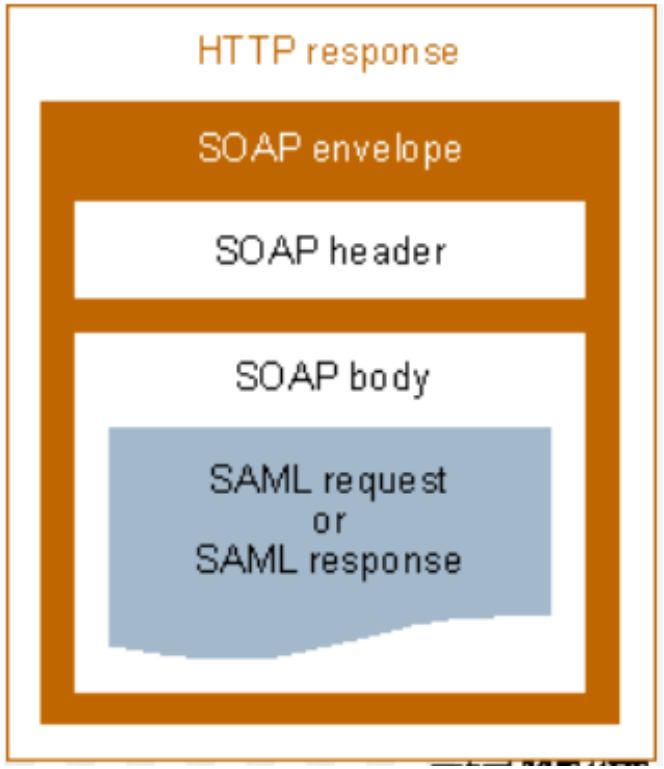
SAML E SOAP

- O Security Assertions Markup Language (SAML) e o Simple Object Access Protocol (SOAP) são protocolos utilizados para prover autenticação e segurança.

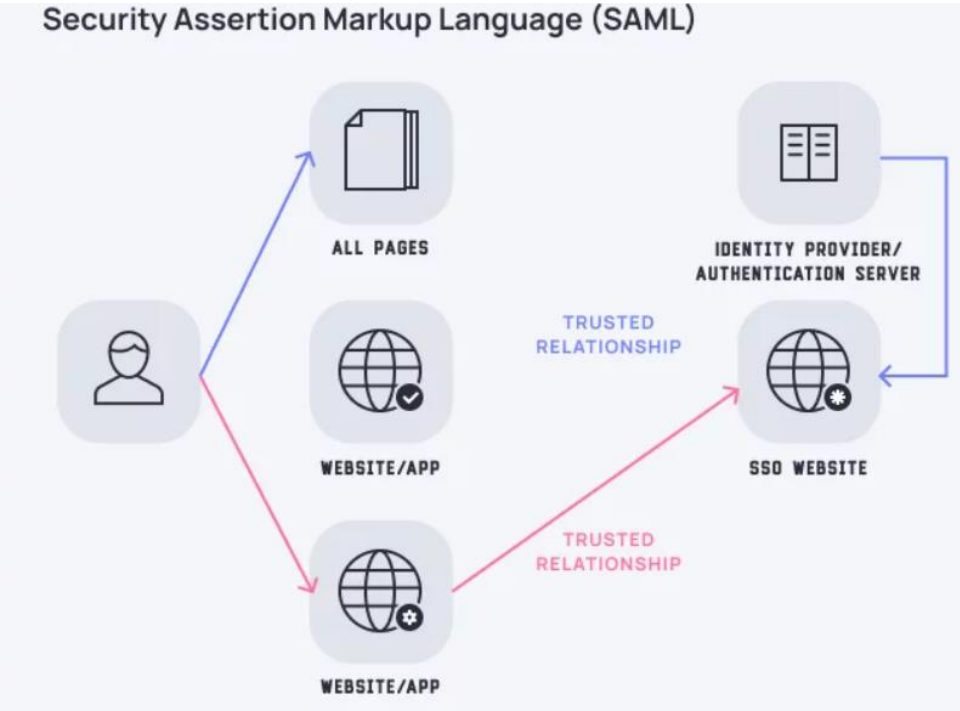
1. SAML:
   - Padrão de segurança baseado em XML;
   - Proporciona a troca de informações de autenticação e autorização.

SAML E SOAP

- Componentes do SAML:
  - Afirmações (Assertions);
  - Provedor de identidade (IdP);
  - Provedor de Serviço;
  - Pacotes SAML (SAML Artifacts);
  - Protocolos SAML.



Fonte: Research Gate.
Disponível em: <https://www.researchgate.net/figure/Figura-1-Estrutura-de-uma-mensagem-SOAP-KALIN-2009_fig1_273316362>.
Acesso em: 18 mar. 2024.



Fonte: Front egg.
Disponível em: <https://frontegg.com/guides/saml>
Acesso em: 18 mar. 2024.

SAML E SOAP

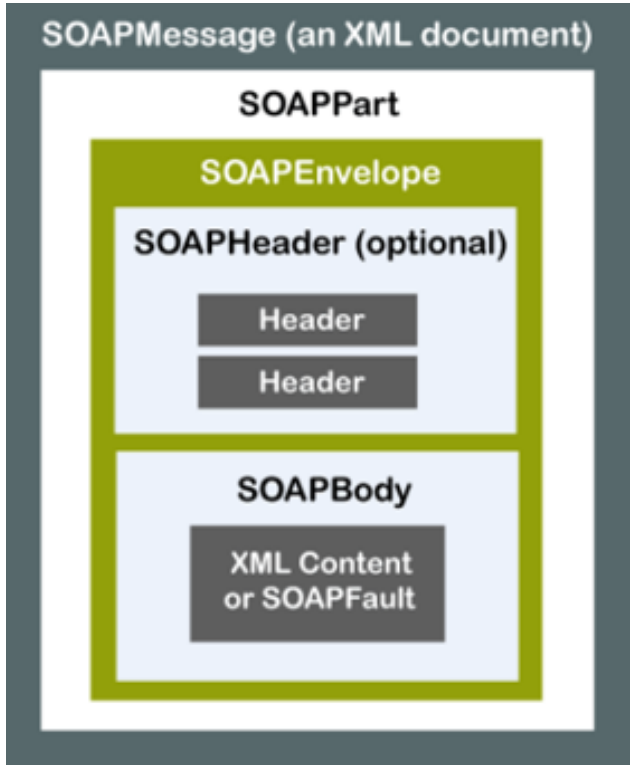
- Fluxo de Autenticação SAML:
  - Um usuário acessa serviço (SP);
  - O SP redireciona o usuário para o IdP apropriado;
  - O IdP autentica o usuário e emite uma afirmação SAML;
  - O usuário é redirecionado de volta para o SP com a afirmação SAML.
  - O SP verifica a assinatura digital do token SAML e concede o acesso.

SAML E SOAP

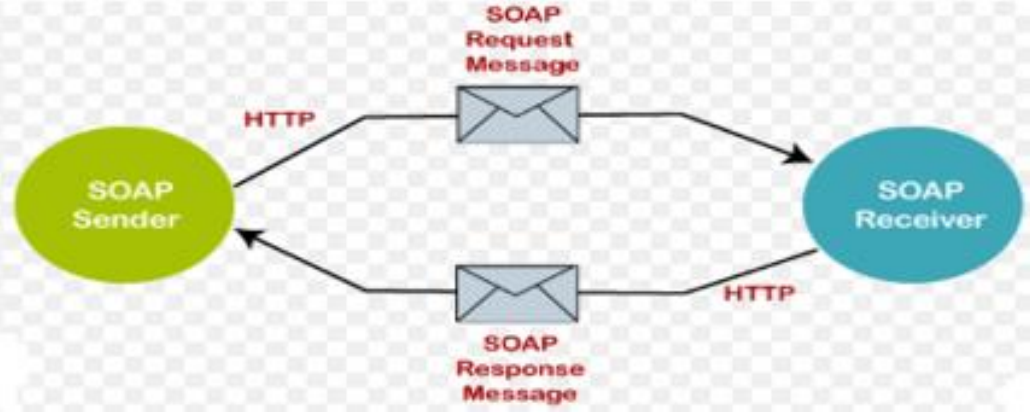
2 SOAP:

- Protocolo de comunicação baseado em XML;
- Proporciona a troca de mensagens entre aplicativos em uma rede.

- Componentes do SOAP:
  - Envelope SOAP;
  - Header SOAP;
  - Body SOAP;
  - Protocolo de transporte.



Fonte: Atitude reflexiva.
Disponível em: <https://atitudereflexiva.wordpress.com/2019/08/06/soap-introducao/>.
Acesso em: 18 mar. 2024.



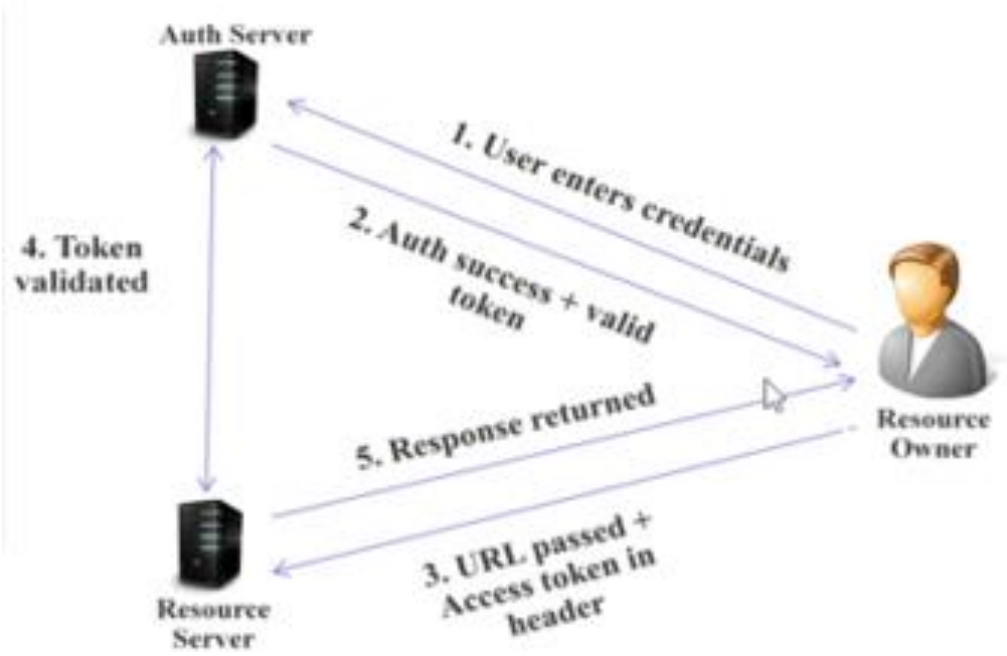
Fonte: Linkedin.
Disponível em: <https://www.linkedin.com/pulse/soap-simple-object-access-protocol-danuka-hettiarachchi-cxxoc/?trk=public_post_main-feed-card_feed-article-contente>.
Acesso em: 18 mar. 2024.

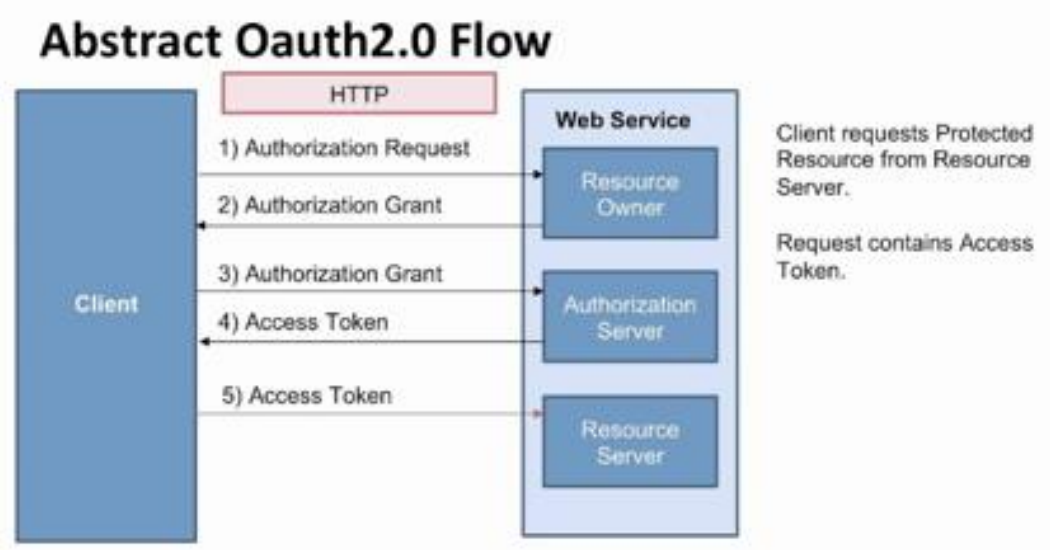
SAML E SOAP

- Fluxo do SOAP:
  - O aplicativo cliente cria uma mensagem SOAP com a solicitação/dados encapsulados;
  - Esta mensagem é enviada para o serviço;
  - O serviço recebe a mensagem SOAP, extrai os dados do corpo (Body) da mensagem e processa a solicitação.
  - O serviço gera resposta em formato SOAP e envia de volta ao cliente;
  - O cliente recebe, extrai os dados e processa a resposta conforme necessário

RESTFUL OAUTH

- É um protocolo de autorização.
- Permite que um aplicativo de terceiro acesse recursos de um usuário, sem a necessidade de compartilhar suas credenciais de autenticação.
- Funcionamento do OAuth:
  - 1. Componentes do OAuth:
    - Cliente (Client);
    - Proprietário dos recursos (Resource Owner);
    - Servidor de autorização (Authorization Server);
    - Servidor de recursos (Resource Server).





Fonte: Youtube.
Disponível em: <https://www.youtube.com/watch?app=desktop&v=_-qpXT8qiB0>.
Acesso em: 18 mar. 2024.

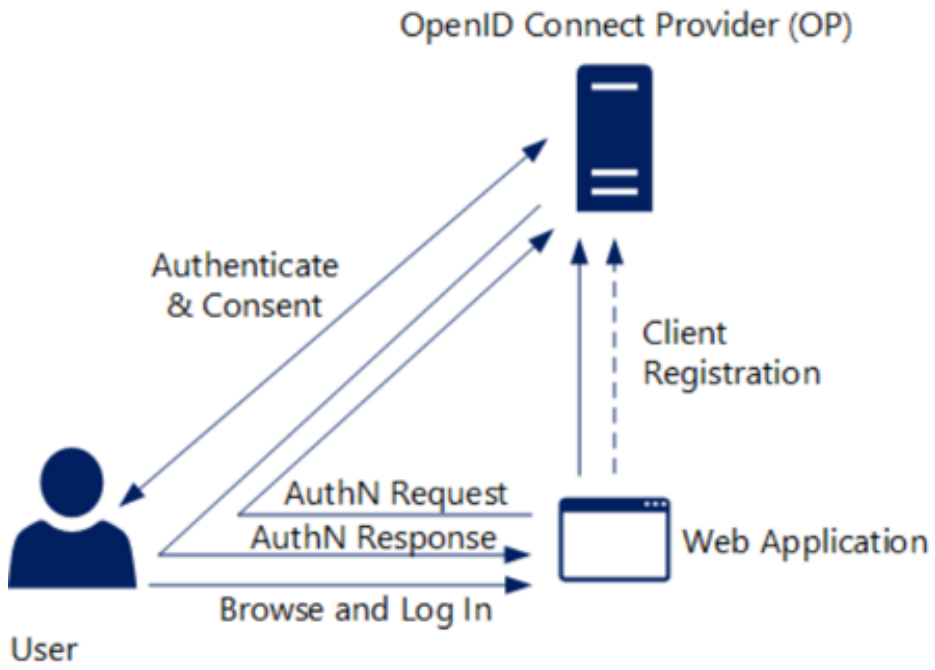
RESTFUL OAUTH

- 2. Registro do cliente:
- 3. Fluxos OAuth;
- 4. Fluxo de autorização de código (Authorization Code Flow);
- 5. Token de acesso;
- 6. Intercâmbio do código por um Token de acesso;
- 7. Acesso a recursos protegidos;
- 8. Escopo;
- 9. Renovação de tokens.

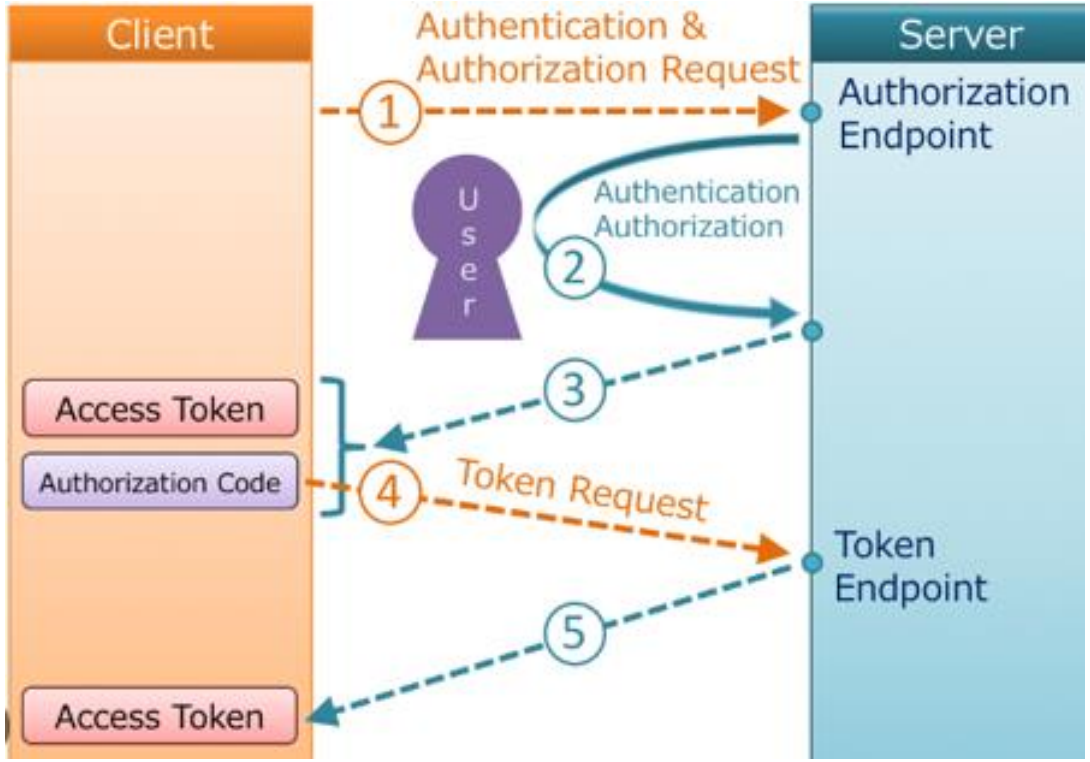
OPENID CONNECT (OIDC)

- É um protocolo de autenticação e autorização baseado no OAuth 2.0.
- Etapas do funcionamento:

1. Atores envolvidos:
   - Provedor de Identidade (IdP);
   - Cliente;
   - Usuário final.
2. Registro do cliente;
3. Autenticação do usuário;
4. Emissão do Token de identificação;



Fonte: Subscription.
Disponível em: <https://subscription.packtpub.com/book/data/9781789132304/6/ch06lvl1sec45/openid-connect-oidc>.
Acesso em: 18 mar. 2024.



Fonte: Lins de Vasconcellos.
Disponível em: <https://www.linsdevasconcellos.org.br/integrate-and-develop-oauth-v2-api-and-rest-api-pp-6DNlO4sp>.
Acesso em: 18 mar. 2024.

OPENID CONNECT (OIDC)

- 5. Redirecionamento de volta ao cliente;
- 6. Verificação do Token de identificação;
- 7. Autorização adicional (opcional);
- 8. Solicitação de Token de acesso;
- 9. Acesso a recursos protegidos;
- 10. Renovação e expiração de Tokens;
- 11. Segurança;
- 12. Compartilhamento de informações do usuário.

5

HACKERS DO BEM_

Módulo 05

Gerenciamento de Identidades e Contas

Aula 04

Políticas de Pessoal

Softex SENAI RNP MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Introdução

Nesta aula, você conhecerá os seguintes assuntos:

- Uso de dispositivos pessoais no trabalho;
- Técnicas de treinamento pessoal;
- Política de mesa limpa;
- Campanhas de esclarecimento de *phishing*;
- Conceitos de Shadow IT.

Aula 04

Políticas de Pessoal

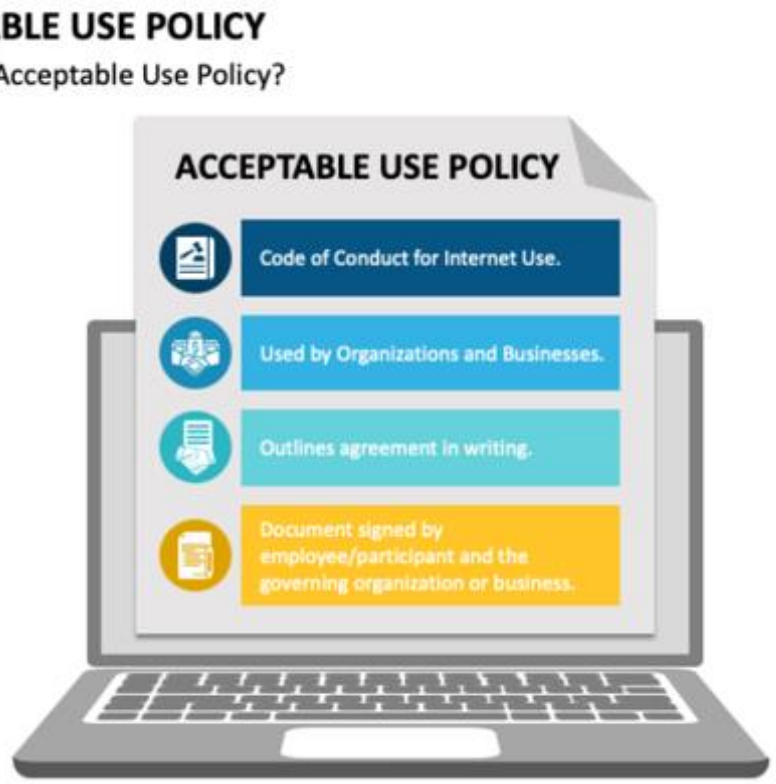
Política de Conduta

POLÍTICA DE CONDUTA

- Refere-se ao conjunto de diretrizes, normas e regras forjados pela organização;
- Visa orientar o comportamento das equipes quanto à segurança das informações e sistemas de tecnologia da empresa.
- Promove a cultura organizacional que prioriza a confidencialidade, integridade e disponibilidade dos ativos de informação.

POLÍTICA DE USO ACEITÁVEL (ACCEPTABLE USE POLICY)

- É a política definida pela organização que regulamenta o uso de recursos de tecnologia e comunicação pelos seus colaboradores.
- Conteúdo da Política:
  - 1. Escopo e objetivos da política;
  - 2. Responsabilidades dos usuários;
  - 3. Restrições e proibições.



Fonte: Tech Target.
Disponível em: <https://www.techtarget.com/whatis/definition/acceptable-use-policy-AUP>.
Acesso em: 18 mar. 2024.

POLÍTICA DE USO ACEITÁVEL (ACCEPTABLE USE POLICY)

- Segurança da informação;
- Monitoramento e auditoria;
- Consequências do não cumprimento;
- Treinamento e conscientização;
- Revisão e atualização;
- Assinatura e aceitação;
- Apoio da alta administração.

USO DE DISPOSITIVOS DE PROPRIEDADE PESSOAL NO AMBIENTE DE TRABALHO

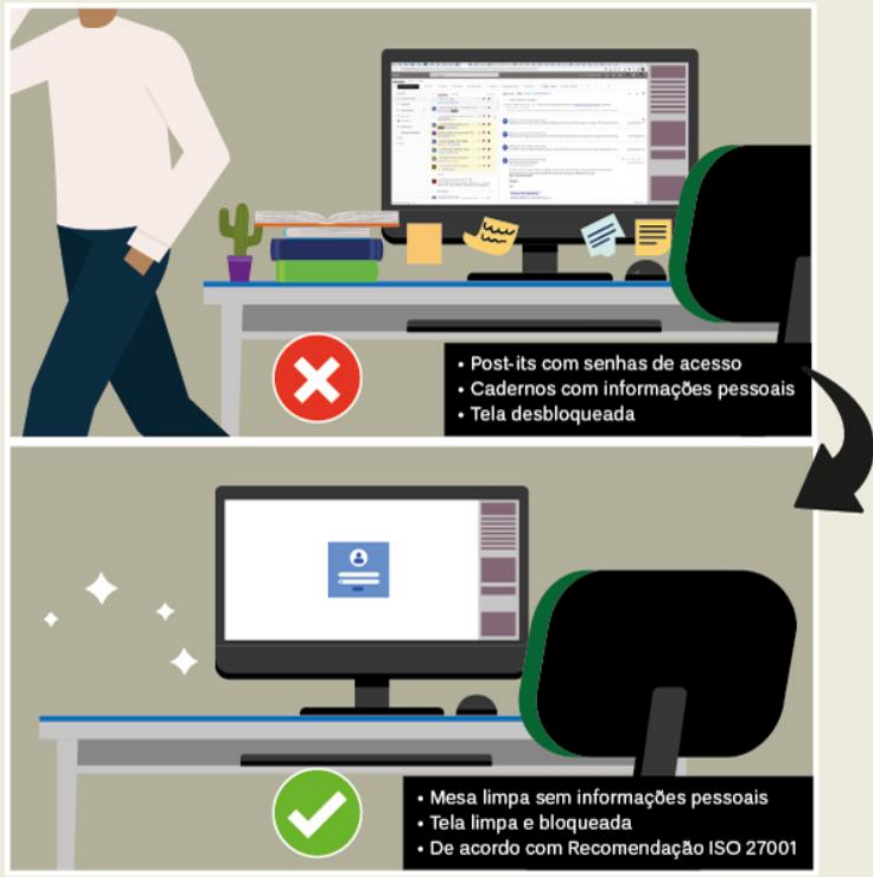
- Regulamentado nas Políticas e Práticas da organização, refere-se ao uso de dispositivos pessoais pelos funcionários no ambiente de trabalho.
- Etapas a serem tratadas pelas práticas:
  1. Escopo e objetivo;
  2. Permissão e registro;
  3. Segurança da informação;
  4. Acesso à rede corporativa;
  5. Política de BYOD (Bring Your Own Device);
  6. Avaliação de riscos.

SHADOW IT

- Trata-se do uso de recursos tecnológicos por funcionários em uma organização, sem autorização.
- Etapas da Política de Pessoal para Shadow IT:
  - 1. Identificação de uso não autorizado;
  - 2. Consequências e educação;
  - 3. Avaliação de riscos;
  - 4. Autorização e supervisão;
  - 5. Comunicação e treinamento;
  - 6. Monitoramento contínuo.

Fonte: Wallarm[1].

[1]Disponível em: <https://www.wallarm.com/what/shadow-it> Acesso em: 18 mar. 2024.



Fonte: Noticias Unb.
Disponível em: <https://noticias.unb.br/76-institucional/6354-sti-da-dicas-para-protecao-de-dados-na-rede>.
Acesso em: 18 mar. 2024.

POLÍTICA DE MESA LIMPA

- Refere-se às políticas de segurança que atuam para minimizar o risco de acesso a informações depositadas nos locais de trabalho.
- Etapas da Política de Mesa Limpa:
  - Remoção de documentos e dispositivos;
  - Armazenamento seguro;
  - Limpeza diária;
  - Sensibilização e treinamento;
  - Monitoramento e conformidade.