Caderno de estes para criação de Baselines de Segurança com I.A

* **Data:** <INFORMAR\_DATA>
* **Responsável pelos testes:** <NOME DO RESPONSÁVEL>

# Objetivo

Este caderno é projetado para orientar os testes de escrita de baselines de segurança usando inteligência artificial, incluindo Chat GPT, Gemini e Claude 3. Ele estrutura as atividades em etapas, com espaço para anotações e métricas de tempo.

# Resumo Executivo

TBD

# Execução dos testes

## Parte 1 - Pesquisa e coleta e preparação dos dados

### 1.1 Pesquisa de documentos

* **Descrição da atividade:** Pesquisar no Google por 'Security best practices for <AWS\_SERVICE>'. Acessar e salvar informações de sites confiáveis como AWS, Trend Micro, etc.
* **Tempo inicial:** <INFORMAR\_HORA\_INICIO>
* **Tempo final:** <INFORMAR\_HORA\_FIM>

**Observações:** <TBD>

### 1.2 Coleta e preparação dos dados

* **Descrição da atividade:** Acessar os hiperlinks salvos e copiar o conteúdo relevante das páginas em arquivos de texto.
* **Tempo inicial:** <INFORMAR\_HORA\_INICIO>
* **Tempo final:** <INFORMAR\_HORA\_FIM>

Prompt para PDFs

Quais recomendações de segurança estão contidas neste documento e podem ser aplicadas ao Amazon S3? Extraia a recomendação por completo, com todas as informações adicionais

**Observações:** <TBD>

# Parte 2 – Extração e enriquecimento dos dados

## 2.1 Extração das recomendações via inteligência artificial (ChatGPT, Gemini, Claude V3)

* **Descrição da atividade:** Inserir o conteúdo de cada documento no chat da inteligência artificial (ChatGPT, Gemini, Claude V3), solicitar a extração dos controles relevantes.
* **Tempo inicial:** <INFORMAR\_HORA\_INICIO>
* **Tempo final:** <INFORMAR\_HORA\_FIM>

**Observações:** <TBD>

### Prompt extração dos controles

|  |
| --- |
| Seja um especialista em segurança da informação AWS e <NOME\_DA\_TECNOLOGIA> e siga o que está descrito em {ROTEIRO}  {ROTEIRO}  - Analisar o conteúdo descrito em {CONTEUDO}  - Criar controles de segurança para o <NOME\_DA\_TECNOLOGIA> com base no conteudo analisado  {REGRAS}  - Omita introduções, conclusões, comentários e avisos sobre limitações de conteúdo.  - Para cada controle criado, adicione a referencia  - Siga o padrão descrito em {PADRAO}  - Escreva o resultado em markdown  {PADRAO}  Controle: Nome do controle escrito em linguagem imperativa  - Referencia: Nome do documento de referência.  {CONTEUDO}  Nome do documento de referencia: <INSERIR REFERÊNCIA >  <INSERIR CONTEUDO COPIADO> |

## 2.2 Consolidação dos dados

* **Descrição da atividade:** Consolidar as informações obtida afim de remover dados duplicados.
* **Tempo inicial:** <INFORMAR\_HORA\_INICIO>
* **Tempo final:** <INFORMAR\_HORA\_FIM>

**Observações:** <TBD>

### Prompt de Consolidação dos documentos

|  |
| --- |
| Seja um especialista em segurança da informação AWS e <NOME\_DA\_TECNOLOGIA> e siga o que está descrito em {ROTEIRO}  {ROTEIRO}  - Analisar o conteúdo descrito em {CONTEUDO} e unificar controles com o mesmo nome  {REGRAS}  - Omita introduções, conclusões, comentários e avisos sobre limitações de conteúdo.  - Unifique apenas controles com o mesmo nome, neste caso, concatene as referencias  - Mantenha o padrão dos controles  - Escreva o resultado em markdown  {CONTEUDO}  <INSERIR CONTROLE GERADO> |

## 2.3 Remoção de controles subjetivos

* **Descrição da atividade:** Remover controles subjetivos e que não podem ser auditados via automação.
* **Tempo inicial:** <INFORMAR\_HORA\_INICIO>
* **Tempo final:** <INFORMAR\_HORA\_FIM>

**Observações:** <TBD>

### Prompt de remoção de controles subjetivos

|  |
| --- |
| Seja um especialista em segurança da informação AWS e <NOME\_DA\_TECNOLOGIA> e siga o que está descrito em {ROTEIRO}  {ROTEIRO}  - Analisar o conteúdo descrito em {CONTEUDO} e remover controles subjetivos.  {REGRAS}  - Omita introduções, conclusões, comentários e avisos sobre limitações de conteúdo.  - Qualquer controle cuja aplicação não seja mandatória deve ser removido.  - Leve em consideração que considerar o uso de um ou mais recursos não é reconhecido com um controle mandatório  - Mantenha o padrão dos controles  - Escreva o resultado em markdown  {CONTEUDO}  <INSERIR CONTROLE GERADO> |

## 2.4 Enriquecimento dos controles

* **Descrição da atividade:** Adicionar informações detalhadas a cada controle incluindo Racional, Riscos Mitigados, Auditoria e Remediação.
* **Tempo inicial:** <INFORMAR\_HORA\_INICIO>
* **Tempo final:** <INFORMAR\_HORA\_FIM>

**Observações:** <TBD>

### Prompt

|  |
| --- |
| Seja um especialista em segurança da informação AWS e <NOME\_DA\_TECNOLOGIA> e siga o que está descrito em {ROTEIRO}  {ROTEIRO}  - Analisar o conteúdo descrito em {CONTEUDO} e adicionar as informações faltantes ao para que ele fique dentro do padrão esperado  {REGRAS}  - Omita introduções, conclusões, comentários e avisos sobre limitações de conteúdo.  - Siga o padrão descrito em {PADRAO}  - Escreva o resultado em markdown  {PADRAO}  ### \*\*Nome do controle escrito em linguagem imperativa\*\*  - \*\*Controle ID:\*\* <nome\_do\_documento\_001>  - \*\*Racional:\*\* Breve descrição do porquê este controle é importante.  - \*\*Riscos Mitigados:\*\* Breve descrição dos riscos mitigados por este controle.  - \*\*Auditoria:\*\* Orientação passo a passo sobre como verificar se o controle está aplicado via console.  - \*\*Remediação:\*\* Orientação passo a passo sobre como aplicar o controle via console.  - \*\*Referências:\*\* Documentações que embasem este controle  {CONTEUDO}  <INSERIR CONTROLE GERADO> |

# 3 Criação do baseline utilizando o modelo padrão

## 3.1 Adicionar os controles enriquecidos no baseline

* **Descrição da atividade:** Copiar os controles para documento padrão e preencher demais informações
* **Tempo inicial:** <INFORMAR\_HORA\_INICIO>
* **Tempo final:** <INFORMAR\_HORA\_FIM>

**Observações:** <TBD>

## 3.2 Consolidação Parte 2

* **Descrição da atividade:** Verificar se faz sentido unificar outros controles para não ter controles redundantes
* **Tempo inicial:** <INFORMAR\_HORA\_INICIO>
* **Tempo final:** <INFORMAR\_HORA\_FIM>

**Observações:** <TBD>

Prompt 1

Eu estou criando um baseline de segurança para o Serviço Amazon S3, seja um especialista em segurana da informação AWS e revise o documento anexo.

{ATIVIDADES}

- Verifique se é possível reduzir a quantidade de controles, unificando controles redundantes

- Faça sugestões de melhorias no documento com base nas melhores práticas de segurança da informação

Prompt 2

Faça uma relação dos controles redundants, porém me mostre apenas os CONTRLO ID dos controles redundantes para eu revisar

### Prompt 1 – Visão geral dos controles

|  |
| --- |
| Siga o que está descrito em {ROTEIRO}  {ROTEIRO}  - Analisar o conteúdo descrito em {CONTEUDO} e criar a tabela de alterações seguindo o padrão  {REGRAS}  - Omita introduções, conclusões, comentários e avisos sobre limitações de conteúdo.  - Siga o padrão descrito em {PADRAO}  - Escreva o resultado em markdown  {PADRAO}  ### Visão geral dos controles  | Controle | Racional | Aplicabilidade | Local de aplicação do controle |  |--------|--------------------|--------------------|--------------------|  | <CONTROLE> | <RACIONAL> | <NAO\_PREENCHER> | <NAO\_PREENCHER |  {CONTEUDO}  <INSERIR CONTROLES ENRIQUECIDOS> |

### Prompt 2 – Histórico de alterações

|  |
| --- |
| Siga o que está descrito em {ROTEIRO}  {ROTEIRO}  - Analisar o conteúdo descrito em {CONTEUDO} e criar a tabela de alterações seguindo o padrão  {REGRAS}  - Omita introduções, conclusões, comentários e avisos sobre limitações de conteúdo.  - Siga o padrão descrito em {PADRAO}  - Escreva o resultado em markdown  {PADRAO}  ### Histórico de Alterações  | Versão | Data de Publicação | Descrição | Alterações |  |--------|--------------------|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------|  | v1.0 | <DATA\_ATUAL> | Lançamento Inicial da Aplicação | - Controles incluídos: Controle A, Controle B<br>- Controles excluídos: Nenhum<br>- Controles alterados: Nenhum |  {CONTEUDO}  <INSERIR CONTROLES ENRIQUECIDOS> |

# Parte 4 - Refinamento do baseline

## 4.1 Detalhamento do controle

* **Descrição da atividade:** Detalhar o controle para que pessoas não familiarizadas sejam capazes de aplica-lo e verificar se o mesmo esta aplicado corretamente
* **Tempo inicial:** <INFORMAR\_HORA\_INICIO>
* **Tempo final:** <INFORMAR\_HORA\_FIM>

**Observações:** <TBD>

Prompt

Seja

## 4.2 Consultoria inteligência artificial (ChatGPT, Gemini, Claude V3) e ajustes no baseline

* **Descrição da atividade:** Interagir com A inteligência artificial (ChatGPT, Gemini, Claude V3) para esclarecer dúvidas e realizar ajustes nos controles do baseline.
* **Tempo inicial:** <INFORMAR\_HORA\_INICIO>
* **Tempo final:** <INFORMAR\_HORA\_FIM>

**Observações:** <TBD>

BREAK