



INTRODUÇÃO À SEGURANÇA DA INFORMAÇÃO

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO – PARTE II

Prof. Dr. Daniel Caetano

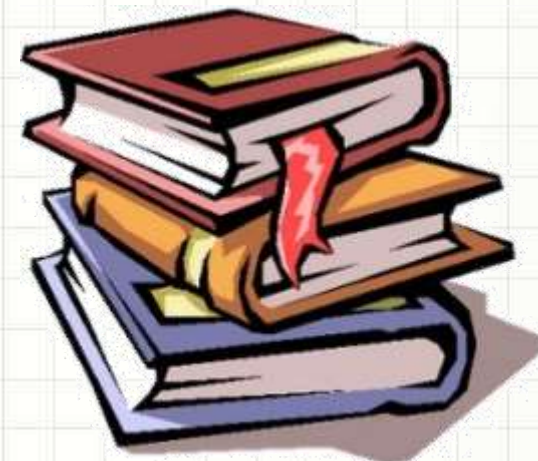
2020 - 1

Objetivos

- Compreender o conceito de autenticidade e não repúdio
- Conhecer os diferentes tipos e mecanismos de autenticação
- Conceituar segurança lógica e física
- Compreender o ciclo de vida da informação



Material de Estudo



Material

Acesso ao Material

Notas de Aula e
Apresentação

<http://www.caetano.eng.br/>
(Segurança da Informação – Aula 2)

Material Didático

Gestão de Segurança da Informação, Cap 1.

Leitura Adicional

<http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf> (TCU - Cap. 2)

Antes de Mais nada...

- **Não deixe de consultar o material da 1ª Aula!**
- **Otimize seus estudos**
 - Toda semana acessar o SAVA!
 - Se preparar para conteúdo da semana seguinte!
- **Exercícios Semanais**
 - Exercícios propostos a cada aula: SAVA
- **Será controlada a presença**
 - Chamada ocorrerá sempre às 20:30 / 22:25

- **Contato**

Professor

Informações de Contato

Daniel Caetano

prof@caetano.eng.br

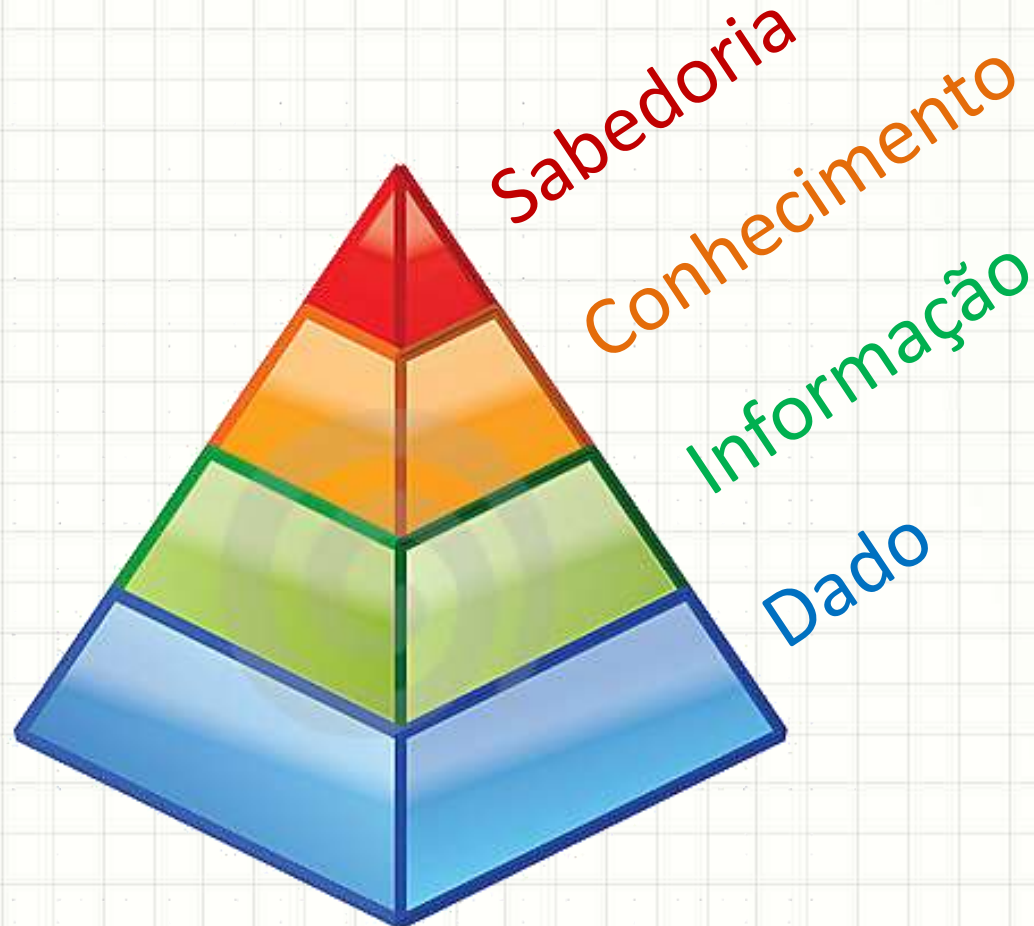


RETOMANDO:

INFORMAÇÕES E SUA SEGURANÇA

Hierarquia DIKW

- Ciência da Informação
 - Pirâmide do conhecimento



Importância da Informação

- Informações são um **ativo** da empresa
 - Devem ser protegidas!
 - Garantir continuidade dos negócios
 - Maximizar o retorno de investimentos/oportunidades
 - Minimizar transtornos.
- Informação em constante risco
 - Em especial porque muitas são “sensíveis”
 - Proteção dos negócios
 - Lei Geral de Proteção de Dados



Princípios Fundamentais

- Equação fundamental da segurança

$$Praticidade = \frac{1}{Segurança}$$

- Objetivo: garantir
 - **Confidencialidade**
 - **Integridade**
 - **Disponibilidade.**



AUTENTICIDADE E NÃO-REPÚDIO

Problemas de Autenticidade

- **Ex.:** alguém sacar seu dinheiro em seu nome
- Alguns outros problemas possíveis
 - Alguém enviar mensagem em seu nome
 - Alguém acessar um sistema em seu nome
 - Alguém visualizar documentos que só você deveria
 - Alguém interceptar mensagem destinadas a você
 - ...
- Como evitar?

Garantia de Autenticidade

- **Autenticidade:** sem adulterações
 - De usuário/pessoa
 - Do documento/autor.
- Autenticidade garantida por dois mecanismos
 - **Autenticação:** Partes são quem dizem ser
 - **Assinatura Digital:** Mensagem inalterada (inclui autoria)

Garantia de Autenticidade

- Requisitos da autenticidade:
 - Autenticação da origem
 - Autenticação do destino
 - Integridade da informação.

- Consequência: **não-repúdio**
 - Garantir a responsabilização dos envolvidos

Garantia da Autenticidade

- Segurança: lógica + física
 - Conteúdo + Meio Portante
- Controle de Acesso





CONTROLE DE ACESSO

Controle de Acesso

- Segurança pressupõe controle de acesso
 - Físico: portões, muros etc.
 - Lógico: login, registros (logging etc.).
- Envolve
 - Recurso: o que será protegido
 - Usuário: quem pode acessá-lo / modificá-lo

**Tudo é proibido a menos que
expressamente permitido**

Controle de Acesso

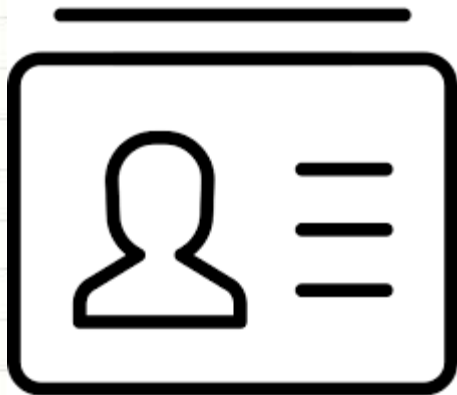
- Dois pontos fundamentais de interesse
 - **Proteger informações e transações** de usuários não autorizados
 - **Monitoramento do acesso** a recursos críticos para a empresa.
- Permitir a responsabilização dos usuários
- Permitir a auditoria
 - Identificar a falha e como ela foi explorada.

Controle de Acesso: Procedimento

- **Logon/Login:** dois processos básicos
 - Identificação: qual é o usuário e suas permissões
 - Autenticação: comprovar a identidade
- **Identificação:** por meio de informação única
 - Número de identificação, nome de usuário...
- **Autenticação:** informação ou item de posse exclusiva do usuário
 - Senha, medição biométrica, chave criptográfica...

Controle de Acesso: Procedimento

- **Logon/Login:** dois processos básicos
 - Identificação: qual é o usuário e suas permissões
 - Autenticação: comprovar a identidade
- Resumindo
 - **Identificação + Algo que usuário sabe ou tem**



Dificuldades Associadas

- **Logon:** muito importante
 - Restringir as operações aos usuários permitidos
 - Registrar ações executadas
- Processo precisa ser resistente à “invasão”:
 - Cartões: podem ser perdidos
 - Userids: podem ser fornecidos facilmente
 - Senhas: anotações, senhas fracas, força bruta...
 - Biometria: falsos negativos, custo...
- Limitar o número de tentativas

Sistemas de Registro (Logging)

- Finalidade: auditoria
- Logs devem registrar
 - Tudo que um usuário fez
 - Quem fez qualquer coisa.
- Demanda ações da administração do sistema
 - Cadastro / Comunicação de Senhas
 - Cada usuário é único no sistema (incluindo adms)
 - Controle de alterações nas permissões
 - Gerenciamento de Logs
 - Auditorias Frequentes.



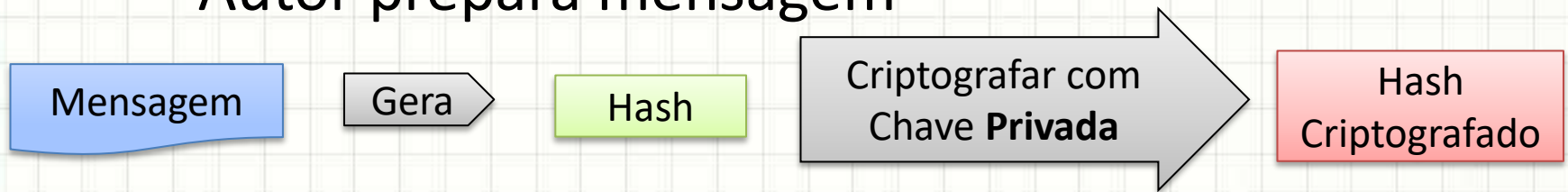
Assinaturas Digitais

- Objetivo: garantir integridade e não-repúdio
- Requisitos
 - Receptor: verificar identidade do autor
 - Autor: não repudiar o conteúdo
 - Receptor/Intermediário: não alterar/forjar conteúdo.
- Meio comum: Criptografia de Chave Pública
 - Chave Privada: só o autor da mensagem possui
 - Chave Pública: disponível publicamente em local confiável

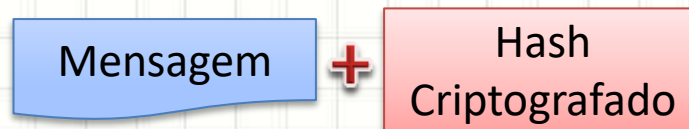
Assinaturas Digitais

- Mecanismo

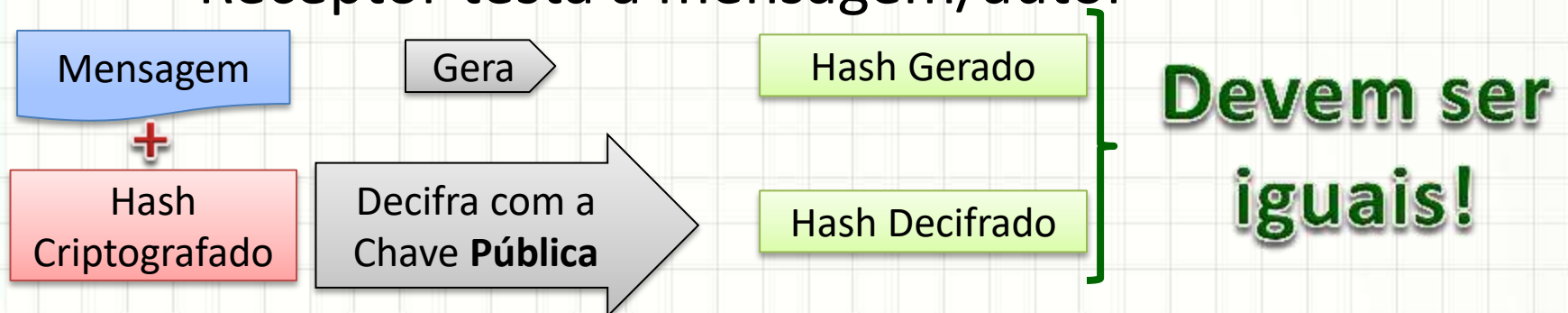
- Autor prepara mensagem



- Autor envia a mensagem



- Receptor testa a mensagem/autor





SEGURANÇA FÍSICA X LÓGICA

Aspectos Lógicos x Físicos

- Dado em Si x Meio Portante
 - Texto em uma folha de papel
 - Bytes em um SSD.
- Integridade
 - Lógica: conteúdo e autoria preservados
 - Física: integridade do meio portante

Aspectos Lógicos x Físicos

**Não existe segurança lógica
sem segurança física**



Aspectos Lógicos x Físicos

- Elementos da Segurança lógica:
 - Identificação/Autenticação
 - Registro em Logs
 - Controle de Permissões de Acesso.
- Elementos da Segurança Física?
 - Aspectos físicos do controle de acesso
 - Quais?

Aspectos Lógicos x Físicos

- Elementos da Segurança Física
 - Segurança puramente física
 - Portão com cadeado, porta com chave
 - Ainda assim, existe uma espécie de autenticação!
 - Suporte aos mecanismos lógicos
 - Identificação/autenticação falhou: barrar invasor
 - Portas, muros, grades
 - Invasor entrou: detectá-lo / identificá-lo
 - Sensores, câmeras, alarmes

Segurança Lógica x Física

- Papel chave no controle de acesso físico
 - Nada é seguro se houver acesso físico
 - Há muitos anos... (FBI)
 - 72% dos ataques originam-se em funcionários
 - 20% por autorizados pela empresa
 - 8% por agentes externos (pessoas sem permissões)
 - Hoje (Kaspersky/Redteam)
 - 50%+ ainda são originados em funcionários
 - 71% dos vazamentos acidentais
 - 68% dos vazamentos por ignorar a política
 - 61% dos casos de vazamento maliciosos

Segurança Lógica x Física

- Controle de Acesso Físico Automatizado
 - Software: controle de acesso e apoio à auditoria
 - Características desejáveis
 - Proteção contra ataques forçados
 - Atualização do sistema
 - Registro de acessos detalhado
 - Autenticação por senha (smartcard + senha)
 - Bloqueio de múltiplos acessos
 - Controle centralizado de acesso
 - Monitoração e relatórios de incidentes
 - Proteção de equipamentos e sistema backup.

Segurança Física

- Retomando
 - Segurança Física sem Lógica: Ok (Cadeado)
 - Segurança Lógica sem Física: Não Ok (Muro?)
 - Pular muro
- Investimentos em segurança Física
 - Grades, muros e portas
 - Guardas, crachás, sistemas de portas duplas
- É só controle de acesso?
 - Proteção contra agentes naturais e criminosos
 - Dificultar espionagem.



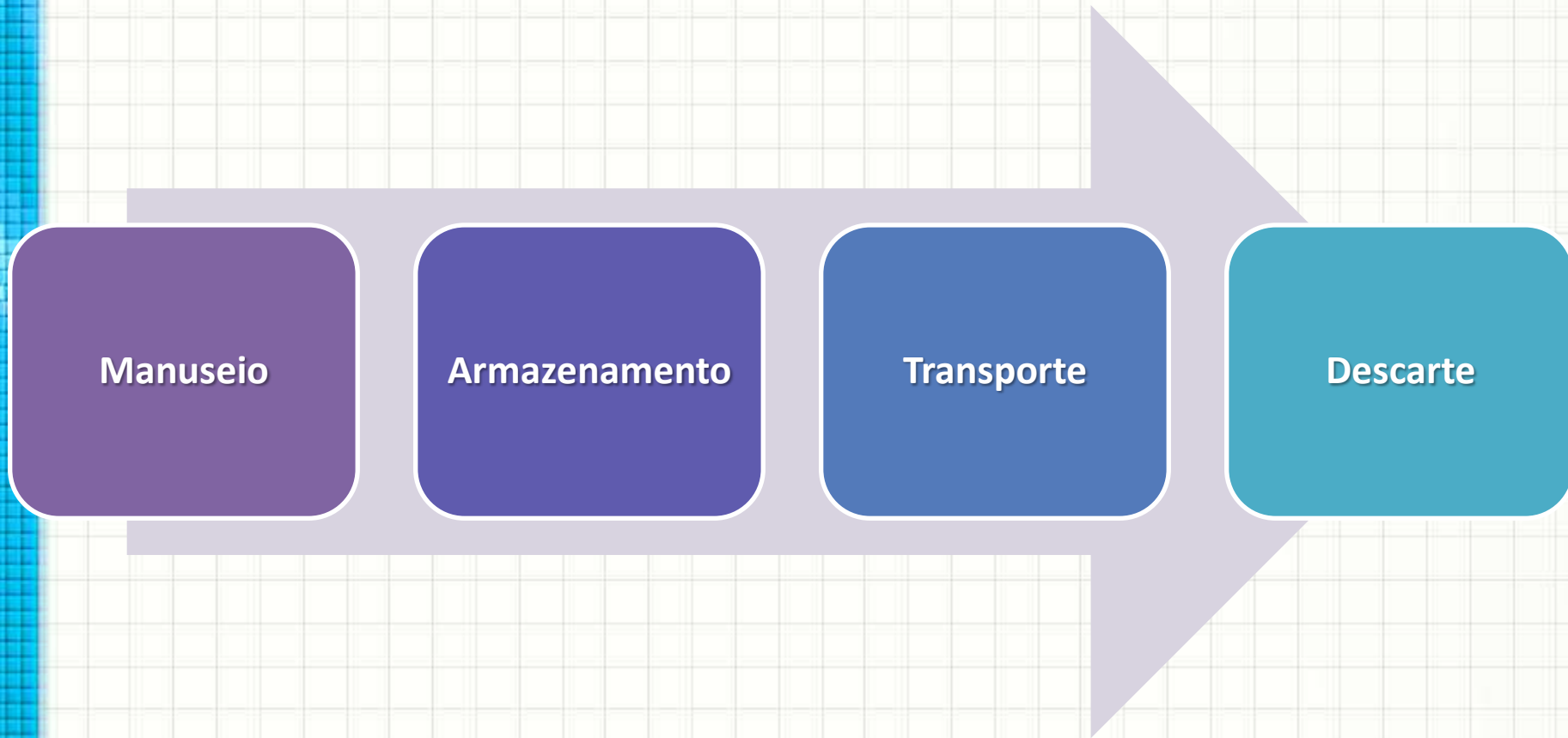
CICLO DE VIDA DA INFORMAÇÃO

Informação: do Berço ao Túmulo

- A informação é eterna?
 - Não!
- Em algum momento ela é criada...
 - E depois de ser usada...
 - Pode ser que seja destruída.
- O que mais pode ocorrer?
 - Ciclo de Vida da Informação

Ciclo de Vida da Informação

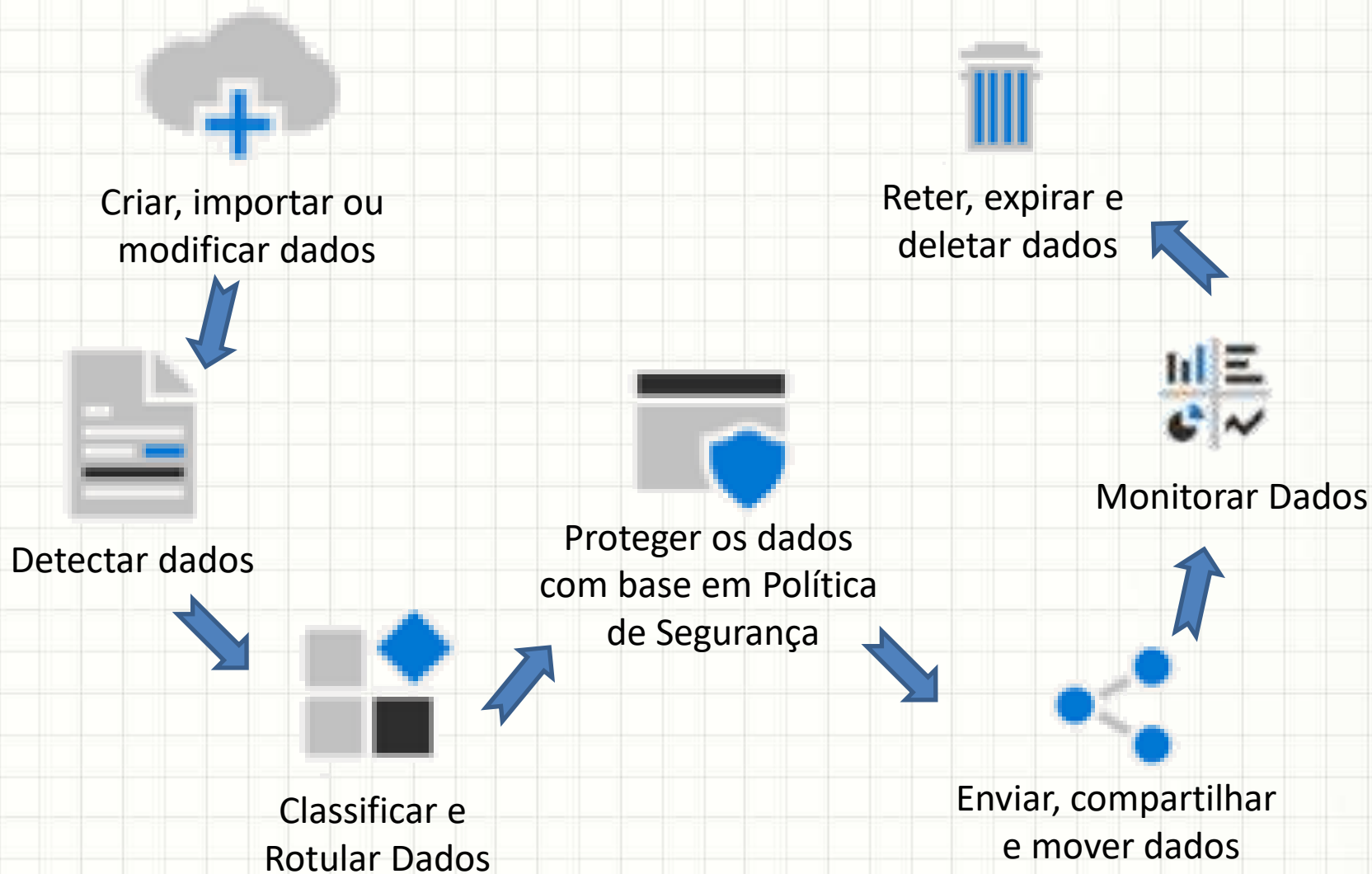
- Sintetizando em 4 etapas



Ciclo de Vida da Informação



Ciclo de Vida da Informação





CONCLUSÕES

Resumo e Próximos Passos

- Autenticidade e Não-Repúdio
 - Controle de Acesso
 - Segurança Lógica x Física
 - Ciclo de Vida da Informação
-

- O que é gestão de risco?
- Qual é o processo?
- Análise de Risco

A stylized graphic of a white wave on a blue background with a grid pattern. The wave is white with a blue outline and a dashed line underneath. The background is a blue gradient with a white grid pattern.

PERGUNTAS?