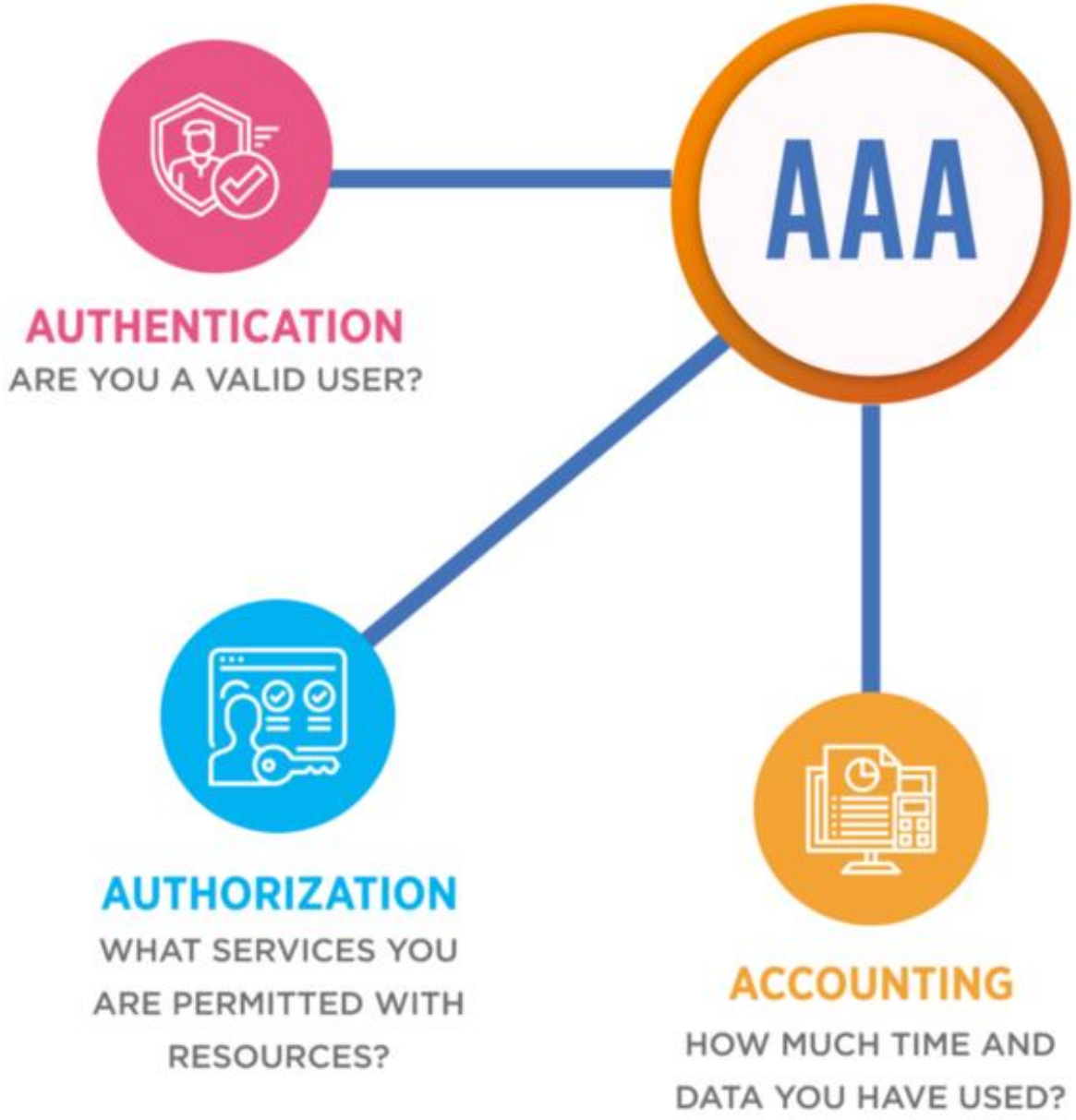
Controle de Acessos

Conceitos AAA

- O controle de acesso é um dos pilares da segurança da informação, responsável por garantir que apenas usuários devidamente identificados e autorizados possam acessar recursos e informações dentro de um sistema ou organização. O modelo **AAA** — *Autenticação, Autorização e Auditoria* — estrutura essa lógica de maneira sistemática:



Autenticação

- Processo de **verificação de identidade**. Seu objetivo é confirmar que o usuário é realmente quem diz ser. Exemplos comuns incluem o uso de senhas, tokens, cartões inteligentes, certificados digitais, ou fatores biométricos (impressão digital, reconhecimento facial, íris, etc.). Sistemas modernos frequentemente aplicam **autenticação multifator (MFA)**, combinando algo que o usuário *sabe* (senha), algo que ele *possui* (token, celular) e algo que ele *é* (biometria).

Autorização

- Após autenticado, o usuário precisa ser **autorizado** para acessar determinados recursos. A autorização define **o que ele pode ou não fazer —** por exemplo, ler um arquivo, modificar dados ou administrar um sistema. Essa decisão baseia-se em políticas internas de controle de acesso, frequentemente associadas ao cargo ou perfil de cada usuário.

Auditoria

- A auditoria é o **registro e análise das ações** realizadas pelos usuários autenticados e autorizados. Serve tanto para fins de **conformidade** (com normas como ISO 27001, LGPD, HIPAA) quanto para **investigação de incidentes**. Logs de auditoria confiáveis permitem identificar acessos indevidos, alterações críticas ou tentativas de violação.

Modelos de Controle de Acesso

- Os modelos de controle de acesso definem **como as permissões são atribuídas e gerenciadas**. A escolha do modelo depende do contexto organizacional, do nível de risco e da complexidade da infraestrutura.
  - **Discricionário (DAC – Discretionary Access Control)**
  - **Baseado em Papéis (RBAC – Role-Based Access Control)**
  - **Baseado em Atributos (ABAC – Attribute-Based Access Control)**

Modelo Discricionário (DAC – Discretionary Access Control)

- O controle de acesso é **determinado pelo proprietário do recurso**. Cada usuário tem liberdade para definir quem pode acessar seus arquivos, pastas ou sistemas. É comum em sistemas operacionais como Windows e UNIX, onde o dono de um arquivo decide as permissões (leitura, escrita, execução). Apesar da flexibilidade, o DAC apresenta riscos: usuários podem conceder permissões excessivas, o que favorece vazamentos e propagação de malware.
- **Características principais:**
  - Controle descentralizado.
  - Fácil de administrar em pequenos ambientes.
  - Vulnerável a falhas humanas ou concessões indevidas.

Modelo Baseado em Papéis (RBAC – Role-Based Access Control)

- As permissões são associadas a **funções (roles)** dentro da organização, e não diretamente aos usuários. Um usuário herda as permissões do papel que ocupa — por exemplo, "Analista Financeiro", "Administrador de Sistema", "Usuário Padrão". O RBAC promove **padronização e consistência**, reduzindo erros administrativos.
- **Exemplo prático:**
  - Papel *Gerente*: acesso total aos relatórios financeiros.
  - Papel *Analista*: acesso somente para leitura.
  - Papel *Estagiário*: acesso restrito a dados não confidenciais.
- **Vantagens:**
  - Escalabilidade e facilidade de manutenção.
  - Alinhamento direto com a estrutura organizacional.
  - Cumprimento facilitado de normas e auditorias.

Modelo Baseado em Atributos (ABAC – Attribute-Based Access Control)

- Modelo mais flexível e dinâmico. As decisões de acesso são baseadas em **atributos** do usuário, do recurso e do contexto da requisição. Esses atributos podem incluir horário, localização, nível de classificação da informação, dispositivo de origem, entre outros.
- **Exemplo:**
  - "Permitir acesso ao sistema financeiro **somente** se o usuário estiver no grupo *Financeiro* **e** conectado de um dispositivo corporativo, **durante o horário comercial**."
- O ABAC é amplamente adotado em ambientes de **computação em nuvem**, **microserviços** e **infraestruturas zero trust**, pois permite políticas adaptativas e centralizadas.

Controle Físico vs. Controle Lógico

- **Controle Físico**
  - Refere-se a mecanismos que **limitam o acesso físico** a ambientes ou equipamentos críticos, como data centers, salas de servidores e áreas restritas. Incluem:
    - Fechaduras eletrônicas.
    - Cartões de proximidade.
    - Biometria de acesso.
    - Câmeras e monitoramento (CCTV).
    - Guardas e barreiras físicas.
  - O objetivo é **proteger os ativos tangíveis**, evitando danos, roubo de hardware ou instalação de dispositivos maliciosos (como keyloggers e sniffers físicos).

Controle Físico vs. Controle Lógico

- **Controle Lógico**
  - Abrange os mecanismos **digitais** de proteção e restrição de acesso a sistemas, redes e dados. Incluem:
    - de identidades (IAM).
  - Os controles físicos e lógicos são **complementares** e devem operar de forma integrada dentro de um sistema de segurança.

Práticas de Segurança

- **Senhas**
- **MFA**
- **Biometria**

Senhas

- Ainda são o método mais comum de autenticação, mas também o mais vulnerável. Boas práticas incluem:
  - Utilizar senhas longas e complexas (combinação de letras, números e símbolos).
  - Evitar reutilização entre diferentes sistemas.
  - Alterações periódicas com base em políticas de risco.
  - Armazenamento seguro com hashing e salting (ex: bcrypt, Argon2).

Autenticação Multifator (MFA)

- Combina **dois ou mais fatores independentes** para confirmar a identidade. Essa camada adicional reduz significativamente o risco de invasão mesmo em caso de comprometimento de senhas. Fatores comuns:
  - **Conhecimento:** algo que o usuário sabe (senha, PIN).
  - **Posse:** algo que o usuário tem (token, smartphone, cartão).
  - **Inerência:** algo que o usuário é (biometria).

Biometria

- Baseia-se em características físicas ou comportamentais únicas. Exemplos incluem impressão digital, reconhecimento facial, voz e íris. Apesar da conveniência, a biometria requer **cuidados adicionais de privacidade e proteção de dados**, uma vez que não pode ser alterada como uma senha.

Políticas de Acesso em Empresas

- Empresas maduras em segurança da informação implementam **políticas formais de controle de acesso**, definindo diretrizes, responsabilidades e exceções. Essas políticas devem:
  - Basear-se no **princípio do menor privilégio** (acesso mínimo necessário).
  - Garantir **segregação de funções** (evitar concentração de poderes).
  - Estabelecer **procedimentos de revisão periódica** de acessos.
  - Definir **processos de provisionamento e desativação** de contas.
  - Registrar e monitorar todas as alterações críticas de acesso.
- As políticas são fundamentais para conformidade com normas de segurança e legislações como **LGPD**, **ISO/IEC 27001**, **NIST 800-53**, entre outras.

Atividade Prática – Perfis de Acesso no ERP Integrado ao CRM

- Seu grupo está projetando um **ERP (Enterprise Resource Planning)** integrado a um **CRM (Customer Relationship Management)**. O objetivo é simular o controle de acesso e a definição de perfis de usuários considerando os princípios e modelos estudados.
- O sistema ERP gerencia módulos como **Financeiro**, **Recursos Humanos**, **Estoque** e **Vendas**, enquanto o CRM lida com **Gestão de Clientes**, **Propostas Comerciais** e **Pós-venda**.
- Vocês devem definir **perfis de acesso baseados em papéis e atributos**, considerando os seguintes aspectos:
  - Quais usuários terão **acesso total**.
  - Quais terão **acesso restrito a determinados módulos**.
  - Que políticas devem ser aplicadas em caso de **integração entre ERP e CRM.**
  - Como implementar o **princípio do menor privilégio** em cada módulo.
  - Quais atributos adicionais poderiam ser utilizados em um **modelo ABAC**.
  - Que mecanismos de **auditoria** devem ser aplicados para registrar ações críticas, como exclusão de registros financeiros ou exportação de dados de clientes.