

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**

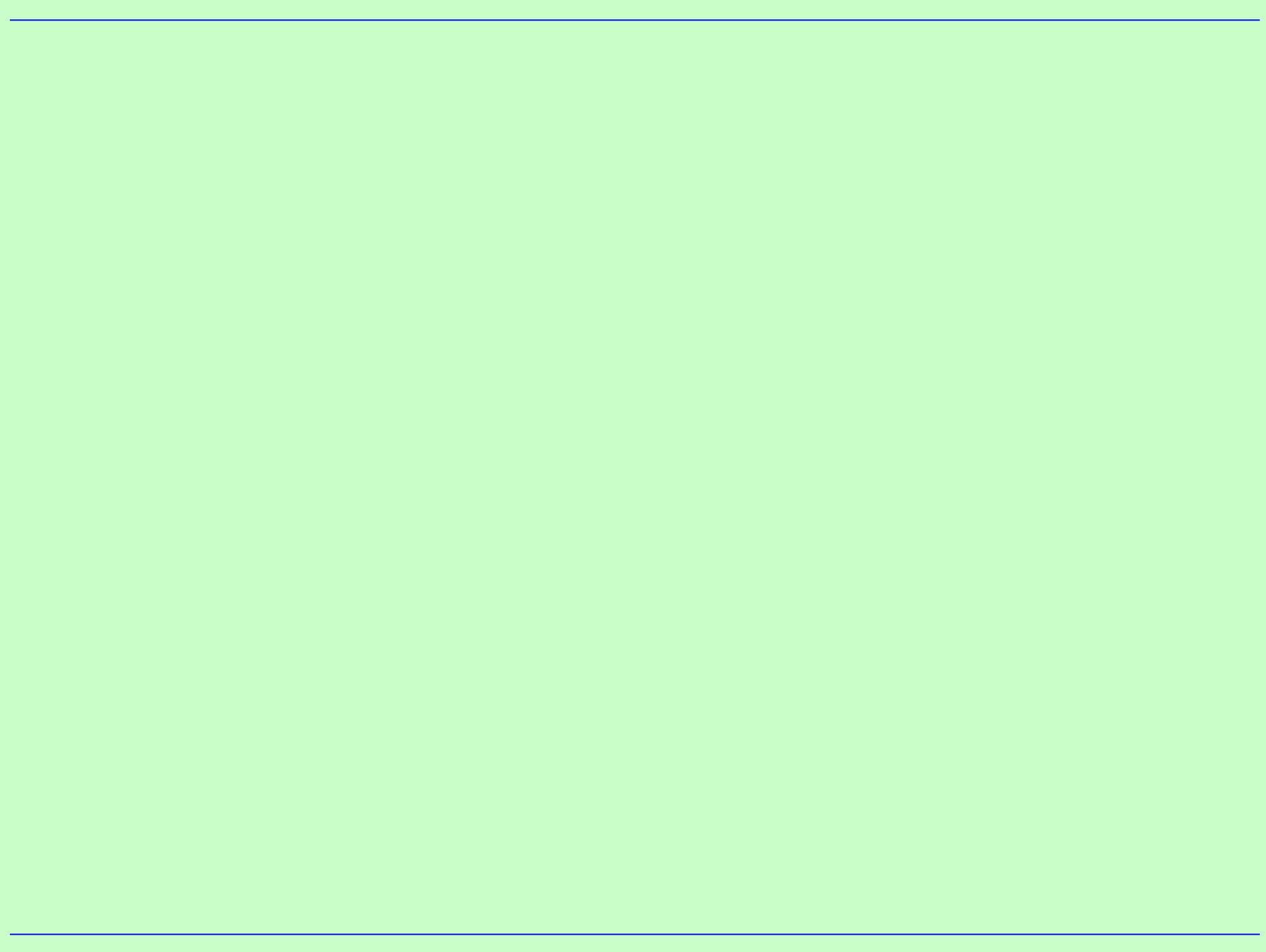
1. OBJETIVO E EMENTA

➤ **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

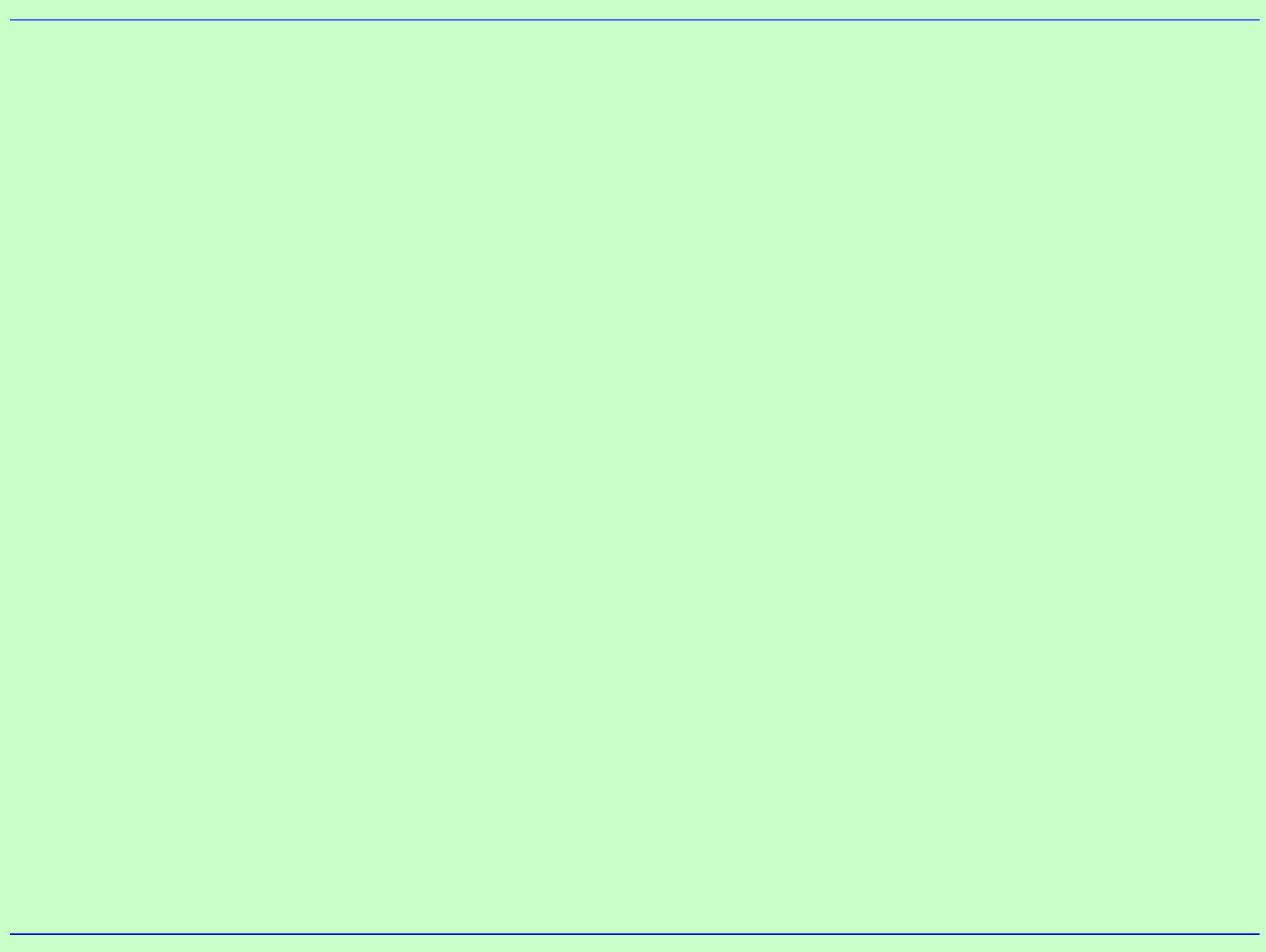
2. INTEGRIDADE

- **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

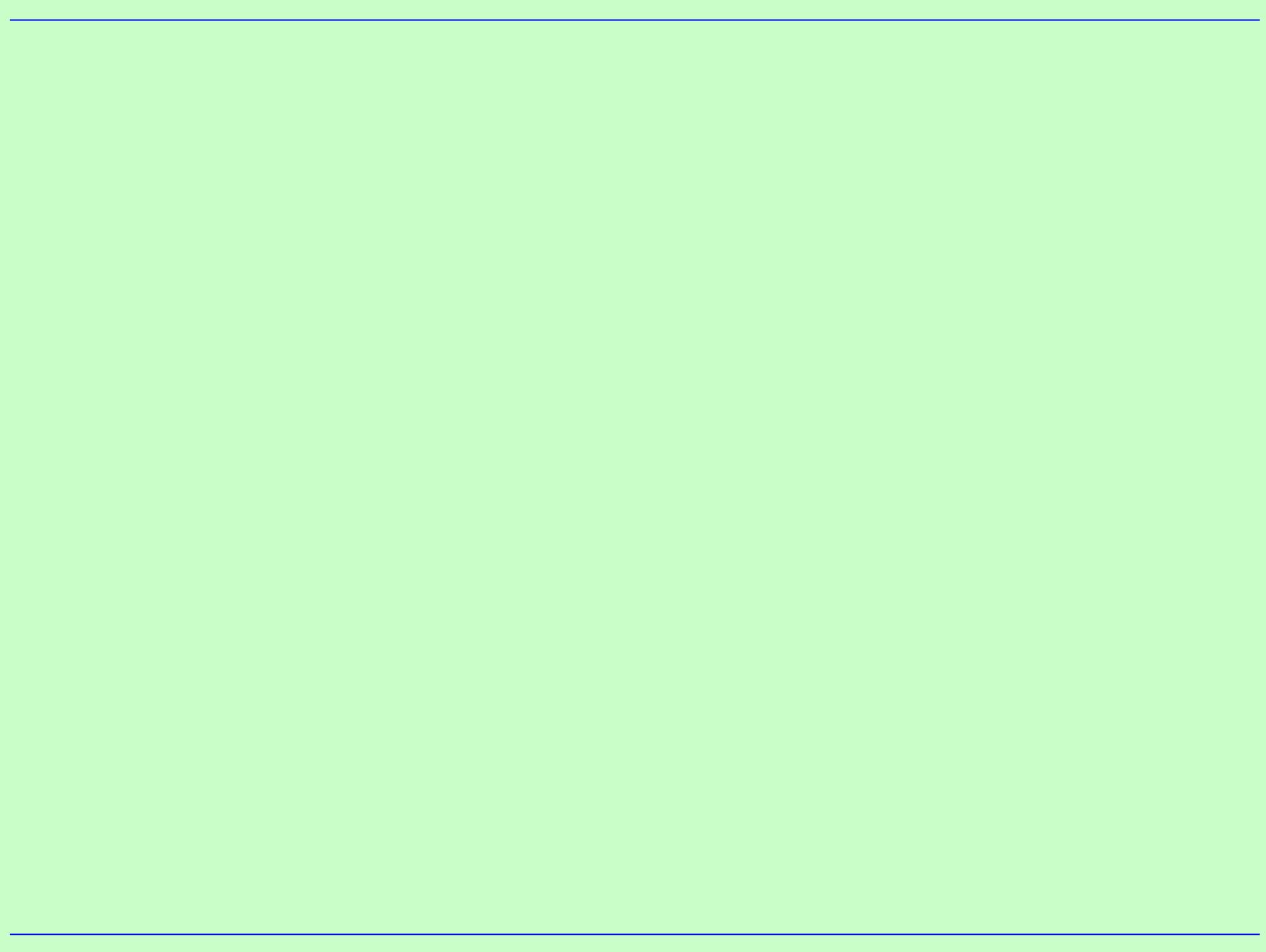
2. Gerenciamento de Identidade

- 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**.

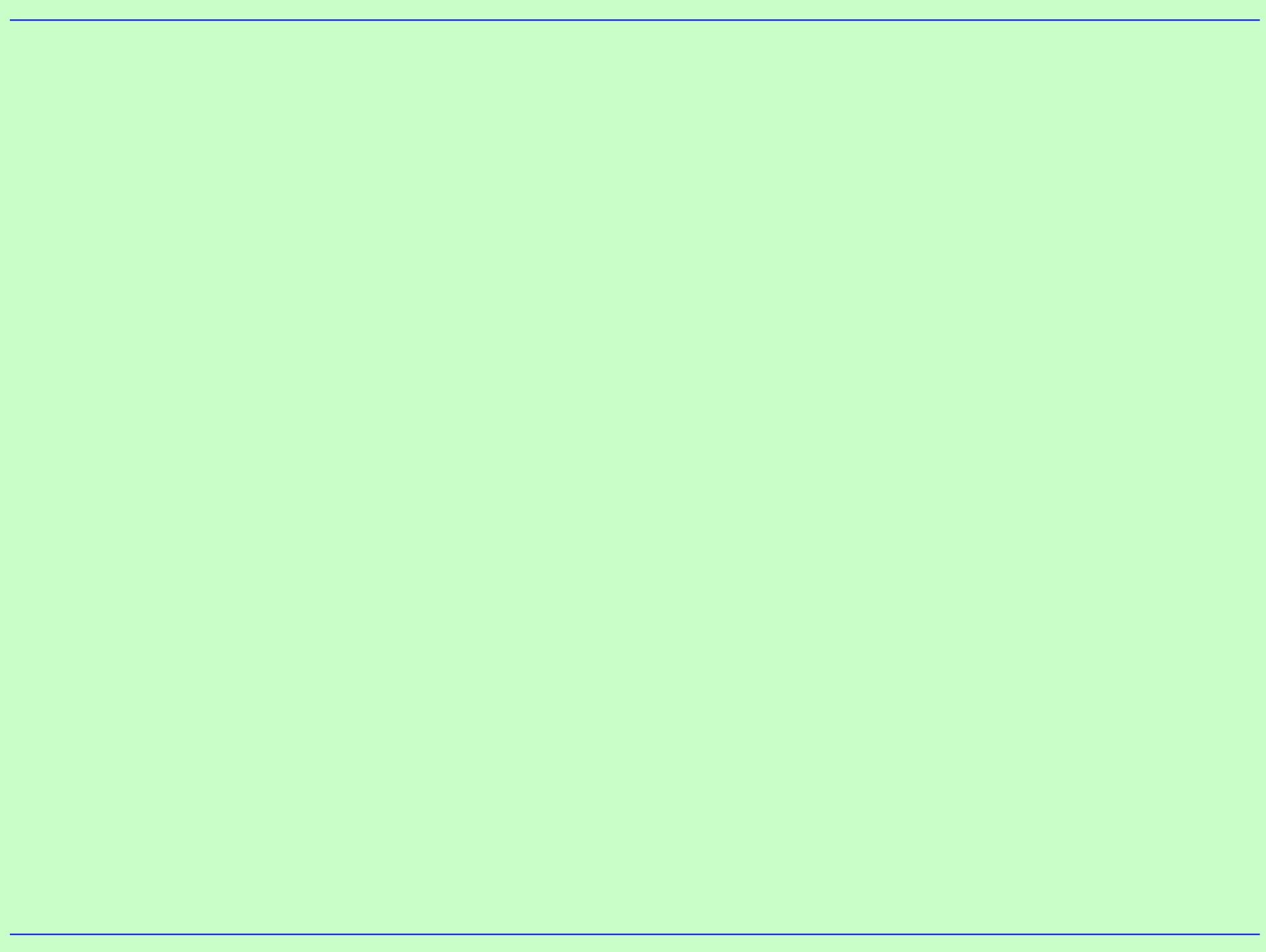
3. CONTROLES DE ACESSO E AUTORIZAÇÃO

3. Conformidade Regulatória (Compliance)

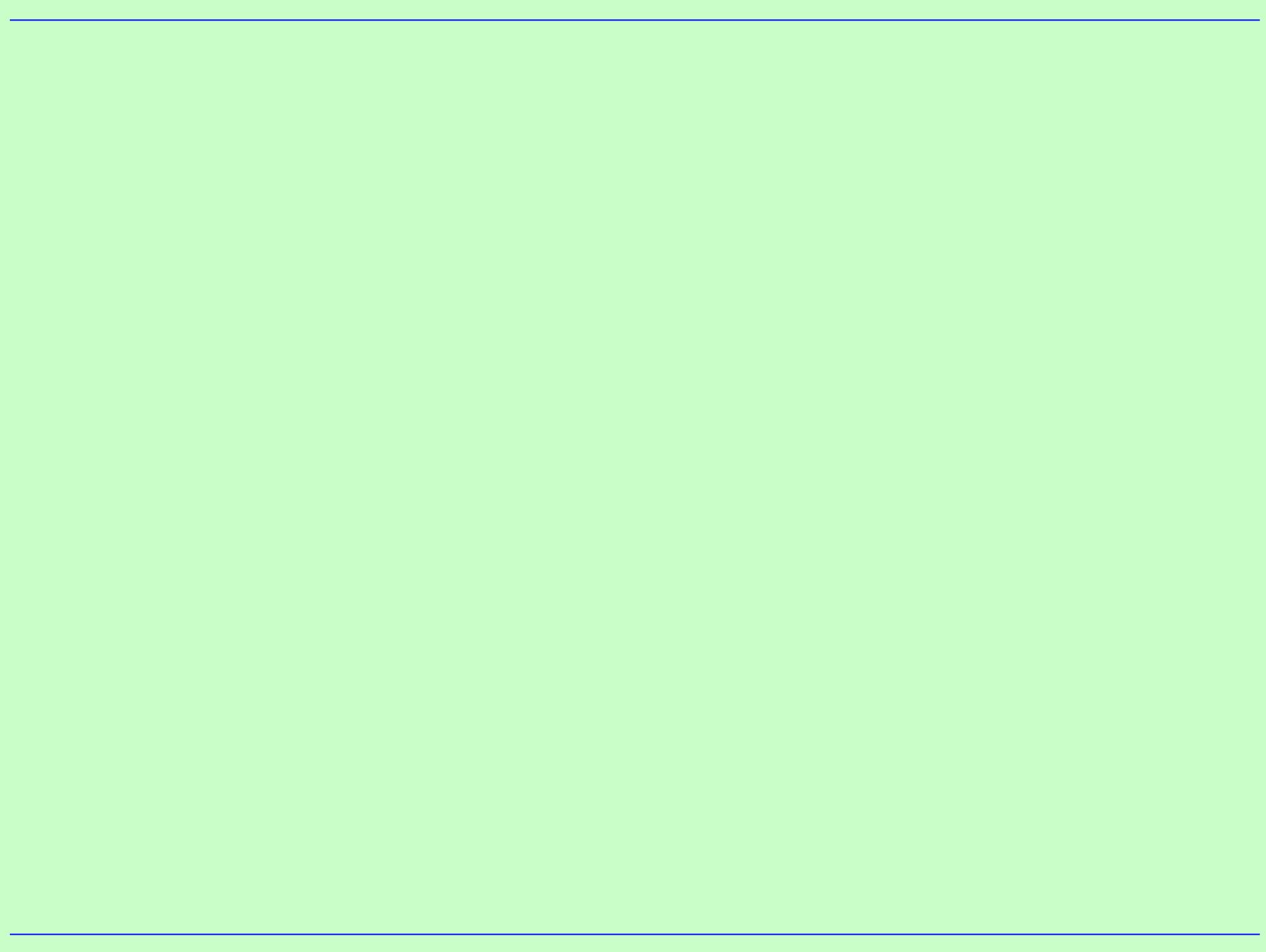
- Os **controles de acesso e autorização** ajudam as organizações a **cumprirem** as rigorosas **regulamentações** de proteção de dados, que muitos setores estão sujeitos, tais como: o GDPR na União Europeia e a **LGPD no Brasil**, entre outras.

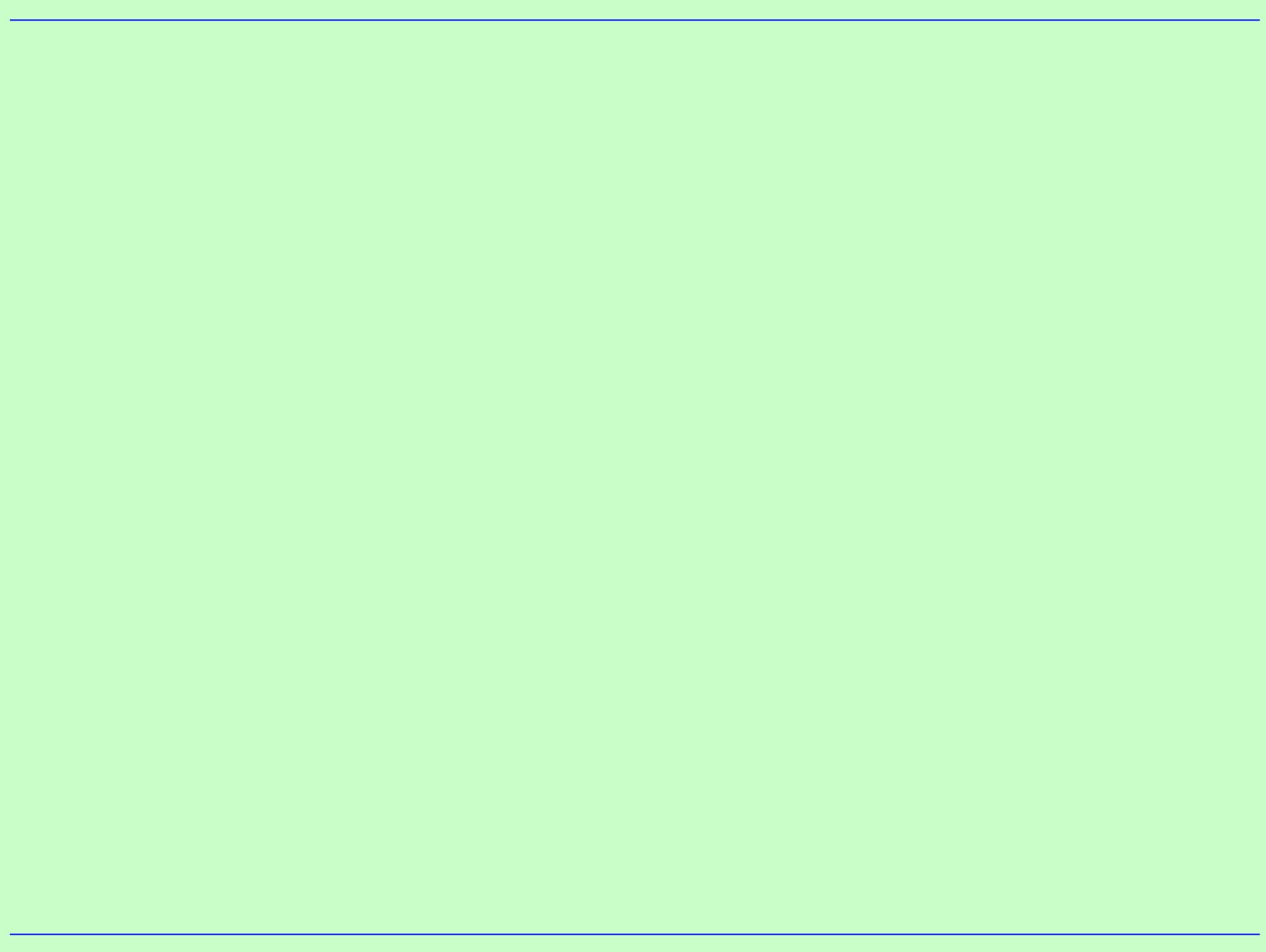


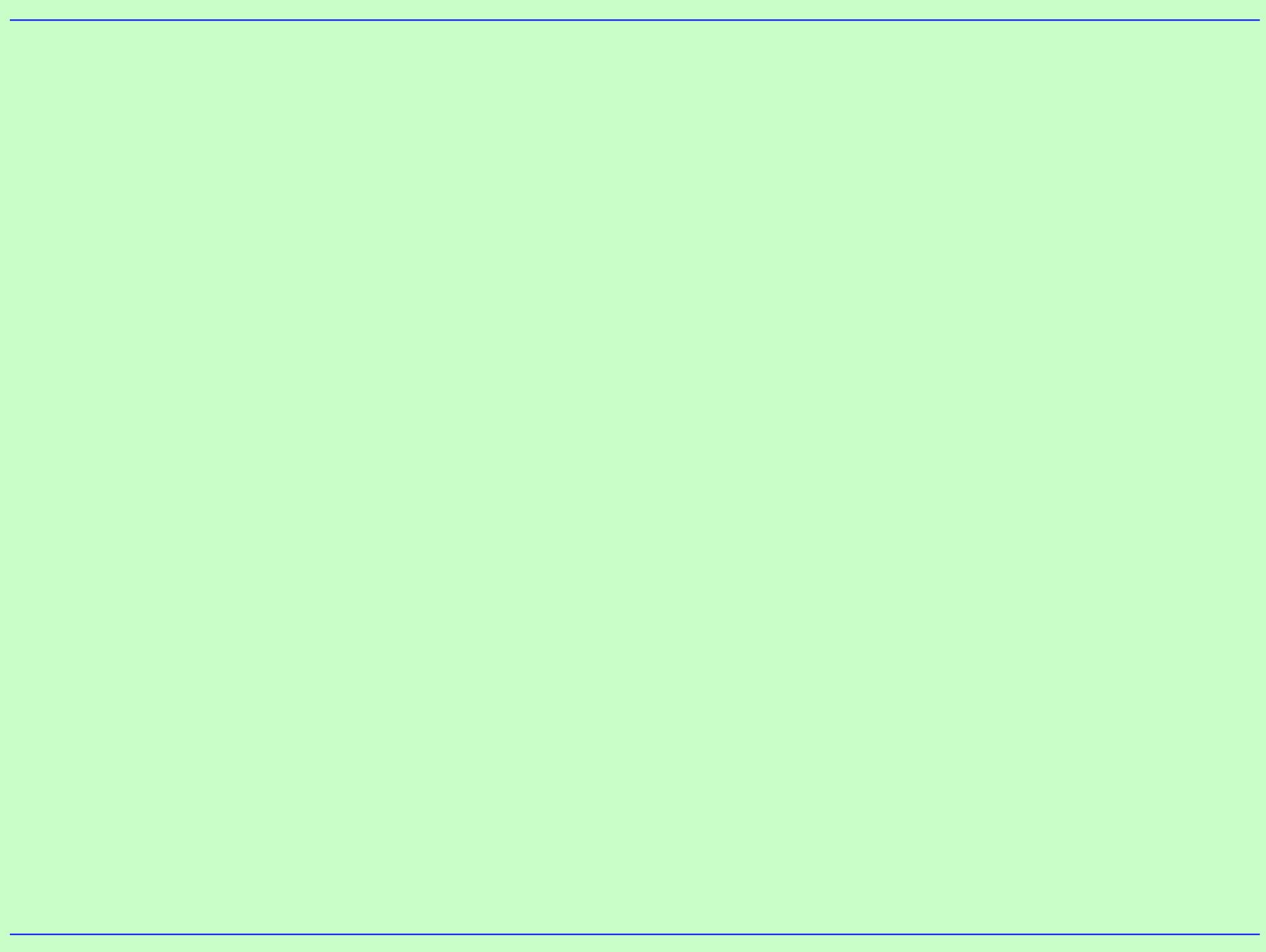
4. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

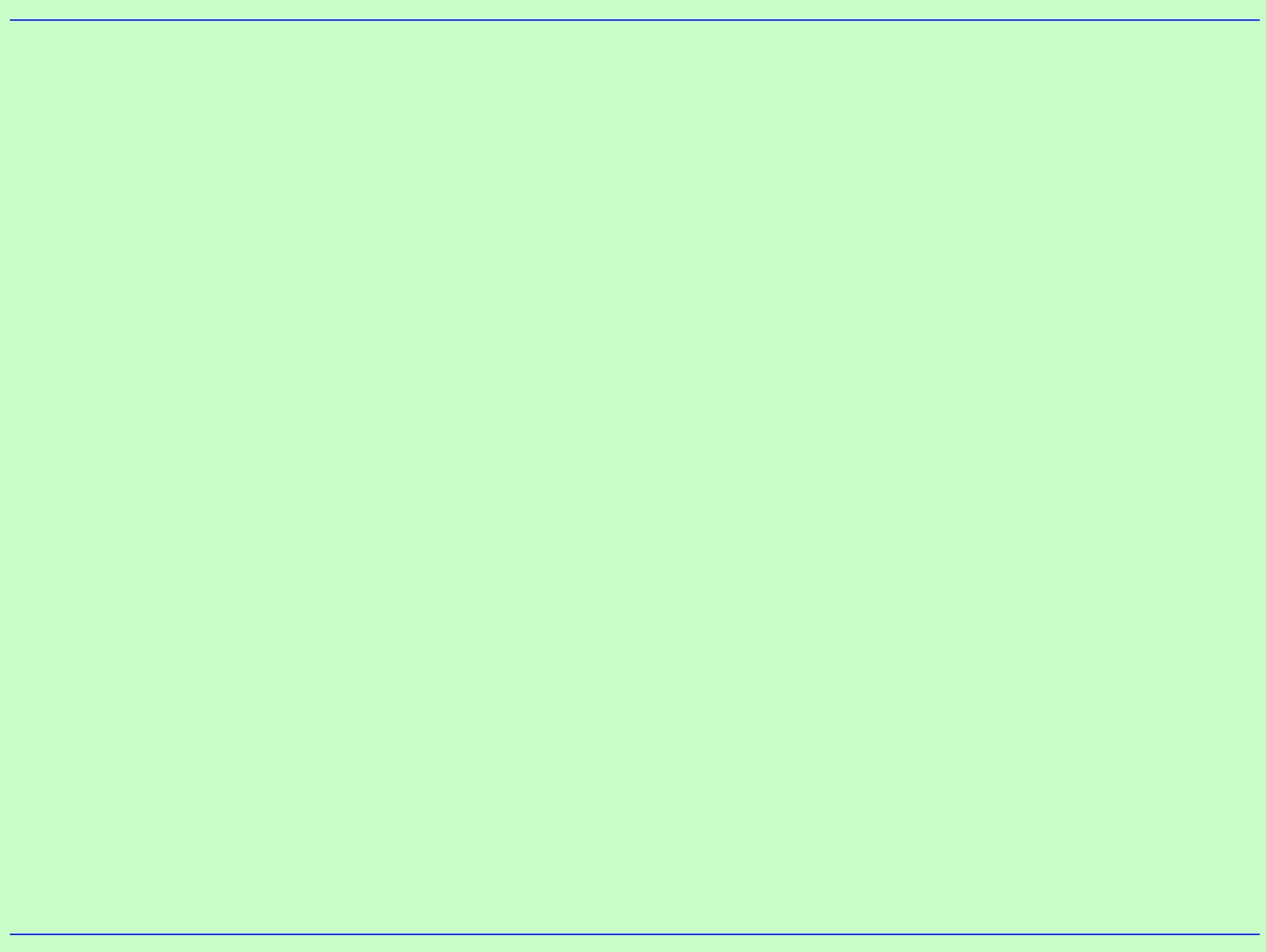


5. MODELOS E MECANISMOS DE CONTROLES DE ACESSO E AUTORIZAÇÃO









CST Desenvolvimento de Software Multiplataforma (DSM)

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

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