Criação de Baseline de Segurança com Inteligência Artificial

# 1. Objetivo

Este Procedimento Operacional Padrão (POP) visa orientar a criação sistemática de baselines de segurança para serviços AWS, utilizando inteligência artificial para auxiliar no processo.

# 2. Escopo

Este POP abrange as atividades desde a pesquisa inicial de melhores práticas de segurança até a consolidação das informações e criação dos baselines de segurança.

# 3. Responsabilidades

* O responsável pelos testes deve seguir este POP para garantir a consistência e a qualidade dos baselines de segurança gerados.
* O gerente do projeto deve assegurar que todas as etapas do POP sejam cumpridas e revisadas.

# 4. Procedimento

Este POP abrange as atividades desde a pesquisa inicial de melhores práticas de segurança até a consolidação das informações e criação dos baselines de segurança.

## 4.1 – Pesquisa, Coleta e Preparação dos dados

Esta etapa envolve a coleta de informações de melhores práticas de segurança para serviços AWS específicos e a preparação desses dados para análise subsequente.

1. Pesquisa de Documentos
   1. Pesquisar no Google por “**Security best practices for <NOME\_DO\_SERVIÇO\_AWS>**”.
   2. Acessar e salvar informações de fontes confiáveis como AWS, Trend Micro, entre outros.
2. Coleta e Preparação dos Dados
   1. - Acessar os hiperlinks salvos e copiar o conteúdo relevante das páginas em arquivos de texto.
   2. Para conteúdo em formatos como PDF ou PPT, anexar o arquivo no chat de IA e utilizar o prompt: “**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.**”.
   3. Salvar as informações extraídas em arquivos de texto seguindo o padrão definido abaixo:
      1. Nome do documento: Deve ser composto pelo fabricante ou fonte e pelo título principal do documento.
      2. Estrutura do documento:
         1. Referência: Incluir fabricante ou fonte, título principal do documento e URL para acesso direto.
         2. Conteúdo Copiado: Incluir o conteúdo relevante extraído do documento ou da interação com a IA.

## 4.2 – Extração das recomendações via inteligência artificial

**Descrição da atividade**

Esta etapa consiste em usar a inteligência artificial para analisar o conteúdo coletado e extrair controles de segurança específicos para o serviço AWS em questão. O objetivo é identificar práticas recomendadas e controles aplicáveis ao contexto de segurança da tecnologia avaliada.

**Atividade**

1. Inserir o conteúdo de cada documento no ChatGPT.
2. Utilizar o prompt abaixo para solicitar a análise do conteúdo e a extração de controles de segurança relevantes.

**Prompt para 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> |

## 4.3 – Revisão e clarificação das recomendações

**Descrição da atividade**

Esta etapa envolve a revisão e a consolidação dos controles de segurança extraídos, com o objetivo de identificar e remover duplicatas e controles genéricos. O foco é garantir que cada controle seja único, específico e diretamente aplicável ao contexto da tecnologia AWS em análise. Controles genéricos, caracterizados por recomendações vagas ou ações não claras, serão eliminados para manter a precisão e a relevância do baseline de segurança.

**Atividade**

1. Inserir o conteúdo de cada documento no ChatGPT.
2. Utilizar o prompt abaixo para solicitar a revisão e consolidação do conteúdo extraído.

**Prompt para Unificação e Clarificação de Controles**

|  |
| --- |
| Seja um especialista em segurança da informação AWS e Amazon S3 e siga o que está descrito em {ROTEIRO}  {ROTEIRO}  - Analisar o conteúdo descrito em {CONTEUDO}, remover controles genéricos e unificar controles que têm exatamente o mesmo nome, assegurando que sejam escritos em linguagem imperativa.  {REGRAS}  - Omita introduções, conclusões, comentários e avisos sobre limitações de conteúdo.  - Remova controles genéricos, que são aqueles que não fornecem instruções específicas ou são muito vagos, como "Considerar uso de" ou "Aplicar menor privilégio".  - Unifique controles que têm exatamente o mesmo nome, combinando as informações e referências em uma única entrada de controle. Assegure que estes controles unificados sejam escritos em linguagem imperativa, dando comandos claros e diretos.  - Mantenha um padrão de clareza, especificidade e aplicabilidade direta em todos os controles documentados.  - Documente os controles em formato markdown.  {CONTEUDO}  - <INSERIR CONTROLES GERADOS> |

## 4.4 – Enriquecimento dos controles

**Descrição da atividade**

O objetivo desta etapa é adicionar informações detalhadas aos controles de segurança, incluindo identificação, racional, riscos mitigados, auditoria e remediação. **É crucial realizar este processo com um controle por vez para assegurar que cada um seja enriquecido com o nível de detalhe necessário e evitar a perda de qualidade na informação.**

**Atividade**

1. Inserir o conteúdo de cada controle no ChatGPT.
2. Utilizar o prompt abaixo para solicitar o enriquecimento de cada controle.

**Atenção: Execute o prompt individualmente para cada controle para garantir a precisão e o detalhamento adequado das informações**

**Prompt de Enriquecimento 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} 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}  - Faça um passo a passo detalhado para os campos “Auditoria” e “Remediação”  - Leve em consideração que pessoas de T.I farão a leitura do controle e precisam ser capazes de aplica-lo e valida-lo  - A explicação sobre como aplicar o controle ou audita-lo dever ser realizada no contexto console da AWS preferencialmente, ou se não for possível via console, via AWS CLI  - 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 e detalhada sobre como verificar se o controle está aplicado via console.  - \*\*Remediação:\*\* Orientação passo a passo e detalhada sobre como aplicar o controle via console.  - \*\*Referências:\*\* Documentações que embasem este controle  {CONTEUDO}  <INSERIR CONTROLE GERADO> |

## 4.5 Criação do baseline utilizando o modelo padrão

Criar um baseline de segurança para o serviço analisado utilizando como base um documento modelo.

### 4.5.1 Preparação do documento

**Descrição da atividade**

A atividade consiste em preparar o documento base para o baseline de segurança, utilizando um modelo pré-definido e adaptando-o para o serviço AWS específico em análise.

**Atividade**

1. Fazer uma cópia do “Modelo\_baseline\_seguranca.docx”
2. Acessar o local onde o “Modelo\_baseline\_seguranca.docx” está armazenado.
3. Fazer uma cópia do documento modelo.
4. Renomear o documento copiado seguindo o padrão “Baseline\_Seguranca\_” + “<NOME\_DO\_SERVIÇO>”. Substituindo <NOME\_DO\_SERVIÇO> pelo nome específico do serviço AWS analisado.

### 4.5.2 Substituir a variável ‘<NOME\_DO\_SERVIÇO>’

**Descrição da atividade**

Esta atividade envolve a substituição da variável ‘<NOME\_DO\_SERVIÇO>’ no documento do baseline de segurança pelo nome específico do serviço AWS que está sendo analisado. A variável aparece principalmente no título do documento e na seção de descrição do Escopo.

**Atividade**

1. Abrir o documento de baseline de segurança renomeado na etapa anterior.
2. Localizar a variável `<NOME\_DO\_SERVIÇO>` no título do documento e substituí-la pelo nome exato do serviço AWS analisado.
3. Procurar e substituir a mesma variável na seção "Escopo" do documento, assegurando que o nome do serviço esteja correto e consistente em todo o documento.

### 4.5.3 Atualizar o tópico Escopo

**Descrição da atividade**

A atividade consiste em atualizar a seção "Escopo" do documento de baseline de segurança com uma descrição detalhada do serviço AWS em análise. A descrição deve fornecer uma visão clara do que o serviço é e para que serve.

**Atividade**

1. No documento de baseline de segurança, navegue até a seção "Escopo".
2. Utilize o prompt a seguir para gerar uma descrição do serviço AWS específico que está sendo analisado. Insira essa descrição na seção "Escopo" do documento.

**Prompt para Descrição do Serviço**

|  |
| --- |
| Gere uma breve descrição do serviço <NOME\_DO\_SERVIÇO>, o que é, para que serve e etc. |

### 4.5.4 Preencher a Tabela do Tópico Visão Geral dos Controles

**Descrição da atividade**

Esta atividade envolve a criação e atualização da tabela no tópico "Visão Geral dos Controles" no documento de baseline de segurança, utilizando uma tabela gerada em Excel com os dados dos controles de segurança relevantes e preenchidos.

**Atividade**

1. Utilize o ChatGPT para gerar a tabela de controles de segurança, utilizando o prompt específico para criação em formato Excel.
2. Faça o download do arquivo em Excel (.xlsx) gerado pelo ChatGPT.
3. Abra a planilha baixada e, se necessário, ajuste as configurações de borda para manter a consistência visual com o documento.
4. Copie o conteúdo da planilha Excel e substitua a tabela existente no tópico “Visão Geral dos Controles” do documento de baseline pela nova tabela copiada.

**Prompt Gerador de Tabela de Controles de Segurança para Excel**

|  |
| --- |
| 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}  - O resultado deve ser disponibilizado em um arquivo xlsx  {PADRAO}  ### Visão geral dos controles  A tabela deve conter as seguintes colunas:  - Controle  - Racional  - Aplicabilidade (deixe em branco)  - Local de aplicação do controle (deixe em branco)  {CONTEUDO}  <INSERIR CONTROLES ENRIQUECIDOS> |

### 4.5.5 Inserir os Controles Gerados no Tópico Detalhamento dos Controles

**Descrição da atividade**

Esta atividade envolve a inserção dos controles de segurança gerados e enriquecidos na seção de detalhamento do documento de baseline, assegurando que cada controle esteja alinhado com a estrutura esperada do documento.

**Atividade**

1. Copie os controles gerados e enriquecidos anteriormente.
2. Cole-os na seção “Detalhamento dos Controles” do documento de baseline de segurança.
3. Revise e edite cada controle para assegurar que ele siga a estrutura esperada, conforme o exemplo abaixo.

**Exemplo de estrutura dos controles detalhados**

Controle

* **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

Repita a estrutura para cada controle, garantindo que todas as informações necessárias sejam incluídas e que os controles estejam organizados e de fácil compreensão.

### 4.5.6 Preencher a Tabela do Tópico Histórico de Alterações

**Descrição da atividade**

Preencher a tabela histórico de alterações com informações relevantes sobre a criação/alteração do documento

**Atividade**

1. Na coluna versão informe a versão do documento seguindo o padrão X.Y sendo o X major e Y minor.
2. Na coluna Data de publicação coloque a data de criação/revisão do documento seguindo o padrao DD/MM/AAAA.
3. Na coluna descrição informe de maneira resumida o que foi feito.
4. Na coluna alterações informe a alteração seguindo o padrão abaixo:
   1. Controles incluídos: <TBD>
   2. Controles excluídos: <TBD>
   3. Controles alterados: <TBD>
5. Para facilitar o preenchimento da coluna alteração, utilize o prompt abaixo:

Prompt Gerador de Histórico de Alterações de 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}  - O resultado deve ser disponibilizado em um arquivo xlsx  {PADRAO}  ### Histórico de Alterações  A tabela no arquivo xlsx deve conter as seguintes colunas:  - Versão  - Data de Publicação  - Descrição  - Alterações  Na coluna "Alterações", as informações devem ser organizadas em subcategorias:  - Controles incluídos: (adicionar "None" se vazio)  - Controles excluídos: (adicionar "None" se vazio)  - Controles alterados: (adicionar "None" se vazio)  {CONTEUDO}  <INSERIR CONTROLES ENRIQUECIDOS> |

## 4.6 Revisão geral I.A

**Descrição da atividade**

Preencher a tabela histórico de alterações com informações relevantes sobre a criação/alteração do documento

**Atividade**

1. Utilize o ChatGPT para analisar o documento de baseline completo.
2. Aplique o seguinte prompt para orientar a revisão.

Prompt de Revisão com IA

|  |
| --- |
| Eu estou criando um baseline de segurança para o serviço <NOME\_DO\_SERVICO>. Seja um especialista em segurança da informação AWS e revise o documento anexo.  {REGRAS}  - Avalie a possibilidade de reduzir a quantidade de controles unificando aqueles que são redundantes.  - Faça sugestões de melhorias com base nas melhores práticas de segurança da informação.  - Consulte as melhores práticas e recomendações de segurança da AWS, CIS, NIST, STIG e outras fontes relevantes.  - Garanta que todas as sugestões de alterações estejam em conformidade com os padrões e normas atuais de segurança da informação.  - Disponibilize uma copia da revisão em docx. |