Pauta

- Reports das iniciativas.
  - Acompanhamento.
  - Comunicação.
  - Infra Básica.
  - Monitoração.
  - Responsabilização/permissionamento.
- **Retorno do Comitê Executivo.**
- Sobre chaves privadas.

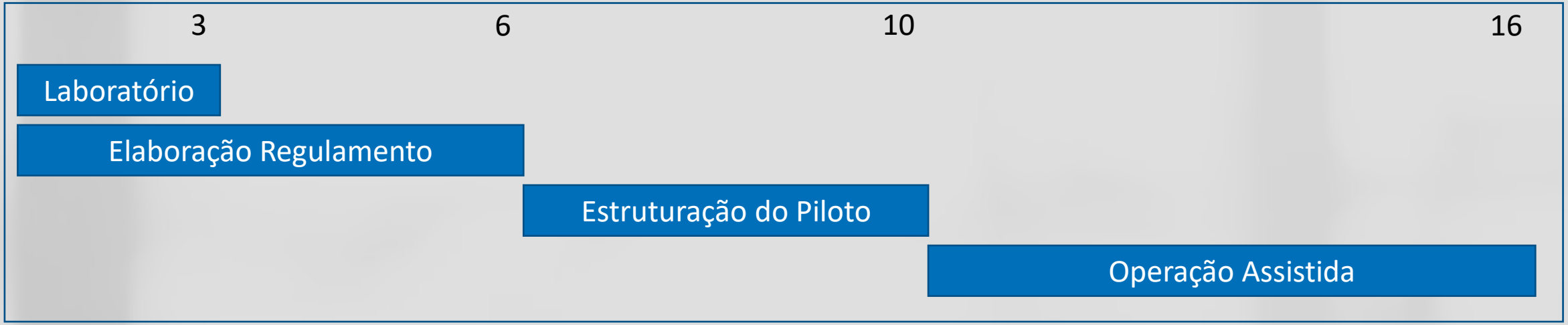
Prazos no Acordo

- Definir um prazo ainda é dificuldade.

A contar da data de assinatura do **ACORDO**:

ATIVIDADES	CRONOGRAMA DE EXECUÇÃO
Implantação da rede laboratório	1º ao 2º mês
Elaboração do regulamento da RBB	1º ao 5º mês
Estruturação do piloto	6º ao 9º mês
Operação assistida do piloto	10º ao 15º mês
Estruturação da produção	16º ao 24º mês
Promoção do uso da rede e evoluções	25º ao 60º mês

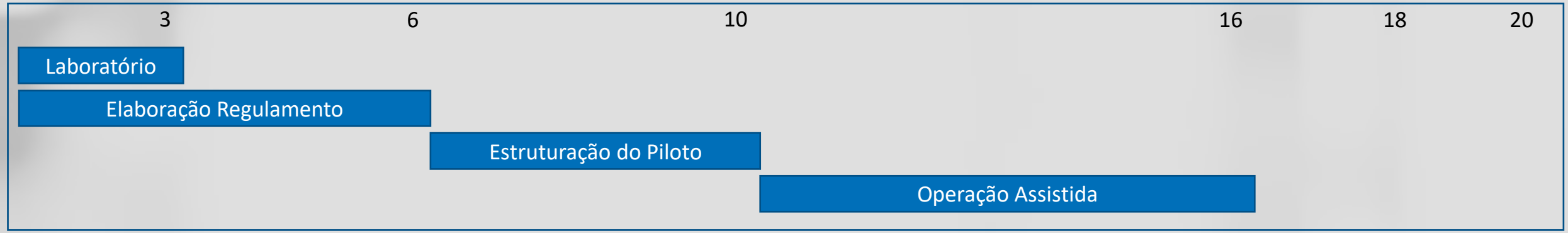
Prazos no Acordo



- Premissas.
  - Arquitetura praticamente definida (baseada na LACChain).
    - Laboratório e Piloto mais curtos.
    - Laboratório já existia.
  - Elaboração de Regulamento em 6 meses.
  - Operação Assistida como tempo para incorporação de aplicações.

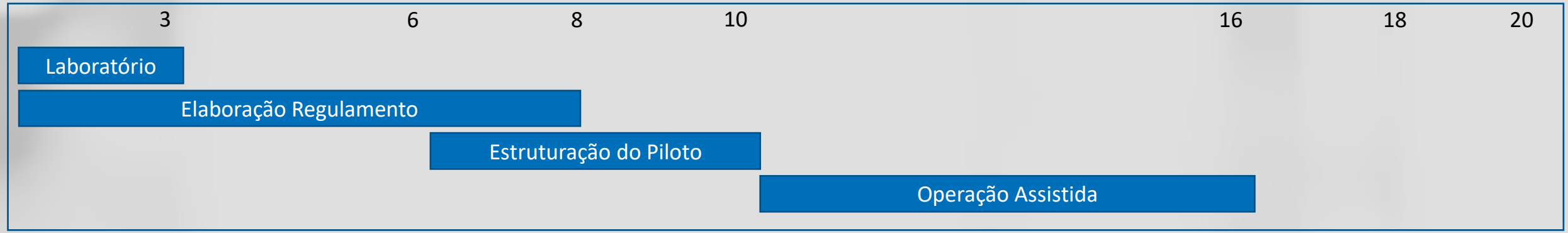
Prazos no Acordo

- Possíveis novas premissas.
  - Elaboração de Regulamento se estendeu.



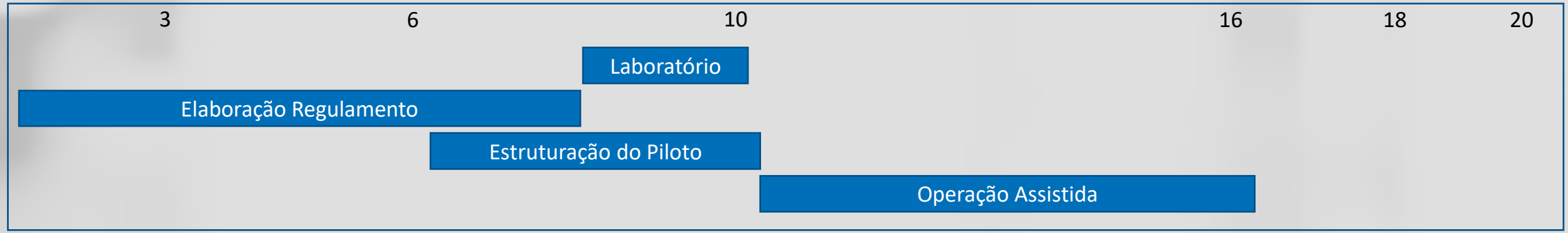
Prazos no Acordo

- Possíveis novas premissas.
  - Elaboração de Regulamento se estendeu.
  - Necessidade de revisão de arquitetura.
  - Necessidade de reset do laboratório.
  - Consequências:
    - Não houve paralelismo.



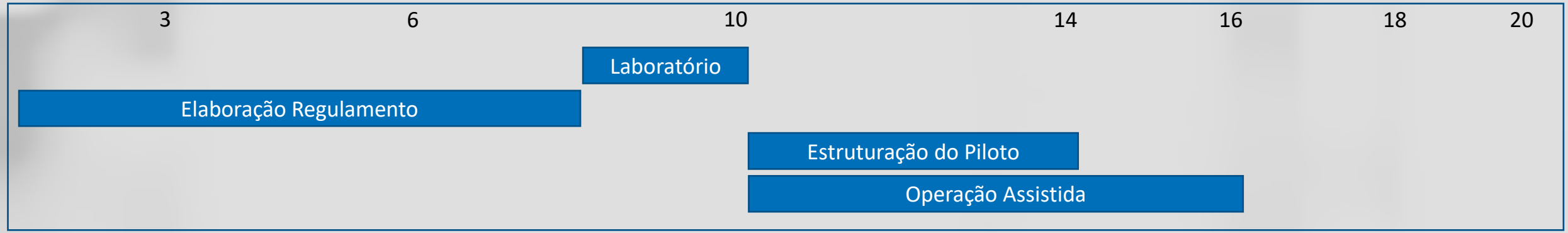
Prazos no Acordo

- Possíveis novas premissas.
  - Elaboração de Regulamento se estendeu.
  - Necessidade de revisão de arquitetura.
  - Necessidade de reset do laboratório.
  - Consequências:
    - Não houve paralelismo.



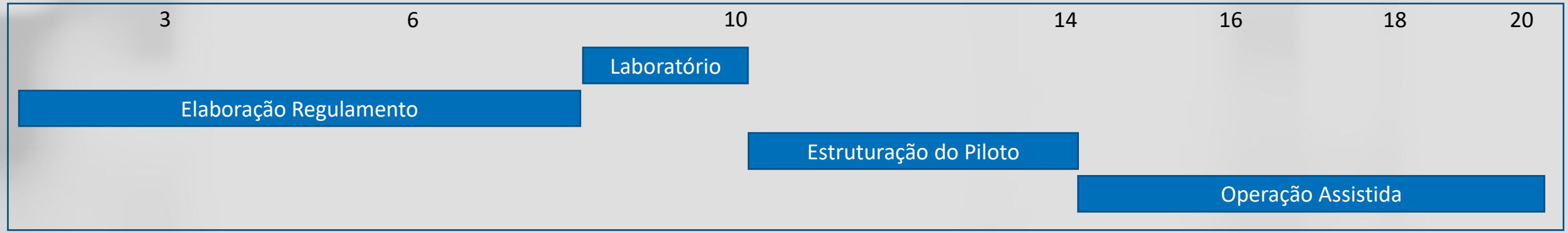
Prazos no Acordo

- Possíveis novas premissas.
  - Elaboração de Regulamento se estendeu.
  - Necessidade de revisão de arquitetura.
  - Necessidade de reset do laboratório.
  - Consequências:
    - Não houve paralelismo.



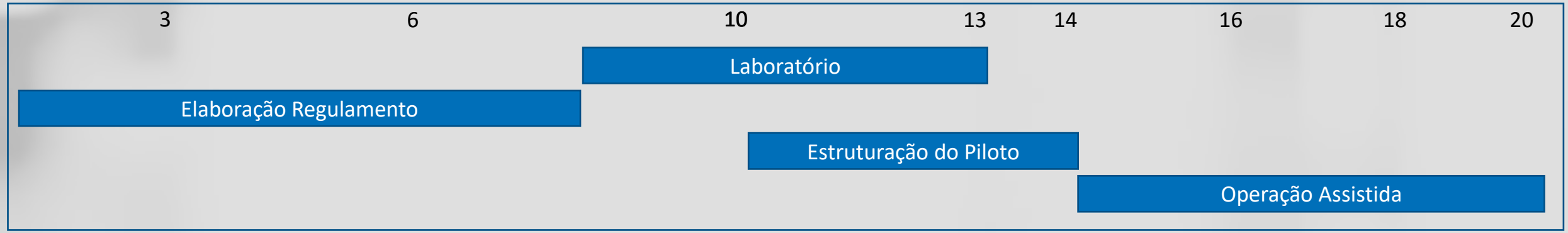
Prazos no Acordo

- Possíveis novas premissas.
  - Elaboração de Regulamento se estendeu.
  - Necessidade de revisão de arquitetura.
  - Necessidade de reset do laboratório.
  - Consequências:
    - Não houve paralelismo.
    - Mais prazo para o laboratório (reset após arquitetura).



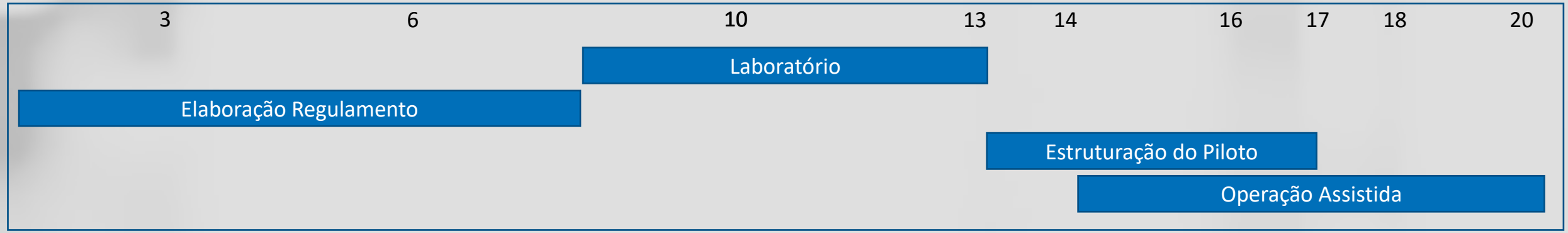
Prazos no Acordo

- Possíveis novas premissas.
  - Elaboração de Regulamento se estendeu.
  - Necessidade de revisão de arquitetura.
  - Necessidade de reset do laboratório.
  - Consequências:
    - Não houve paralelismo.
    - Mais prazo para o laboratório (reset após arquitetura).



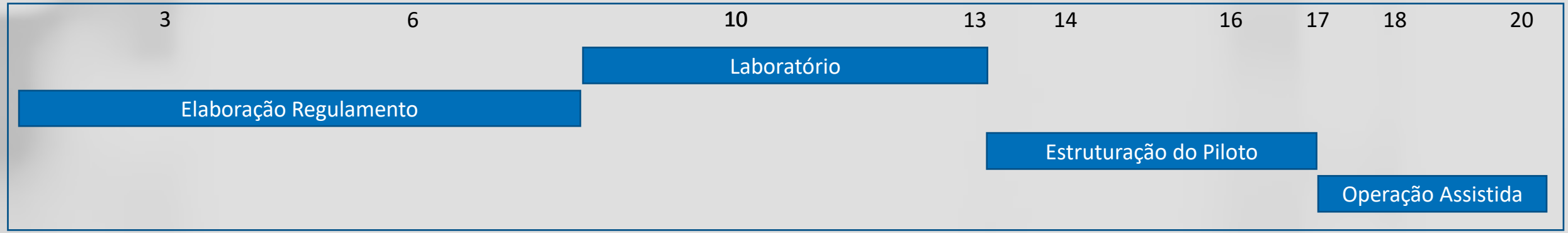
Prazos no Acordo

- Possíveis novas premissas.
  - Elaboração de Regulamento se estendeu.
  - Necessidade de revisão de arquitetura.
  - Necessidade de reset do laboratório.
  - Consequências:
    - Não houve paralelismo.
    - Mais prazo para o laboratório (reset após arquitetura).



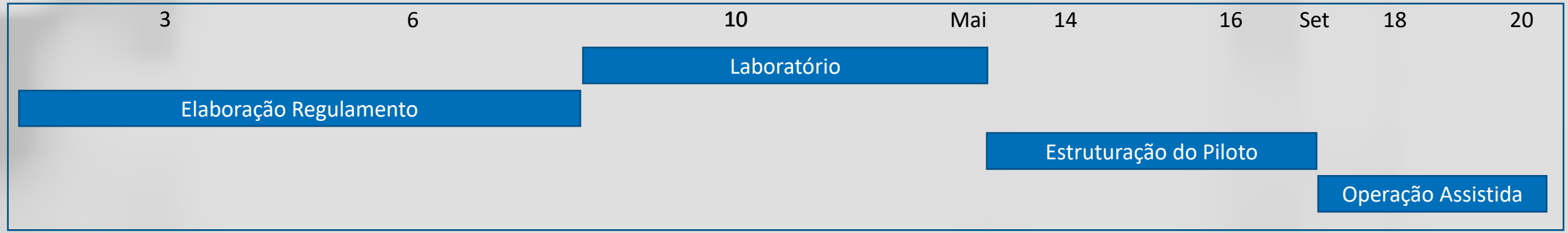
Prazos no Acordo

- Possíveis novas premissas.
  - Elaboração de Regulamento se estendeu.
  - Necessidade de revisão de arquitetura.
  - Necessidade de reset do laboratório.
  - Consequências:
    - Não houve paralelismo.
    - Mais prazo para o laboratório (reset após arquitetura).



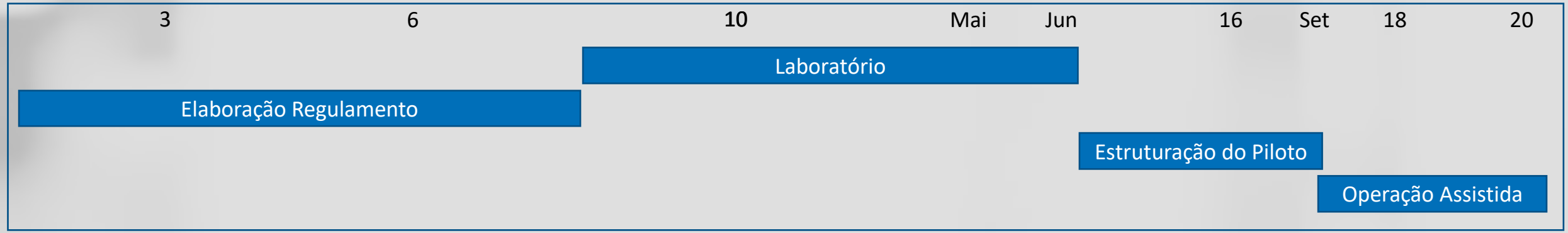
Prazos no Acordo

- Possíveis novas premissas.
  - Elaboração de Regulamento se estendeu.
  - Necessidade de revisão de arquitetura.
  - Necessidade de reset do laboratório.
  - Consequências:
    - Não houve paralelismo.
    - Mais prazo para o laboratório (reset após arquitetura).



Prazos no Acordo

- Possíveis novas premissas.
  - Elaboração de Regulamento se estendeu.
  - Necessidade de revisão de arquitetura.
  - Necessidade de reset do laboratório.
  - Consequências:
    - Não houve paralelismo.
    - Mais prazo para o laboratório (reset após arquitetura).



Prazos do Acordo

- Para validar o cronograma, são necessárias mais informações:
  - Confirmar escopo.
  - Confirmar alocações?

Prazos do Acordo

- Sobre o escopo.
  - Antecipação de itens pouco discutidos para redução de risco.
    - Ex.: Gestão de chaves privadas e upgrade.
  - Detalhamento das frentes.
  - Antecipação de Manual de Operações.
    - Evitar riscos de consenso, de negócio, legais etc.

Prazos do Acordo

- Sobre as alocações.
  - Fechar uma alocação entre empresas não parece viável.
  - Saída é distribuir responsabilidades de forma equilibrada.
    - Avaliação do Comitê Técnico.
  - Cada instituição precisará se comprometer à alocação necessária para cumprir os objetivos acordados.
    - Comitê Técnico prepara planejamento e distribuição de responsabilidades.
    - Aprovação pelo Comitê Executivo.
  - Acompanhar andamento.

Pauta

- Reports das iniciativas.
  - Acompanhamento.
  - Comunicação.
  - Infra Básica.
  - Monitoração.
  - Responsabilização/permissionamento.
- Retorno do Comitê Executivo.
- **Sobre chaves privadas.**

Chaves Privadas

- Objetivo da atividade de planejamento.
  - Esclarecer escopo.
    - Reduzir o risco de surpresas no cronograma.
  - Garantir segurança.
  - Espírito de MVP.
- Questão técnica: quais são e como mitigar os riscos de:
  - Roubo de chave privada de um nó?
  - Roubo de chave privada usada para o permissionamento?
- Premissa.
  - Podemos definir protocolos, mas não os componentes e os procedimentos internos das outras empresas.
- Consequência:
  - Compromisso formal de responsabilidade por mau uso da chave privada.

Chaves Privadas – Chave de Validator

- Risco de roubo da chave privada de um validator.
  - Voto contra em blocos regulares.
  - Proposição de blocos irregulares.
- Aparentemente, o risco é baixo, pois há necessidade de consenso.
- Não pode acontecer o roubo de vários validators.
  - Impacto no consenso.
- Mitigação:
  - Monitoração de proposição de blocos inválidos (previsto).
  - Monitoração de votação (adendo opcional).

Chaves Privadas – Chave de Permissionamento

- Compromisso inicial → Chave será usado apenas para permissionamento.
- Risco de roubo de chave de permissionamento.
  - Parar a rede.
    - Despermissionamento de validators.
    - Despermissionamento de endereços.
    - Exclusão de administradores.

Chaves Privadas – Chave de Permissionamento

- Ataque perfeito → Todos os admins e nós excluídos.
  - Se validators forem despermissionados, a rede para e não é possível alterar o contrato.
  - Se admins forem excluídos, idem (mesmo com rede em pé).
  - Mitigação.
    - Resetar a rede usando outro contrato de permissionamento.
    - O original estará dominado pelo atacante.
    - Efeito: inoperância temporária.

Chaves Privadas – Chave de Permissionamento

- Como parar o ataque?
  - Proposta: regra que garante que só é possível excluir um admin ou nó após 24h da última exclusão pelo mesmo admin.
  - Implementação simples: um mapping!
- Como detectar o ataque?
  - Monitoração específica para exclusão de admin e de nó.
- Incluir regra para acionamento no Manual de Operações.