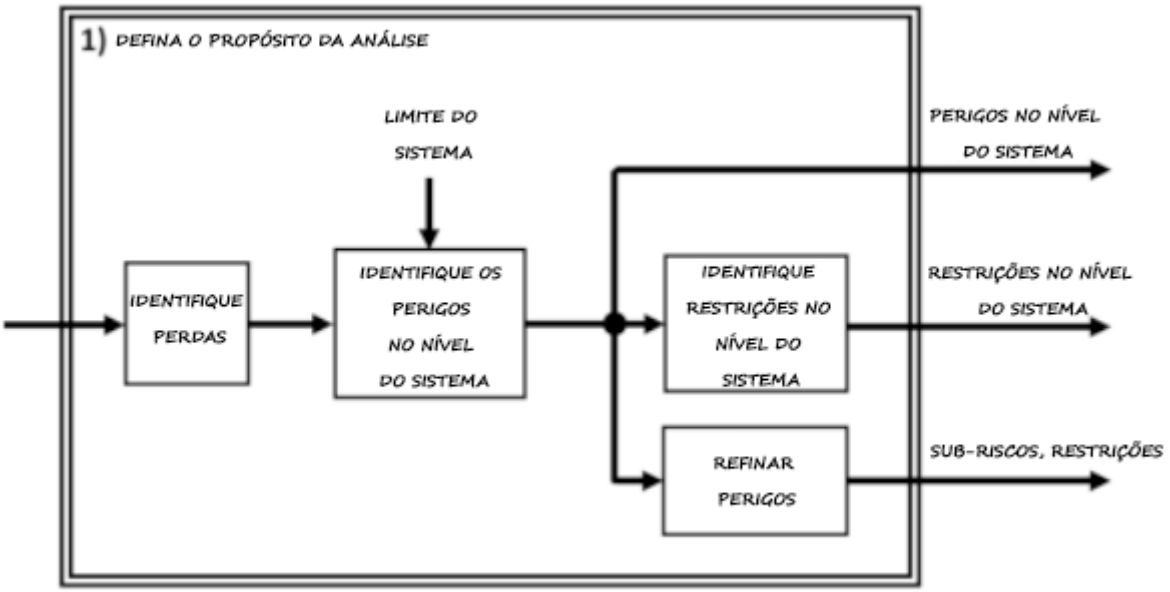
ANÁLISE STPA PARA UM SUBSISTEMA DE CONTROLE DE ACESSO BASEADO EM FUNÇÕES (RBAC)

Última atualização: 27/05/2024

1. Defina o propósito da análise



1.1 Defina e estruture o problema

Nos sistemas de software, especialmente aqueles que processam informações delicadas e/ou sigilosas, os processos de autenticação e autorização são de extrema importância. Eles asseguram que somente usuários devidamente autenticados e com as permissões corretas tenham acesso a recursos específicos ou possam executar certas operações no sistema.

Um método muito eficiente para implementar esses processos é o Controle de Acesso Baseado em Papéis (RBAC), onde os usuários são designados a papéis específicos e os direitos de acesso são concedidos com base nesses papéis. O RBAC é um método muito adotado para administrar o acesso a recursos dentro do sistema de informações de uma organização, empresa, site e afins, atribuindo permissões aos usuários com base em seus papéis, ao invés de definir permissões individuais para cada usuário. Este método traz várias vantagens, como aprimoramento da segurança e simplificação do gerenciamento dos direitos de acesso.

Partindo desse ponto, o objetivo dessa análise STAP é criar uma espécie de roteiro para sistemas RBAC, que poderá ser reutilizada em outros sistemas RBAC.

1.2 Partes interessadas

S1: Usuários

Os usuários são todos que, de alguma forma, interagem com a aplicação web. Podem ser funcionários, clientes, administradores ou outros usuários autorizados.

S2: Administradores

São os responsáveis por toda gestão do sistema RBAC dentro da aplicação web, além de suporte ao usuário e problemas relacionados ao login.

S3: Desenvolvedores

São os responsáveis por todo ecossistema de criação do RBAC, desde o desing, implementação e manutenção.

S4. Pessoal de Segurança

São os stakeholders preocupados com a segurança da aplicação. Eles que garantem a integridade dos dados.

S5. Autoridades regulatórias

Em alguns ramos, a aplicação RBAC conta com autoridades regulatórias na aplicação.

1.3 Propósito e objetivos do sistema

SG-01: Garantir Autenticação e Autorização

- O sistema deve garantir que usuários acessem com suas credenciais, de modo a terem acesso apenas às suas respectivas funcionalidades.

SG-02: Manter a Confidencialidade e Integridade dos Dados [S4]

- O sistema RBAC deve considerar as funções de cada usuário e garantir que cada um execute apenas suas funções. Com isso, **[S4]** garante também a integridade do sistema, limitando que ações indevidas sejam tomadas por quaisquer usuários.

SG-03: Facilitar a Gestão de Funções [S2]

- Similar à um AD em windows server, o sistema RBAC deve fornecer aos administradores as ferramentas necessárias para gerenciar as funções de todos usuários do sistema, seja na atualização, exclusão ou criação de novos usuários e funções específicas.

SG-04: Garantir Disponibilidade [S3]

- O RBAC, de acordo com as funções de **[S3]** deve garantir a disponibilidade do sistema para seus usuários.

SG-05: Garantir o Cumprimento das Leis [S5]

- O sistema deve seguir estritamente as leis dos países onde será implantado, de acordo com **[S5]**.

1.4 Suposições

AS-1: Arquitetura e Limites do Sistema

- Presume-se que **[S3]** tenha projetado o sistema RBAC como um componente modular, capaz de se interligar aos sistemas web de maneira que interaja com as interfaces de usuário, bancos de dados e os limites nos níveis de funções.

AS-2: Ambiente Web

- O RBAC roda dentro de uma aplicação web e é esperado conexão com a rede, servidor seguro com banco de dados e compatibilidade com o navegador web utilizado pelo usuário.

AS-3: Funções

- Presume-se que **[S3]** tenha projetado que os usuários tenham suas respectivas funções, permissões e níveis de acesso dentro da aplicação RBAC web.

AS-4: Conformidade Regulatória e Legal

- Presume-se que o sistema RBAC siga as leis do país onde será executado, garantindo o cumprimento dos regulamentos e padrões do setor.

AS-5: Escalabilidade e Desempenho

- Presume-se que o sistema seja capaz de se expandir de acordo com o número crescente da base de usuários, mantendo assim o desempenho aceitável para possíveis acessos simultâneos sem comprometer a segurança.

1.5 Identifique perdas e acidentes

L1: acesso não autorizado a dados sensíveis.
L2: alterações não autorizadas aos dados.
L3: indisponibilidade do sistema devido a falhas de segurança.
L4: ações maliciosas irrastreáveis.
L5: perda de confiança dos usuários.

1.6 Identifique riscos do sistema e restrições de nível de sistema

1.6.1. Identifique riscos do sistema

H1: o sistema não verifica se o usuário está autenticado. **[L1, L2, L3, L5]**
H2: o sistema não verifica a função do usuário autenticado. **[L1, L2, L5]**
H3: o sistema não monitora o uso de suas funcionalidades (registro de logs). **[L4, L5]**
H4: o sistema não implementa criptografia aos dados sensíveis. **[L1, L5]**

1.6.2. Identifique restrições do sistema

SC1: o sistema deve verificar se o usuário está autenticado. **[H1]**
SC2: o sistema deve verificar qual a função (*role*) do usuário autenticado. **[H2]**
SC3: o sistema deve monitorar o uso de suas funcionalidades. **[H3]**
SC4: o sistema deve criptografar os dados sensíveis. **[H4]**

2. Modelagem da Estrutura de Controle (STPA Step 2)

2.1 Componentes do sistema

- **C1: Controlador de Autenticação**

Responsável por verificar a identidade dos usuários que tentam acessar o sistema.

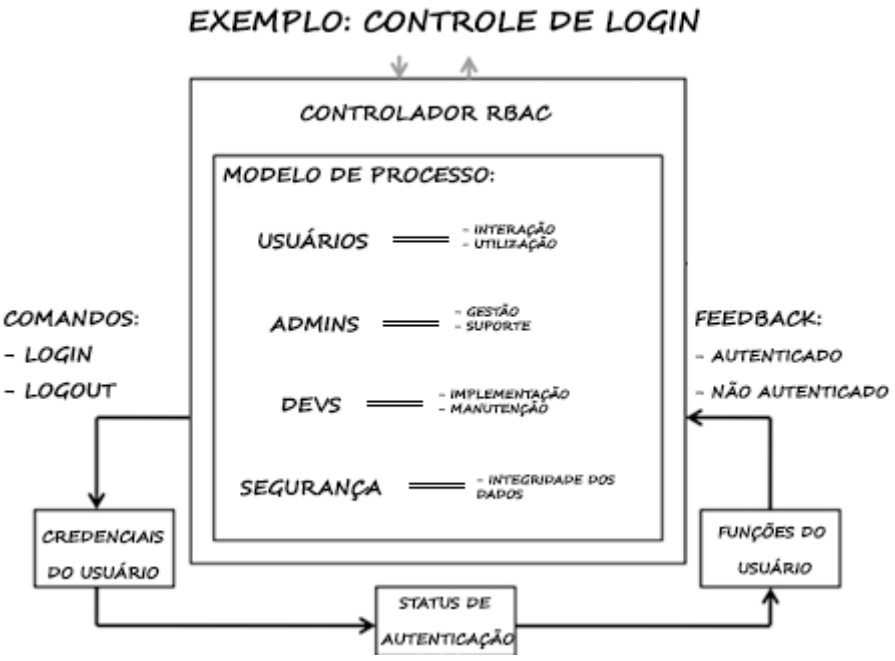
- **C2: Controlador de Autorização**
  Responsável por conceder direitos de acesso com base em funções e permissões predefinidas.
- **C3: Interface de Gerenciamento de RBAC**
  Responsável por gerenciar funções, permissões e contas de usuário dentro do subsistema RBAC.

2.2 Componentes/Controladores, várias de controle do processo e valores das variáveis

Componente/Controlador	Variáveis de controle do processo	Valores das variáveis de controle

C1	`Credenciais do Usuário`
	
	`Status de Autenticação`
		`[Valida, Inválida]`
		
		`[Autenticado, Não autenticado]`

C2	`Funções do Usuário`	`[Função A, Função B, ..., Função N]`
C3	`Configuração do RBAC`	`[Atualizada, Não alterada]`



2.3 Algoritmo de controle

Componente	Algoritmo
C1	**SE** credenciais são válidas **ENTãO** {

	status de autenticação = autenticado
	} **SENãO**{
	status de autenticação = não autenticado
	}

C2	**SE** usuário tem autorização para acessar recurso **ENTãO**
	{
	Acesso permitido
	} **SENãO** {
	Acesso negado
	}

C3	**SE** configuração do RBAC foi atualizada **ENTãO** {
	Comunica atualização para o controlador de autorização
	}

2.4 Responsabilidades dos componentes

Componentes/Controladores		
R1	Controlador de autenticação - verifica credenciais de autenticação, modifica status de autenticação	**SC1, SC2**
R2	Controlador de autorização - gerencia o acesso aos recursos do sistema com base na função do usuário autenticado	**SC1, SC2, SC3**
R3	RBAC Management Interface - armazena as configurações do RBAC, e propaga suas mudanças quando houver	**SC4**

2.5 Estrutura de controle a nível de sistema

[Controlador de Autenticação] <-> [Controlador de Autorização] <-> [Interface de Gerenciamento de RBAC]

2.6 Estrutura de Controle (Refinamento/Aproximação da Estrutura de Controle em Nível de Sistema a ser Analisada)

1. O usuário solicita acesso a um recurso/funcionalidade.
2. O Controlador de Autenticação verifica as credenciais do usuário.
3. O Controlador de Autenticação define o status de autenticação.
4. Se a autenticação for bem-sucedida:

4.1. O Controlador de Autenticação envia o status de autenticação para o Controlador de Autorização.

4.2. O Controlador de Autorização verifica se o usuário possui as funções/permissões necessárias para a ação solicitada.

4.3. Se autorizado, conceder acesso.

4.4. Se não autorizado, negar acesso.

5. Se a autenticação não for bem-sucedida:

5.1. O Controlador de Autorização nega o acesso.

3. Identificar Ações de Controle Inseguras (Passo 3 do STPA)

3.1 Identificar Ações de Controle Inseguras - UCAs

Ação de Controle	Não fornecer causa perigo	Fornecer causa perigo	Muito cedo, muito tarde, fora de ordem	Parado muito cedo, Aplicado por muito tempo
CA1: Verificação de credenciais (C1)	**UCA-1: [C1]** não verifica credenciais **[H1]**	**UCA-2: [C1]** verifica credenciais de maneira incorreta **[H2]**	**UCA-3: [C1]** leva muito tempo para autenticar **[H1]**	N/A
CA2: Verificação de permissões (C2)	**UCA-4: [C2]** não verifica permissões do usuário **[H2]**	**UCA-5: [C2]** verifica as permissões de maneira incorreta **[H2]**	**UCA-6: [C2]** leva muito tempo para verificar as permissões **[H2]**	N/A
CA3: Gerenciamento das configurações do RBAC (C3)	**UCA-7: [C3]** não gerencia corretamente as configurações do RBAC **[H2, H3]**	**UCA-8: [C3]** fornece configurações incorretas sobre o RBAC **[H2]**	**UCA-9: [C3]** leva muito tempo para fornecer a configuração ou atualizar a configuração do RBAC **[H2]**	N/A

3.2 Identificar Restrições de Controladores

Ações de Controle Sem Segurança	Restrição(s) do Controlador
UCA-1	**C-1** deve verificar as credenciais
UCA-2	**C-1** deve verificar as credenciais de maneira correta
UCA-3	**C-1** deve verificar as credenciais em um tempo viável
UCA-4	**C-2** deve verificar as permissões do usuário
UCA-5	**C-2** deve verificar corretamente as permissões do usuário
UCA-6	**C-2** deve verificar as permissões em um tempo viável
UCA-7	**C-3** deve gerenciar corretamente as configurações do RBAC

UCA-8	**C-3** deve sempre fornecer as configurações corretas e atualizadas
UCA-9	**C-3** deve atualizar e fornecer as configurações do RBAC em um tempo viável

Passo 4: Identificar Cenários de Perda (STPA Passo 4)

UCA-1: O sistema não verifica as credenciais

Cenário	Fator causal associado	Recomendações	Justificativa
Falha no login com credenciais corretas	Servidor está offline	● Manutenções periódicas na rede do servidor ● Servidores distribuídos	O servidor precisa estar sempre disponível
Login com credenciais incorretas	O **[C1]** não está sendo acionado	Revisão no código	As funcionalidades devem estar disponíveis apenas para usuários credenciados