

CST Desenvolvimento de Software Multiplataforma (DSM)

**Disciplina: ISG-022 – SEGURANÇA NO
DESENVOLVIMENTO DE APLICAÇÕES (SDA)**

**Tópico 03: CONTROLES DE
ACESSO E AUTORIZAÇÕES**

SUMÁRIO

- 1. Objetivo da Aula – Tópico da Ementa**
- 2. Requisitos da Segurança da Informação**
- 3. Controles de Acesso e Autorização**
- 4. Políticas de Segurança da Informação**
- 5. Modelos e Mecanismos de Controles de Acesso e Autorização**

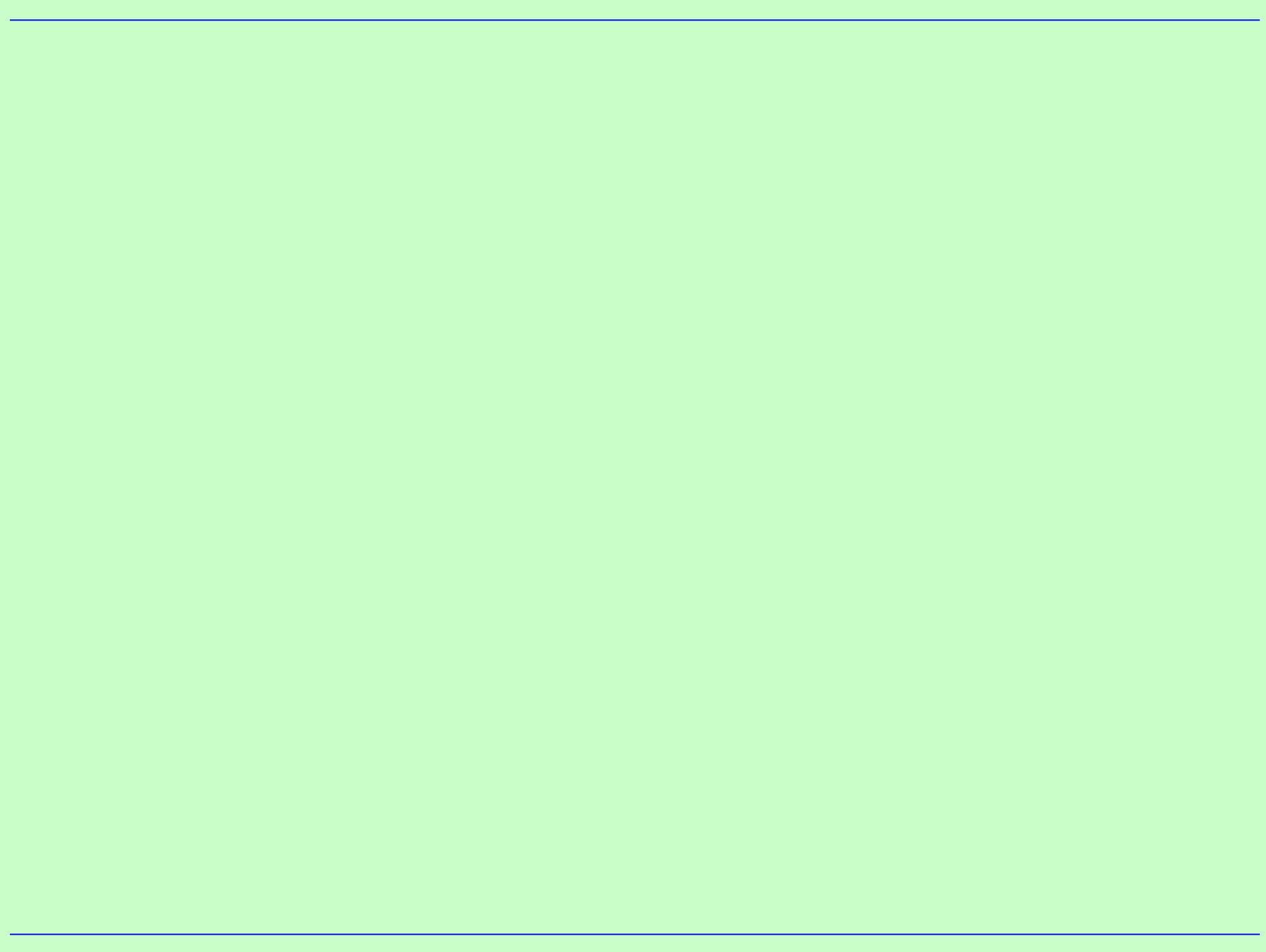
1. OBJETIVO E EMENTA

➤ **Objetivo da Aula**

Proporcionar uma compreensão abrangente sobre os princípios de Controles de Acesso e Autorização, explorando as políticas de segurança, modelos e mecanismos de controle.

➤ **Tópico da Ementa**

Conceitos fundamentais do pilar de segurança: confidencialidade, integridade, disponibilidade e autenticidade.



2. REQUISITOS DA SEGURANÇA DA INFORMAÇÃO

❖ REQUISITOS GERAIS DE SI (CID)

- A segurança da informação visa **proteger dados** contra acessos não autorizados, alterações indevidas, divulgação, destruição ou perda, garantindo os **Requisitos de**

1. Confidencialidade

2. Integridade

3. Disponibilidade

2. REQUISITOS DA SEGURANÇA DA INFORMAÇÃO

1. CONFIDENCIALIDADE

- Garantia de que a informação seja **acessível** apenas por **pessoas autorizadas**.

Os **controles** de acesso e autorização são essenciais para **assegurar** que somente **usuários legítimos** tenham **acesso** às informações sensíveis, **evitando vazamentos** ou **acessos indevidos**.

2. REQUISITOS DA SEGURANÇA DA INFORMAÇÃO

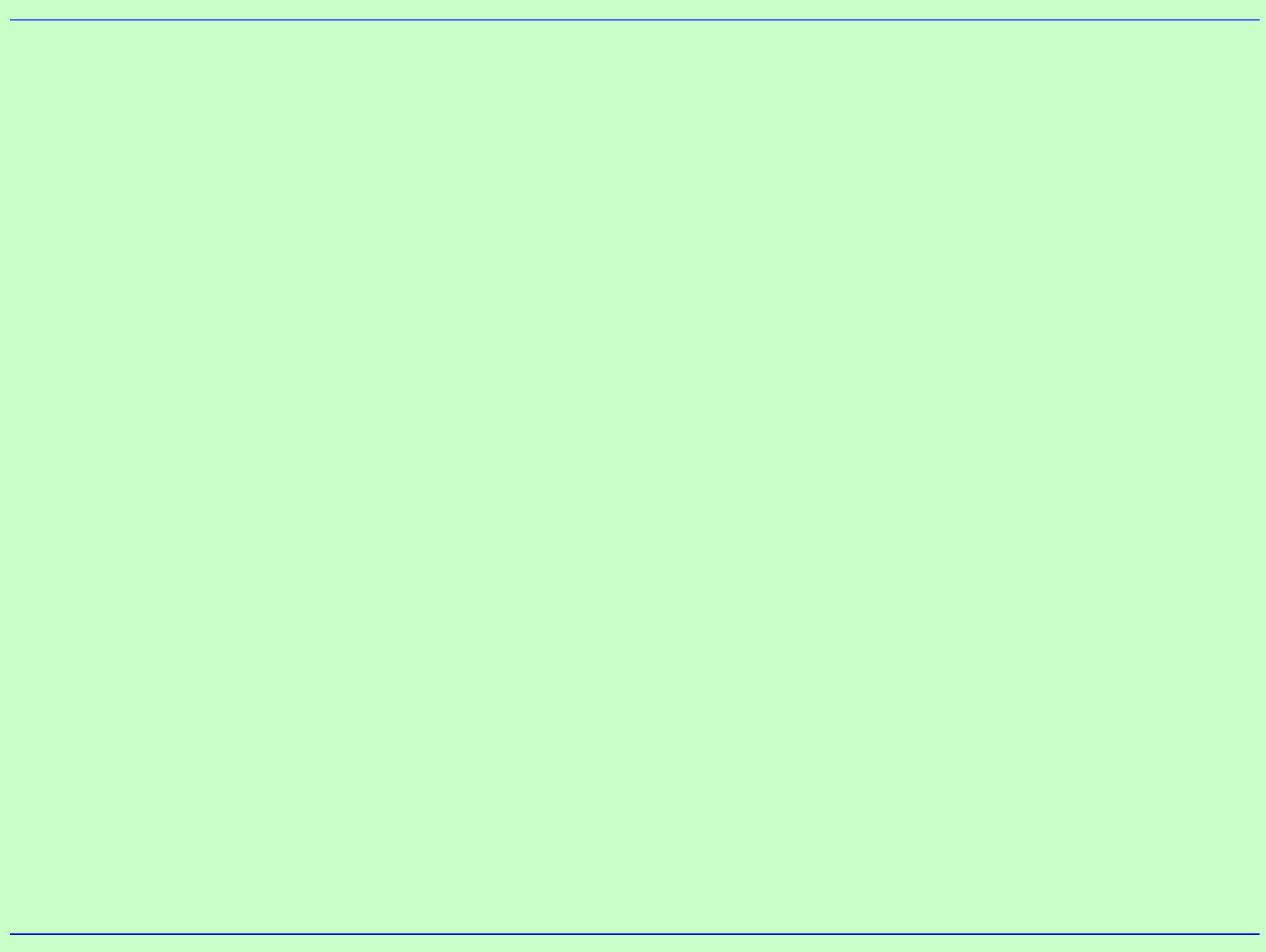
2. INTEGRIDADE

- **Compliance** é um processo de negócio com o objetivo de **garantir** que uma organização esteja em **conformidade** ou em **aderência** com as políticas, diretrizes, regulamentos, legislações, procedimentos, normas e padrões estabelecidos para a realização das suas atividades, **cumprindo** e **fazendo cumprir** todas as **regras internas** e **externas** do **negócio**.

2. REQUISITOS DA SEGURANÇA DA INFORMAÇÃO

3. DISPONIBILIDADE

- **Compliance** é um processo de negócio com o objetivo de **garantir** que uma organização esteja em **conformidade** ou em **aderência** com as políticas, diretrizes, regulamentos, legislações, procedimentos, normas e padrões estabelecidos para a realização das suas atividades, **cumprindo** e **fazendo cumprir** todas as **regras internas** e **externas** do **negócio**.



3. CONTROLES DE ACESSO E AUTORIZAÇÃO

- Os **Controles de Acesso e Autorização** envolvem:
 - 1. Prevenção de Acessos NÃO Autorizados**
 - 2. Gerenciamento de Identidades**
 - 3. Conformidade Regulatória**

3. CONTROLES DE ACESSO E AUTORIZAÇÃO

1. Prevenção de Acessos NÃO Autorizados

- Os controles de acesso são a **primeira linha de defesa** contra **tentativas não autorizadas** de acessar informações. Eles determinam **quem pode** ou **não acessar** determinados recursos dentro de um sistema, baseando-se em **políticas de segurança** bem definidas.

3. CONTROLES DE ACESSO E AUTORIZAÇÃO

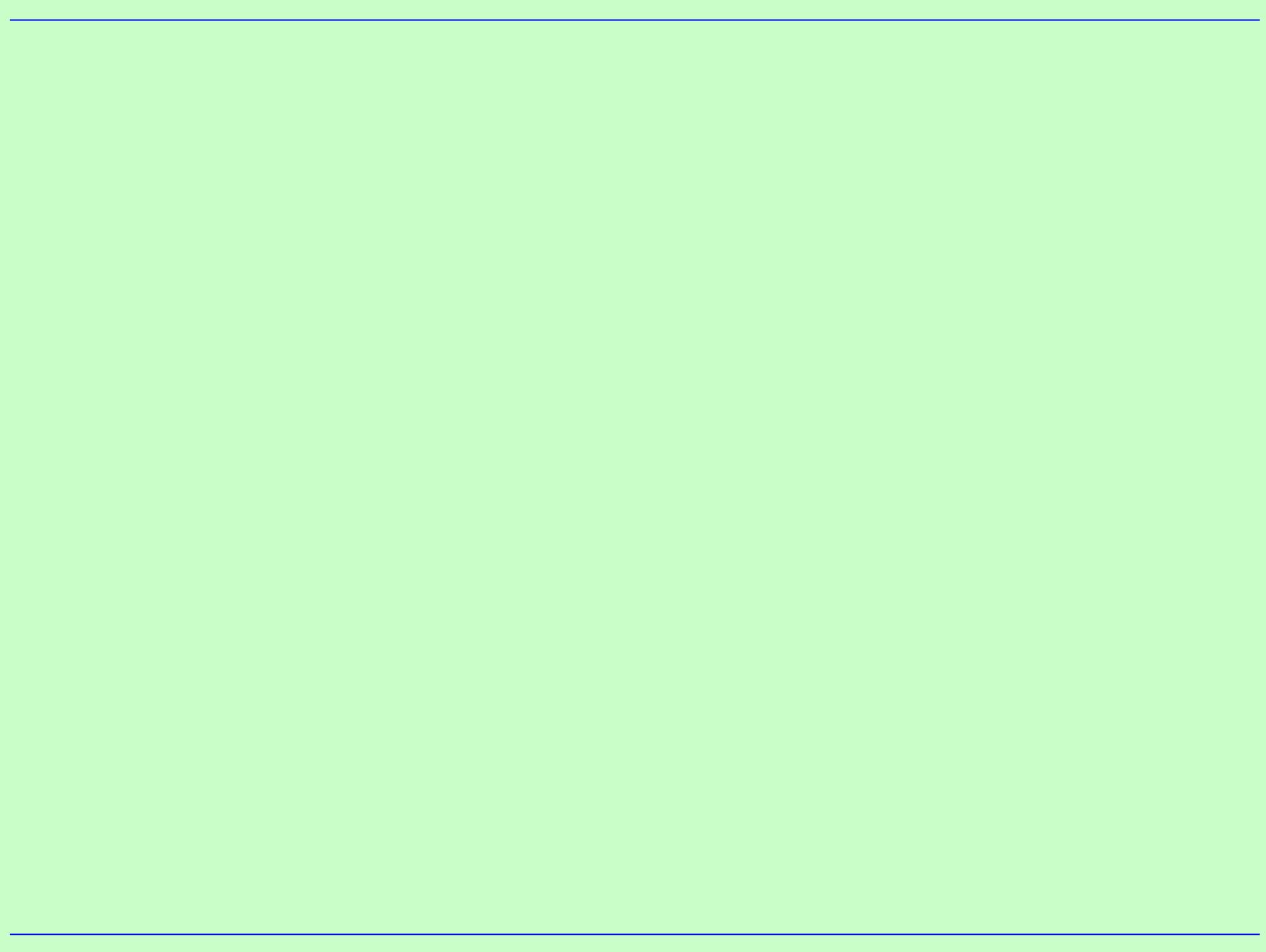
2. Gerenciamento de Identidade

- Os sistemas de controle de acesso garantem, por meio da **autenticação** e da **autorização**, que apenas **usuários autenticados** e com as devidas permissões possam **acessar** os recursos.
Inclui a implementação de **procedimentos seguros** de **login**, **autenticação multifator** e **gestão de senhas**.

3. CONTROLES DE ACESSO E AUTORIZAÇÃO

3. Conformidade Regulatória (Compliance)

- Os **controles de acesso e autorização** ajudam as organizações a **cumprirem** as rigorosas **regulamentações** de proteção de dados, que muitos setores estão sujeitos, tais como: o GDPR na União Europeia e a **LGPD no Brasil**, entre outras.



4. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

➤ Definição: POLÍTICAS DE SEGURANÇA

- Documentos **oficialmente aprovados** que expressam claramente a **posição** de uma **organização** sobre a **segurança da informação**, adaptados às suas **necessidades específicas** e **alinhados** aos **objetivos de negócio**, refletindo os requisitos legais, regulatórios e de mercado. Abrangem vários aspectos, tais como: controles de acesso, gestão de identidades, resposta a incidentes, gestão de vulnerabilidades, criptografia e uso aceitável dos recursos de TI etc.

4. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

➤ IMPORTÂNCIA das Políticas de Segurança

São **fundamentais** para a **proteção dos ativos** de informação de uma organização:

- **Estrutura** para segurança da informação
- **Conformidade** regulatória
- Gestão de **riscos**
- **Cultura** da segurança
- Resposta a **incidentes**
- **Confiança** dos stakeholders

4. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

➤ EXEMPLOS de Políticas de Segurança

- Política de **senhas fortes**
- Política de **controle de acesso**
- Política de **uso aceitável** dos recursos de TI
- Política de **respostas a incidentes**
- Política de **backup e recuperação** de dados
- Política de **segurança física**

4. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

➤ Política de SENHAS FORTES

- **Objetivos:** Garantir que todas as **senhas** criadas sejam **fortes** e resistentes a ataques de força bruta e promover a **educação dos usuários** sobre a importância de senhas fortes.
- **Detalhes:** A política pode especificar **mecanismos** de verificação e **requisitos** de senha forte, como comprimento mínimo da senha, a inclusão de letras maiúsculas e minúsculas, números, e símbolos especiais, além de proibir o uso de senhas previamente violadas ou facilmente adivinháveis.

4. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

➤ Nota: **Ataque de Força Bruta**

- Uma técnica utilizada com o objetivo de descobrir uma senha ou um dado criptografado através da **tentativa sistemática** de todas as **possíveis combinações** de letras, números e símbolos até encontrar a combinação correta.

Não requer conhecimento prévio sobre o sistema alvo, baseando-se puramente no poder computacional e na **persistência**.

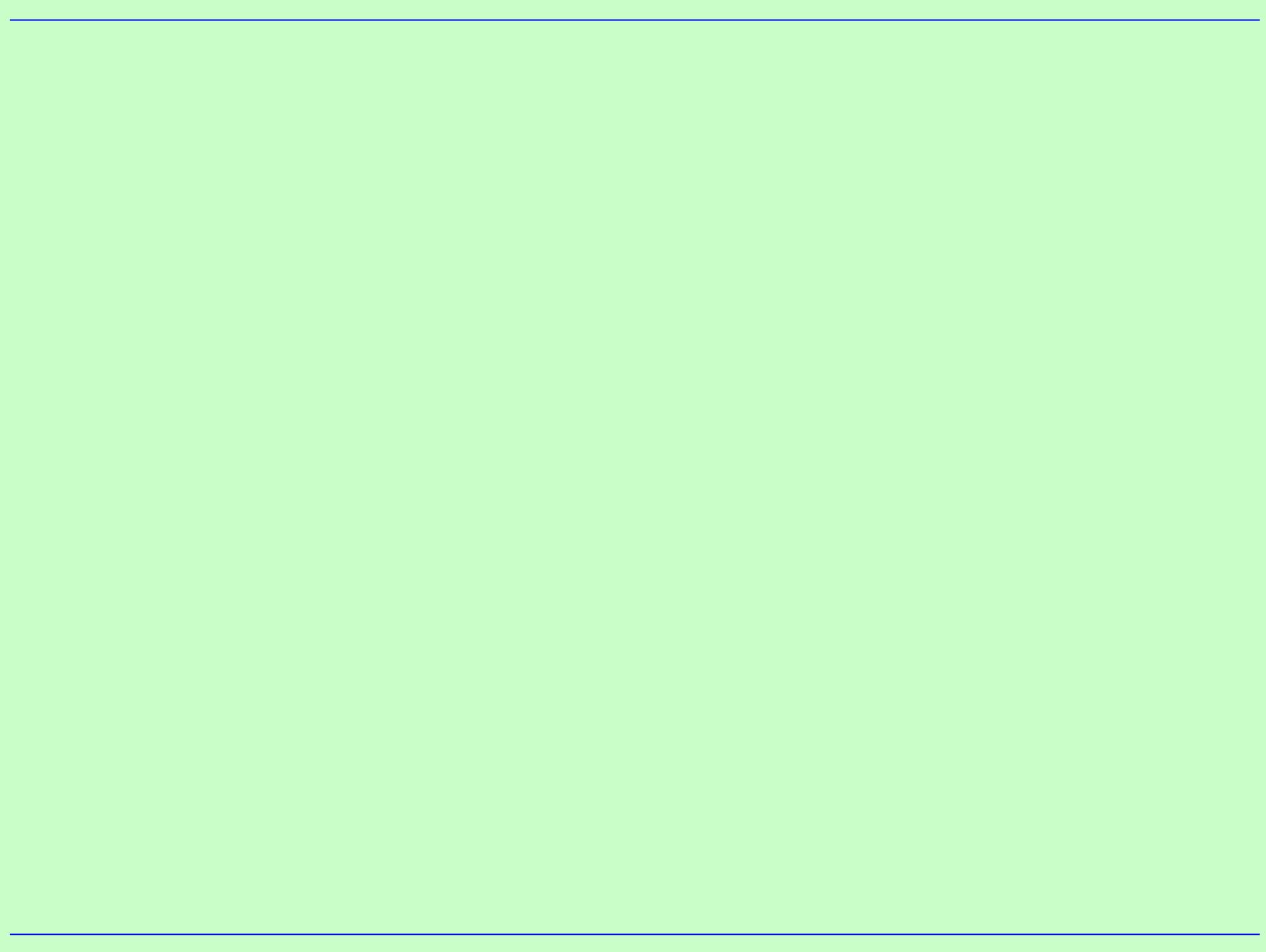
4. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

➤ Política de CONTROLE DE ACESSO

- **Objetivos:** Assegurar que os acessos aos sistemas, aplicações e dados sejam concedidos com **base** nas **funções profissionais** dos usuários, aplicando o princípio do menor privilégio, e possibilitar **auditorias regulares** para garantir que os acessos estejam corretamente alinhados com as funções.
- **Detalhes:** Definir **funções** específicas dentro da organização e os **acessos** necessários para cada uma. Por exemplo, apenas o pessoal de RH deve ter acesso a informações pessoais dos funcionários.

4. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

- Nota: **Princípio do Menor Privilégio**
 - Conceito estabelece que qualquer usuário, programa ou processo deve **operar** usando o conjunto **mínimo de privilégios**, estritamente aqueles necessários, para realizar suas tarefas.
 - O objetivo principal desse princípio, também conhecido como princípio do privilégio mínimo ou princípio de privilégio necessário, é **limitar** o **acesso** e as **permissões** reduzindo a superfície de ataque disponível para agentes maliciosos.



5. MODELOS E MECANISMOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

➤ MODELOS de Controle de Acesso

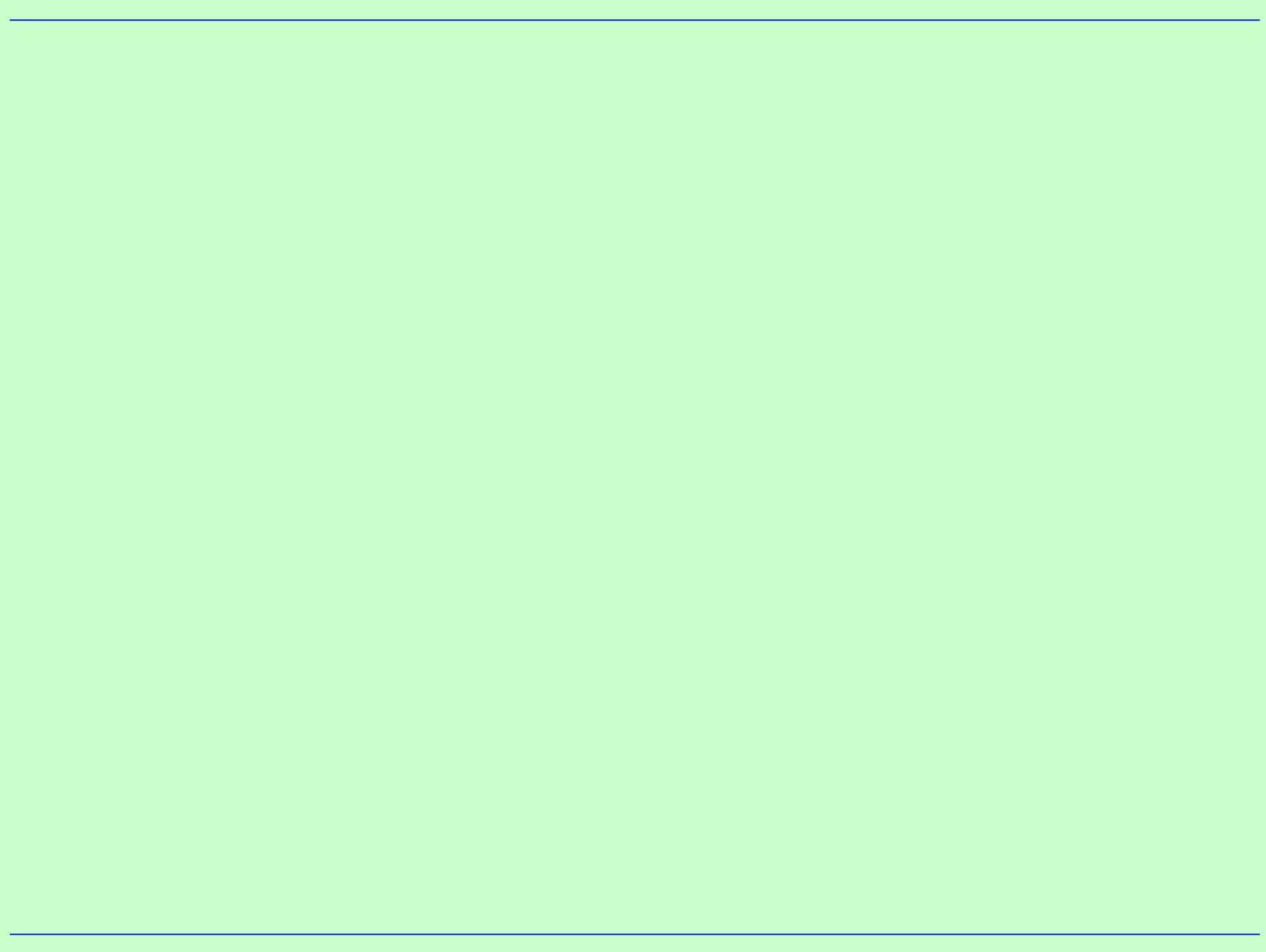
- Os modelos de controle de acesso definem **como** os usuários podem **acessar** diferentes recursos em um sistema. Eles são projetados para **limitar** o **acesso** a arquivos, dados e aplicações a **usuários autorizados**, prevenindo assim vazamentos de dados ou outras formas de comprometimento de segurança.

5. MODELOS E MECANISMOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

➤ MODELOS de Controle de Acesso

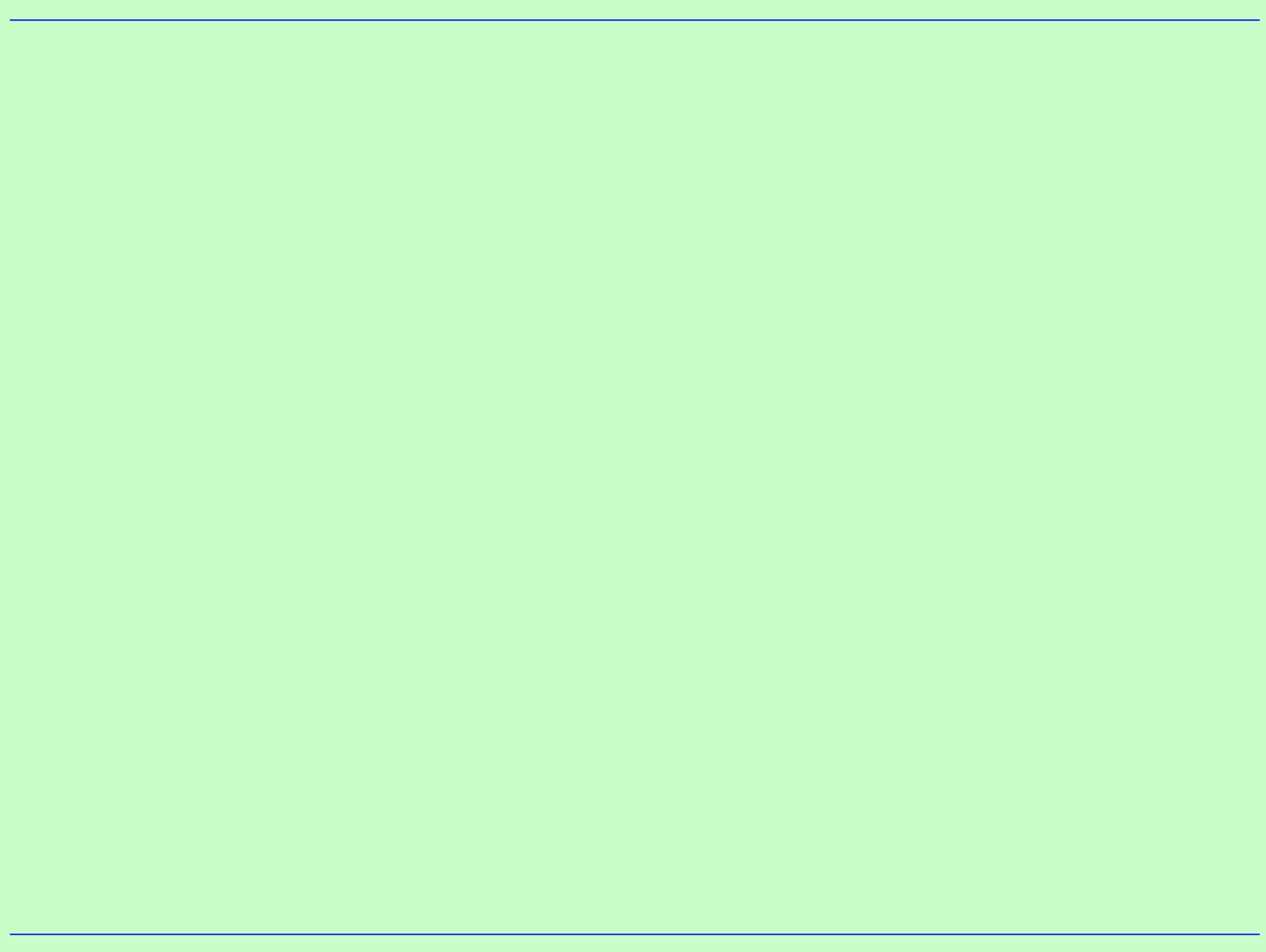
Existem vários modelos de controle de acesso:

- Controle de Acesso Discricionário (**DAC**)
- Controle de Acesso Obrigatório (**MAC**)
- Controle de Acesso Baseado em Atributos (**ABAC**)
- Controle de Acesso Baseado em Papéis (**RBAC**)
- Controle de Acesso Baseado em Políticas (**PBAC**)
- Listas de Controle de Acesso (**ACL**)



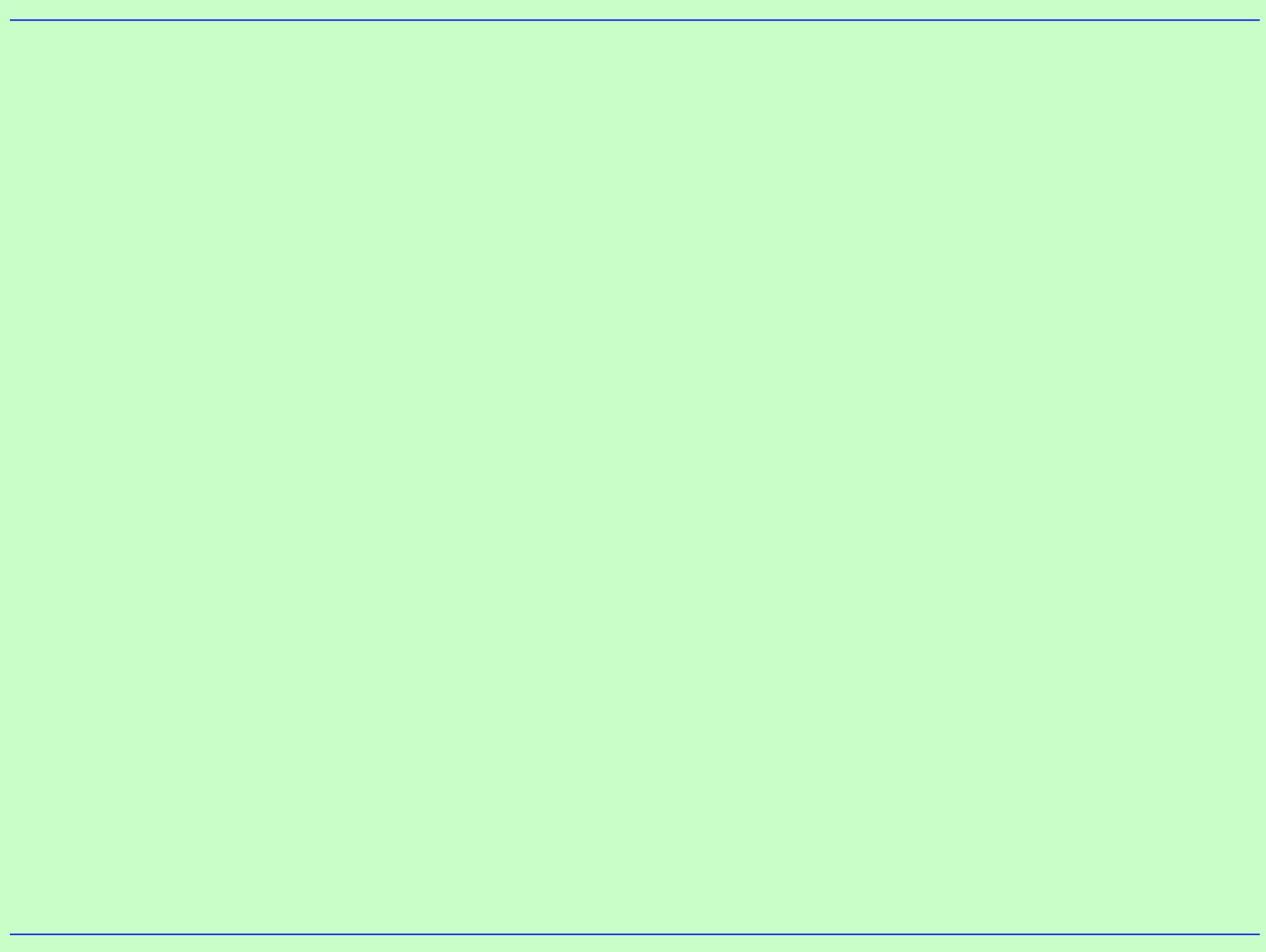
5. MODELOS E MECANISMOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

- Controle de Acesso Discricionário (**DAC**)
- **Discretionary Access Control (DAC)**



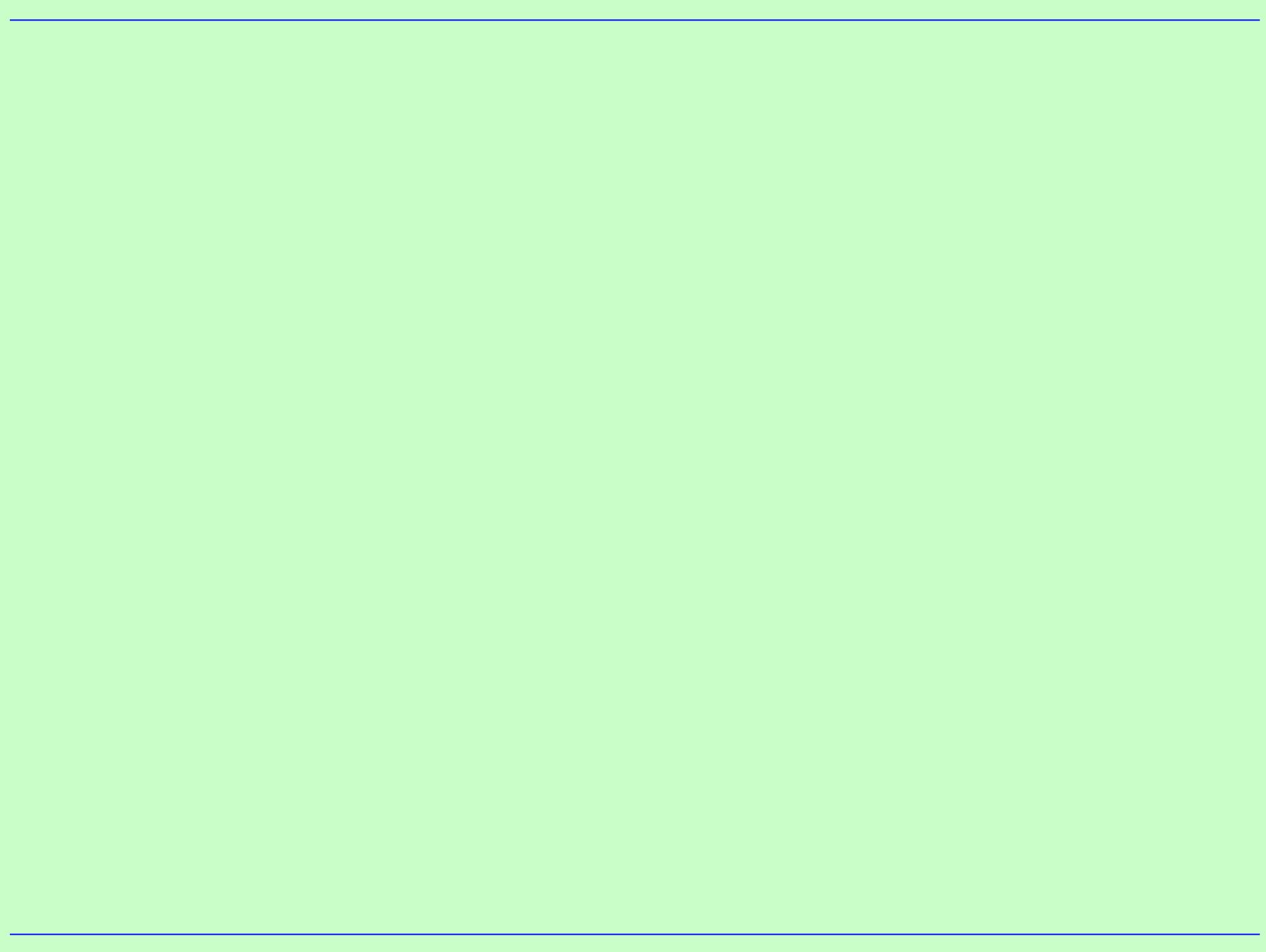
5. MODELOS E MECANISMOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

- Controle de Acesso Obrigatório (**MAC**)
- **Mandatory Access Control (MAC)**



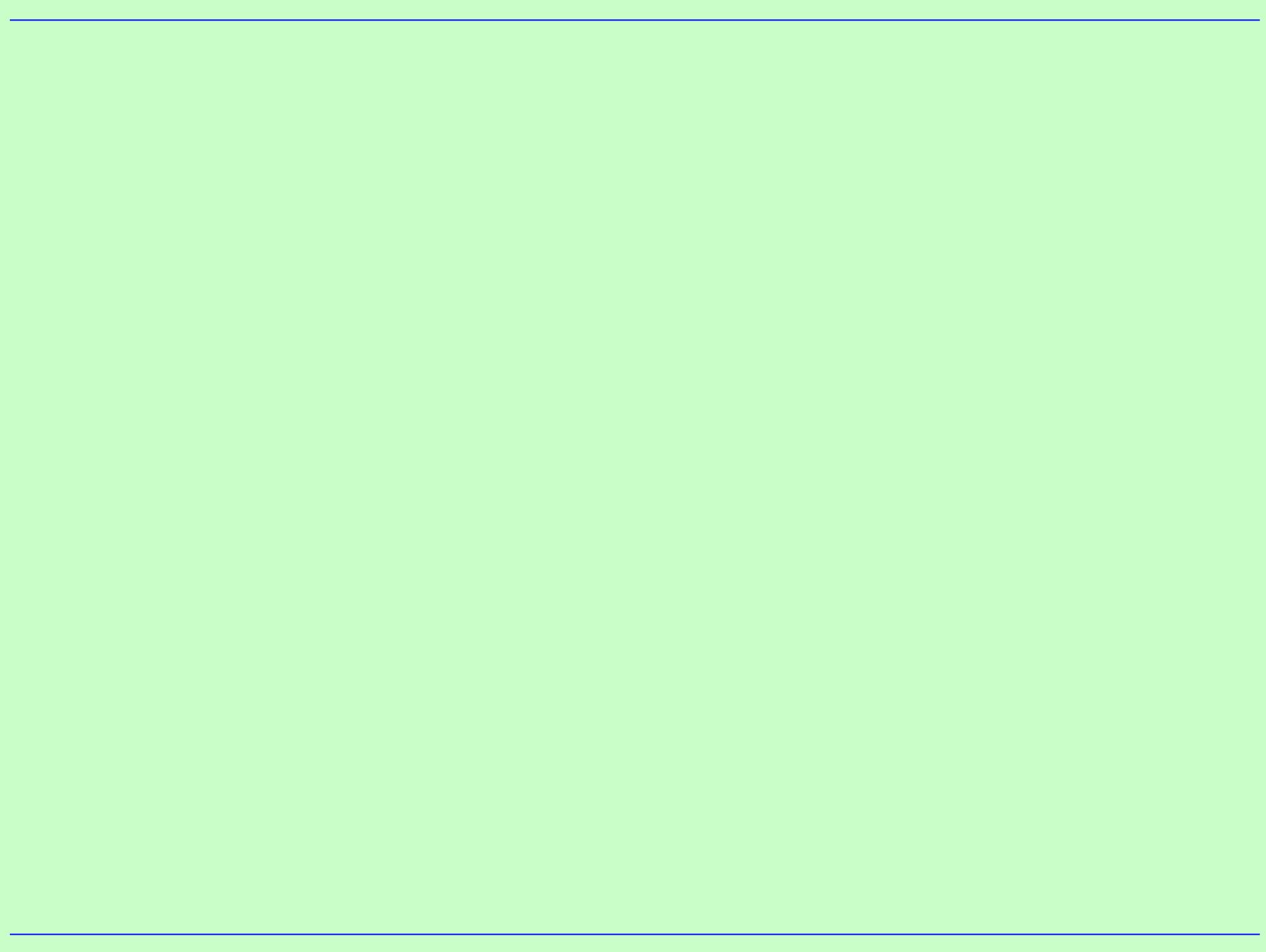
5. MODELOS E MECANISMOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

- Controle de Acesso Baseado em Atributos (**ABAC**)
- **Attribute-Based Access Control (ABAC)**



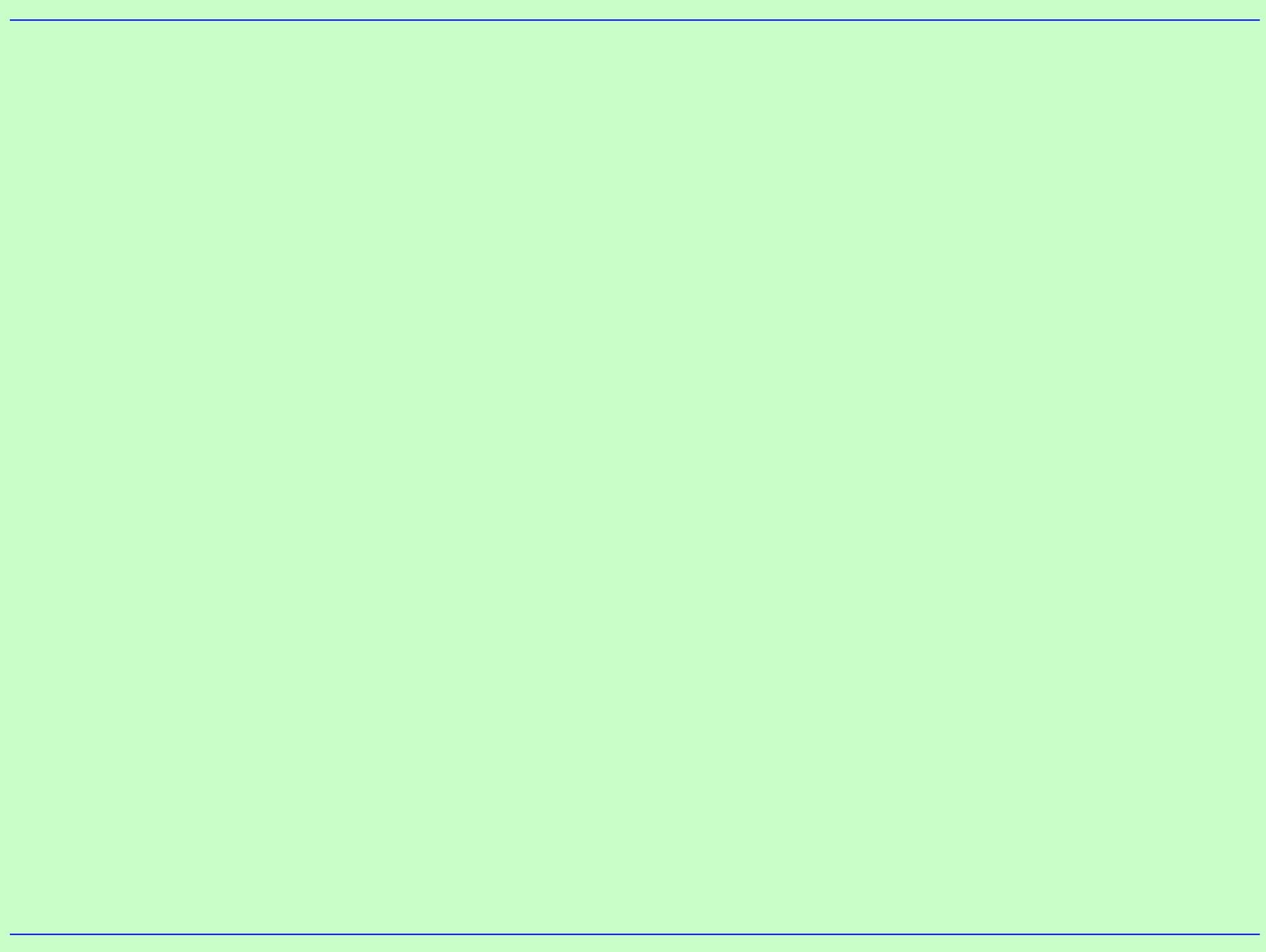
5. MODELOS E MECANISMOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

- Controle de Acesso Baseado em Papéis (**RBAC**)
- **Role-Based Access Control(RBAC)**



5. MODELOS E MECANISMOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

- Controle de Acesso Baseado em Políticas (**PBAC**)
- Policy-Based Access Control(**PBAC**)



5. MODELOS E MECANISMOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO

- Listas de Controle de Acesso (**ACL**)
- Access Control Lists (**ACL**)

CST Desenvolvimento de Software Multiplataforma (DSM)

**Disciplina: ISG-022 – SEGURANÇA NO
DESENVOLVIMENTO DE APLICAÇÕES (SDA)**

**Tópico 03: CONTROLES DE
ACESSO E AUTORIZAÇÕES**