Modelo de ameaças

Registro das ameaças

> Porque ninguém registrou para que servia o status da conta de bitcoins e seus mecanismos de proteção, um desenvolvedor implementou o reset de MFA conforme especificado na história do time. Ele entregou em produção e meses depois a corretora de bitcoins faliu.

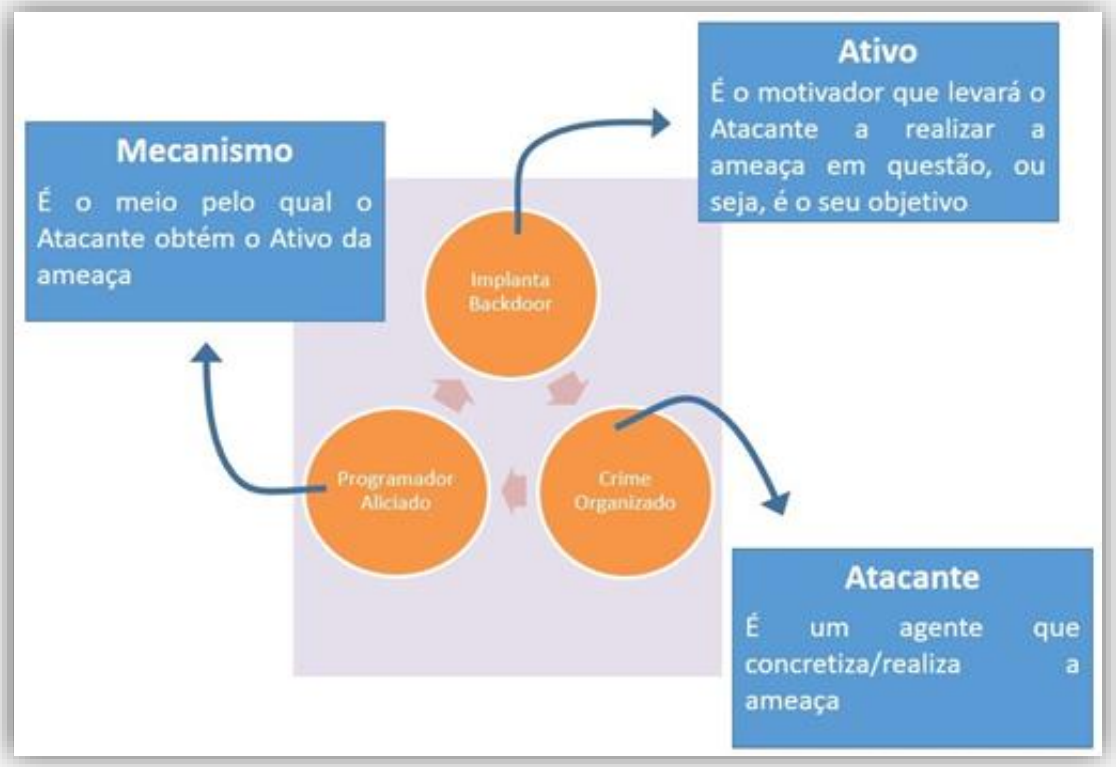
Método de registro de ameaças

Para apresentar o método para o registros das ameaças, vamos tomar como base uma micro modelagem feita analisando-se apenas as informações dadas pela matéria da Veja que apresentou o caso da Máfia do ferro-velho. Assim além de discutir o método de registro, é possível exercitar o raciocínio das ameaças ainda mais.

Método de registro de ameaças

Uma ameaça é composta por três componentes base: Atacante, Mecanismo e Ativo. Estes três componentes são representados graficamente por círculos, compondo a trinca da ameaça.

Esta trinca deve ser interpretada da seguinte maneira: "O Atacante através de um Mecanismo, obtém o Ativo", como por exemplo: "O Crime Organizado através de um Programador Aliciado, Implanta um Backdoor". Desta forma a ameaça é uma representação gráfica de um passo do cenário de ataque.



Método de registro de ameaças

Atacante

O *Atacante* é o agente que realiza ações maliciosas com a motivação de obter um retorno (mesmo que as vezes indireto) financeiro em 99% dos casos.

Mecanismo

O *Mecanismo* é o meio pelo qual o *Atacante* obtém o *Ativo da Ameaça*. Na maioria das ameaças, o *Atacante* utiliza como *Mecanismo* recursos computacionais, mas também pode vir a utilizar recursos humanos. Os meios utilizados são inúmeros, e não estão limitados aos sistemas, abuso de processos da empresa, aliciamento de funcionários. Podendo também utilizar de mais de um meio dependendo do objetivo.

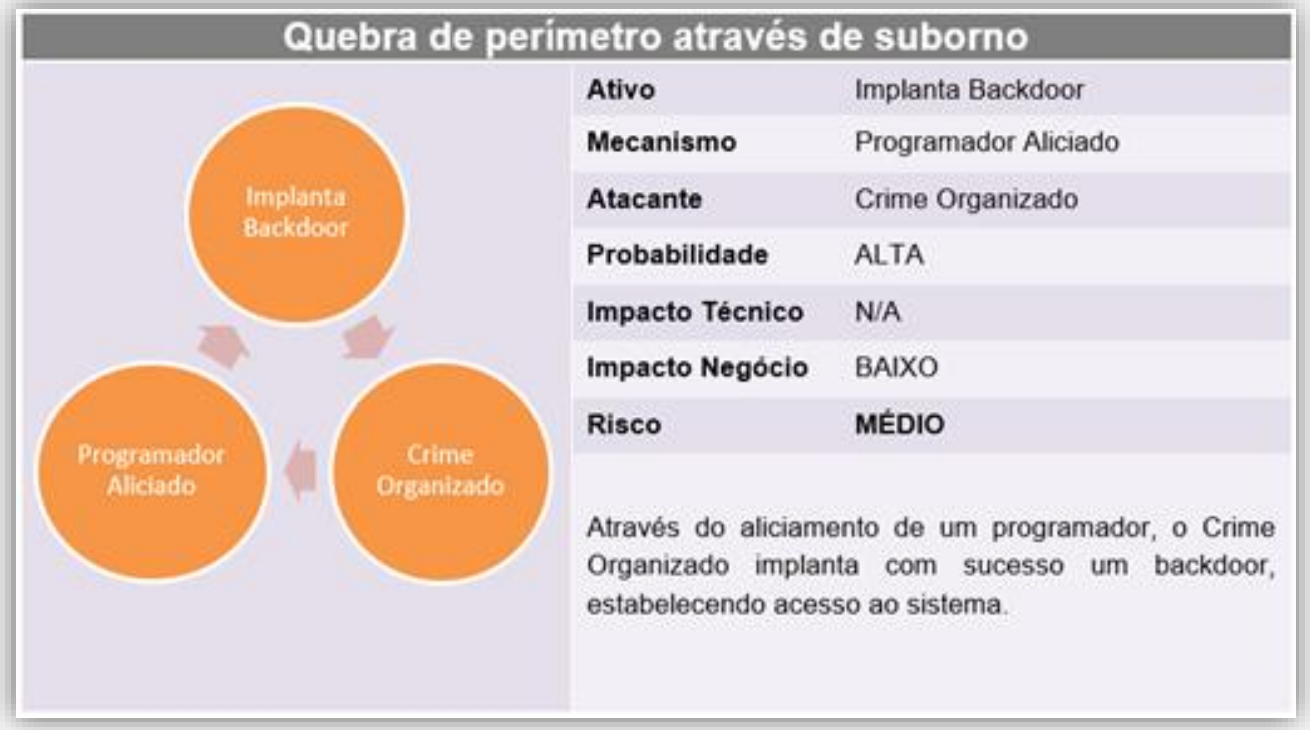
Ativo

O *Ativo* é o motivador que levará o *Atacante* realizar a ameaça em questão, ou seja, é o seu objetivo. O *Ativo* obtido em uma ameaça pode se tornar um *Mecanismo* em outra ameaça.

Método de registro de ameaças

Composição

A ameaça é descrita através de três componentes base e de componentes de risco. Todos os componentes são dispostos na ficha da ameaça.



Método de registro de ameaças

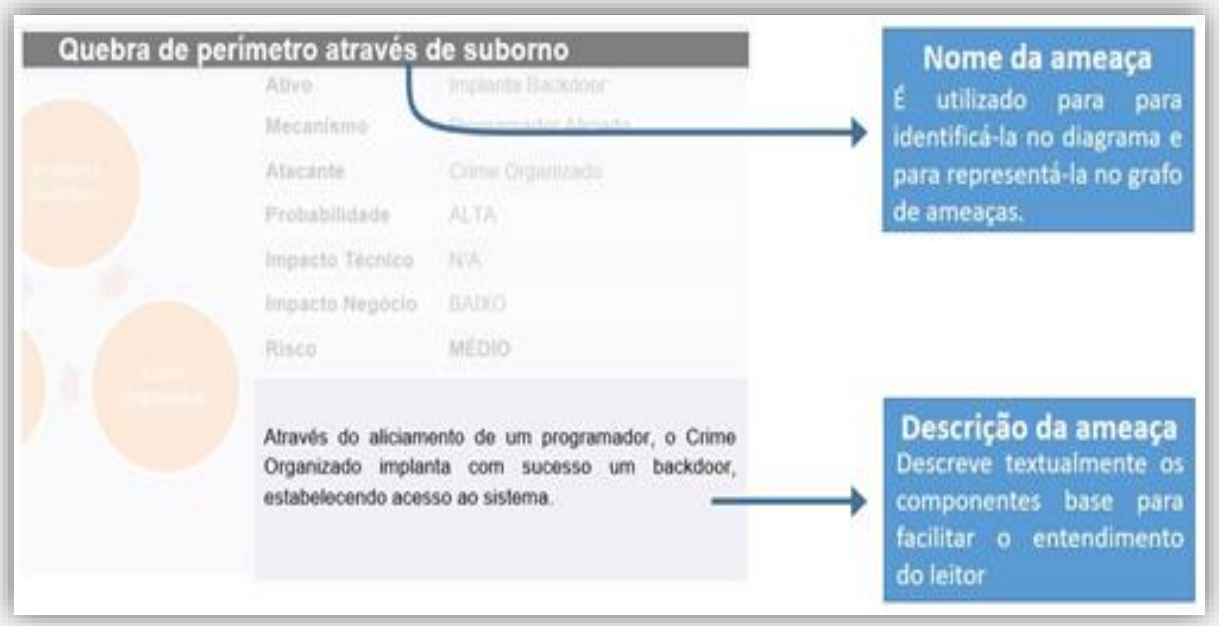
Além dos componentes base, os itens *Nome da ameaça* e *Descrição da ameaça* também são importantes para compreender a ameaça.

Nome da ameaça

O *Nome da ameaça* é o menor resumo de uma ameaça. É utilizado para identificá-la e também para representá-la no *Grafo de ameaças*.

Descrição da ameaça

A *Descrição da ameaça* descreve textualmente os componentes base para facilitar o entendimento do leitor. Em alguns casos, insere alguns detalhes que não são possíveis de representar na trinca.



Método de registro de ameaças

Grau de risco

A representação gráfica dos componentes base é colorida de acordo com o grau de risco da ameaça, que é obtido através da qualificação do mesmo.

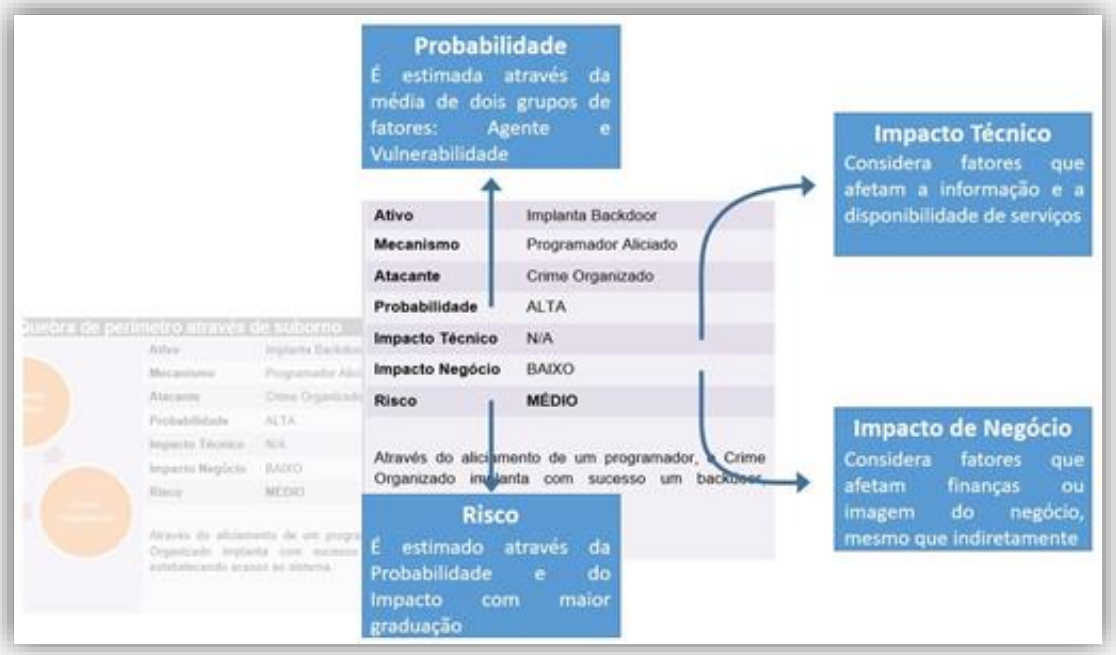
A qualificação é calculada com base em três aspectos: *Probabilidade*, *Impacto Técnico* e *Impacto de Negócio*.

Os aspectos de risco (*Probabilidade*, *Impacto Técnico* e *Impacto de Negócio*) e a metodologia para obter o grau de risco estão descritos no subtópico *Qualificação de ameaças*.

Método de registro de ameaças

A metodologia utilizada para qualificação das ameaças é baseada na metodologia da OWASP (OWASP *Risk Rating Methodology*), que pode ser acessada através do endereço https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

Cada um dos três aspectos de risco é estimado através da média de fatores. Cada fator assume um valor numérico entre zero (0) e nove (9).



Método de registro de ameaças

Probabilidade

A *Probabilidade* é estimada através da média de dois grupos de fatores: *Agente da ameaça*, que possui fatores relacionados ao *Atacante*; e *Vulnerabilidade*, que possui fatores sobre a descoberta e a exploração da vulnerabilidade pelo *Atacante*.

Impacto Técnico e Impacto de Negócio

O *Impacto Técnico* é um aspecto que considera fatores que afetam a informação e disponibilidade de serviços. Enquanto o aspecto *Impacto de Negócio* considera fatores que afetam as finanças ou a imagem do negócio, mesmo que indiretamente.

Ambos os aspectos de *Impacto* também são estimados através da média de fatores. Entretanto, a média de ambos é comparada, e o *Impacto* que apresentar o maior valor é selecionado para calcular o grau do risco.

Método de registro de ameaças

	Probabilidade		Impacto	
	Agente	**Vulnerabilidade**	**Impacto Técnico**	**Impacto de Negócio**
Fatores	Nível de habilidade	Facilidade em ser descoberta	Perda de confiabilidade	Dano financeiro
	Motivação	Facilidade em ser explorada	Perda de integridade	Dano de reputação
	Oportunidade	Experiência	Indisponibilidade	Falta de aderência a normas
	Tamanho	Detecção de intruso	Perda de rastreabilidade	Violação de privacidade

Método de registro de ameaças

A média de cada aspecto (Impacto X Probabilidade) resulta em uma graduação.

- Entre zero (0) e menor que três (3), qualifica-se como Baixo;
- Entre três (3) e menor que seis (6), qualifica-se como Médio;
- Entre seis (6) e nove (9), o aspecto é qualificado como Alto

Risco

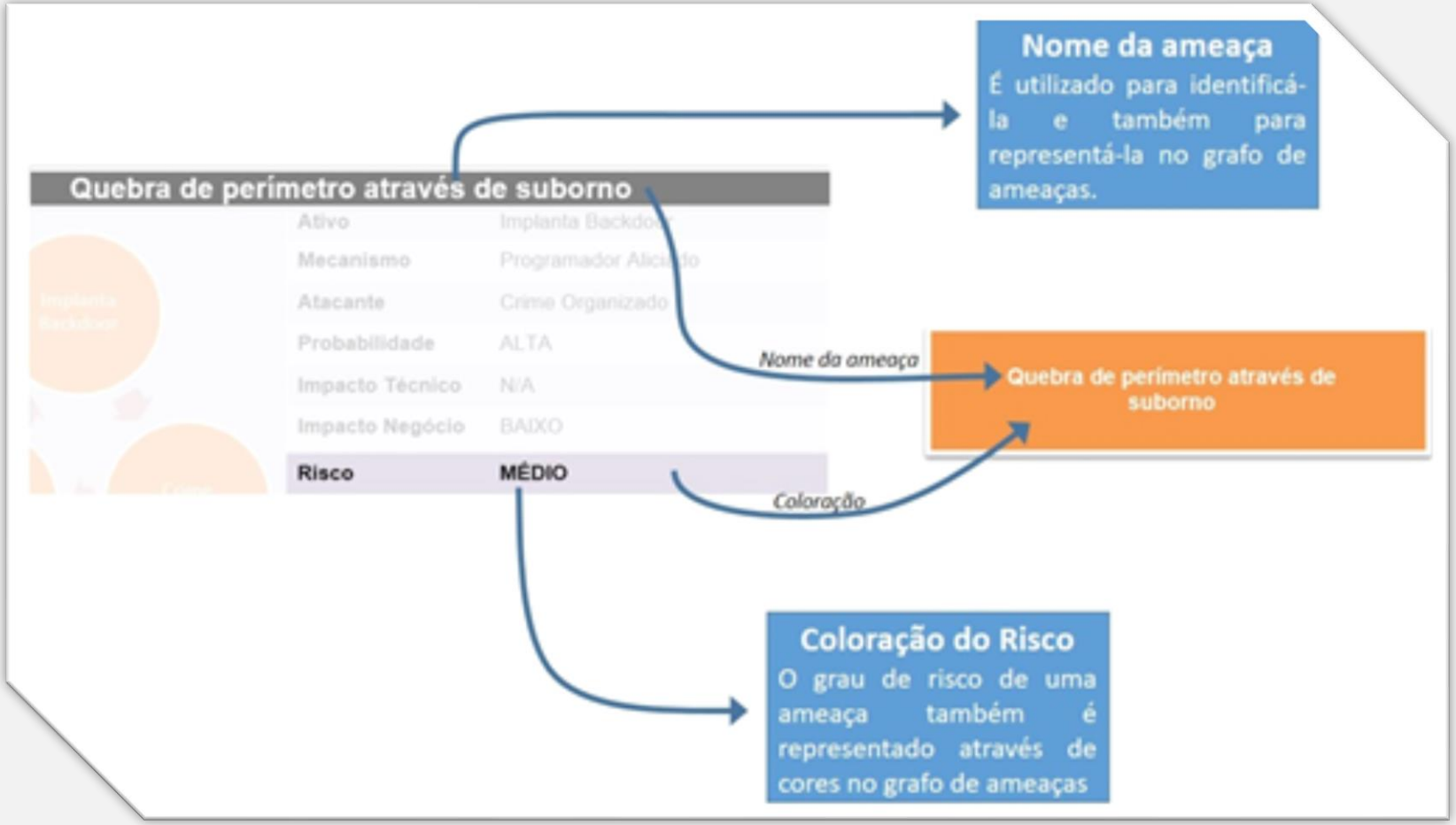
O grau de risco é obtido através da correlação entre a graduação da *Probabilidade* e do *Impacto*, refletido na matriz de risco abaixo.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Método de registro de ameaças

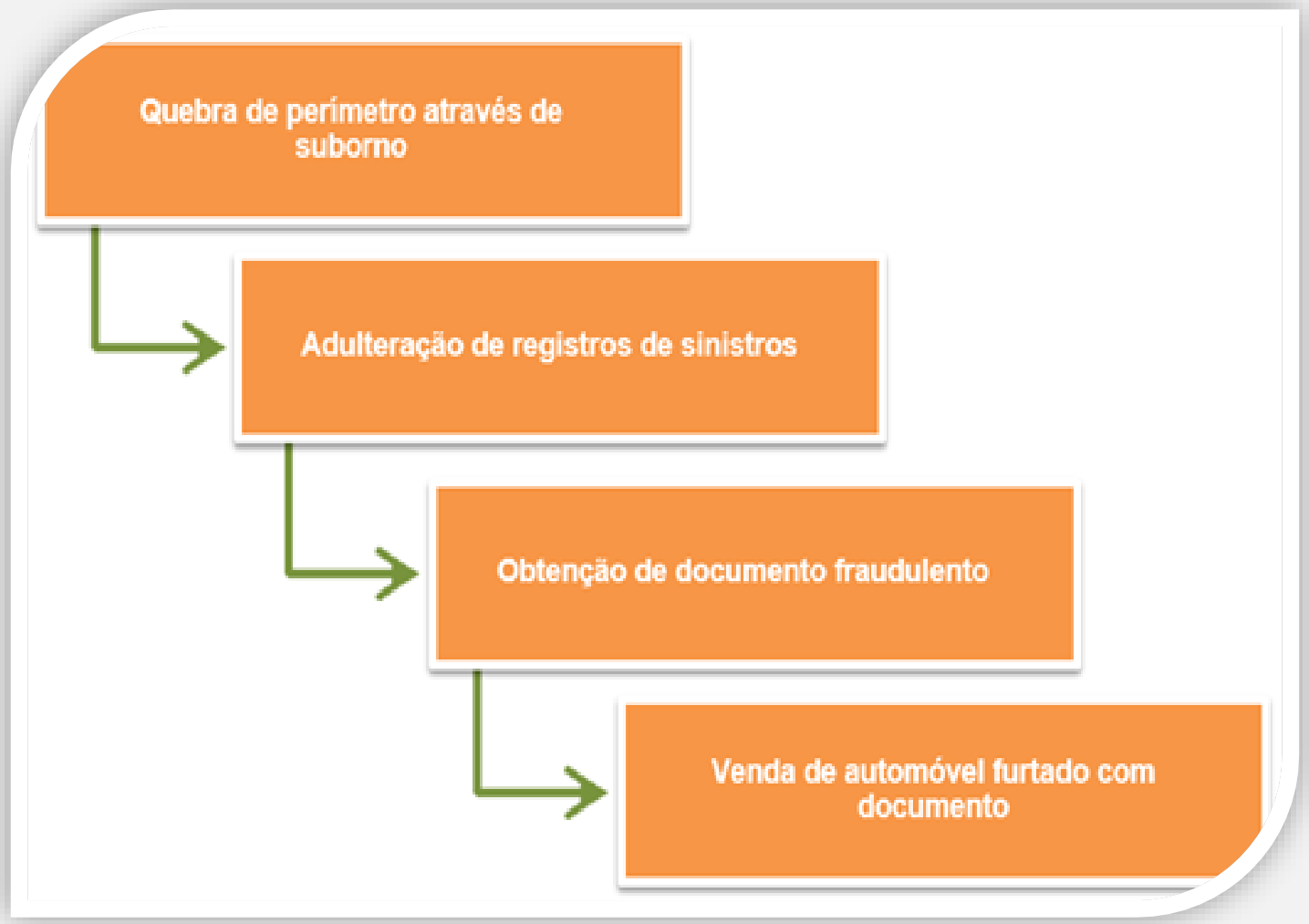
No *Grafo de ameaças*, uma ameaça é representada através de um retângulo. Assim como na representação dos componentes base, a ameaça no *Grafo de ameaças* possui uma coloração de acordo com seu grau do risco.



Método de registro de ameaças

Através do *Grafo de ameaças* é possível observar a sequência de passos que um *Atacante* realiza até obter o resultado final do ataque, que em geral, é representado pelo último nível do grafo.

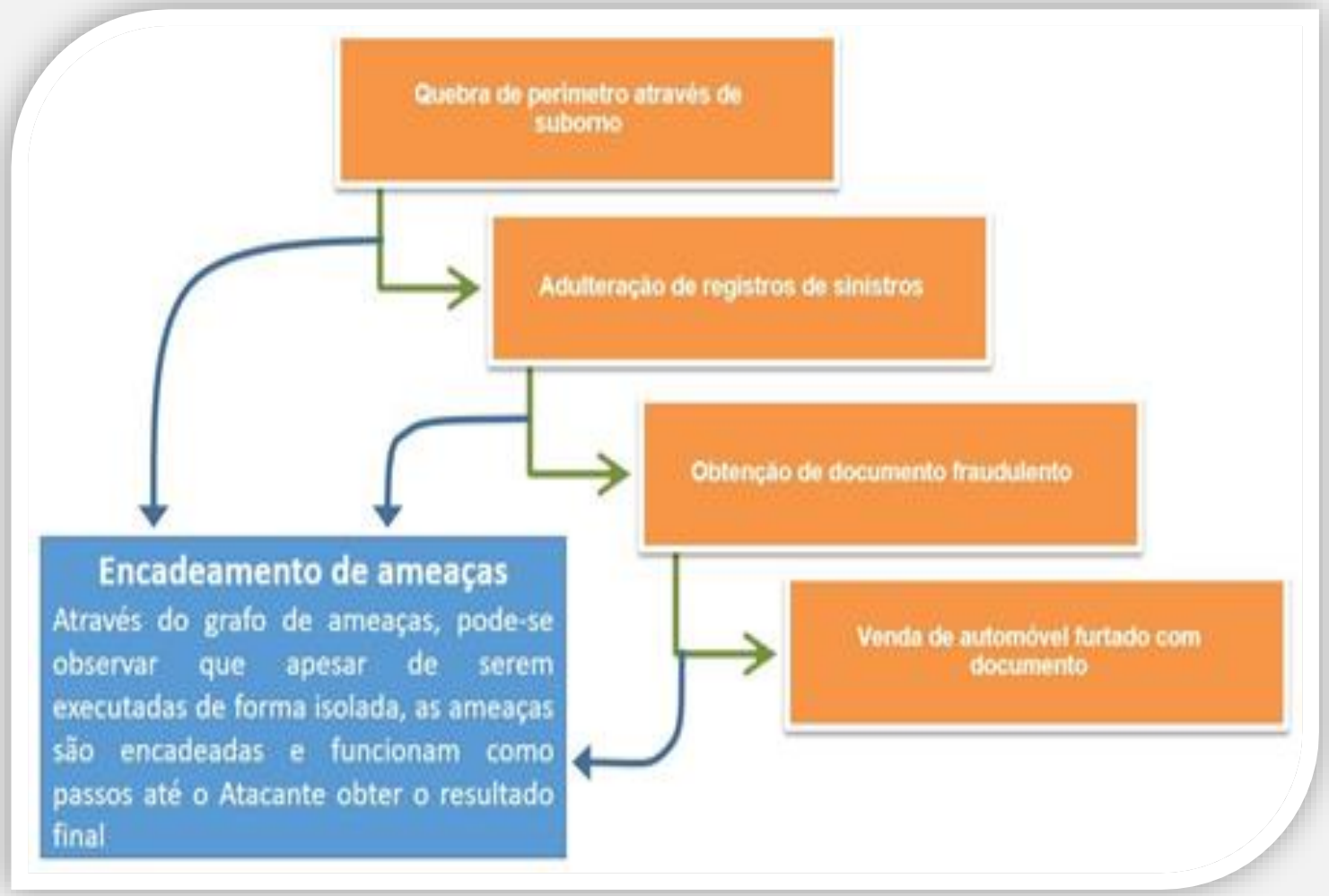
Note que, a partir do processo descrito em uma matéria jornalística, é possível derivar alguns possíveis caminhos de ataque.



Método de registro de ameaças

Em cada ameaça o *Atacante* visa obter um *Ativo*, que é o seu objetivo, mas o *Ativo* obtido pode não ser o objetivo final. Uma vez obtido, o *Ativo* de uma ameaça pode se tornar um *Mecanismo* em outra ameaça. Por esse fato as ameaças podem ser encadeadas.

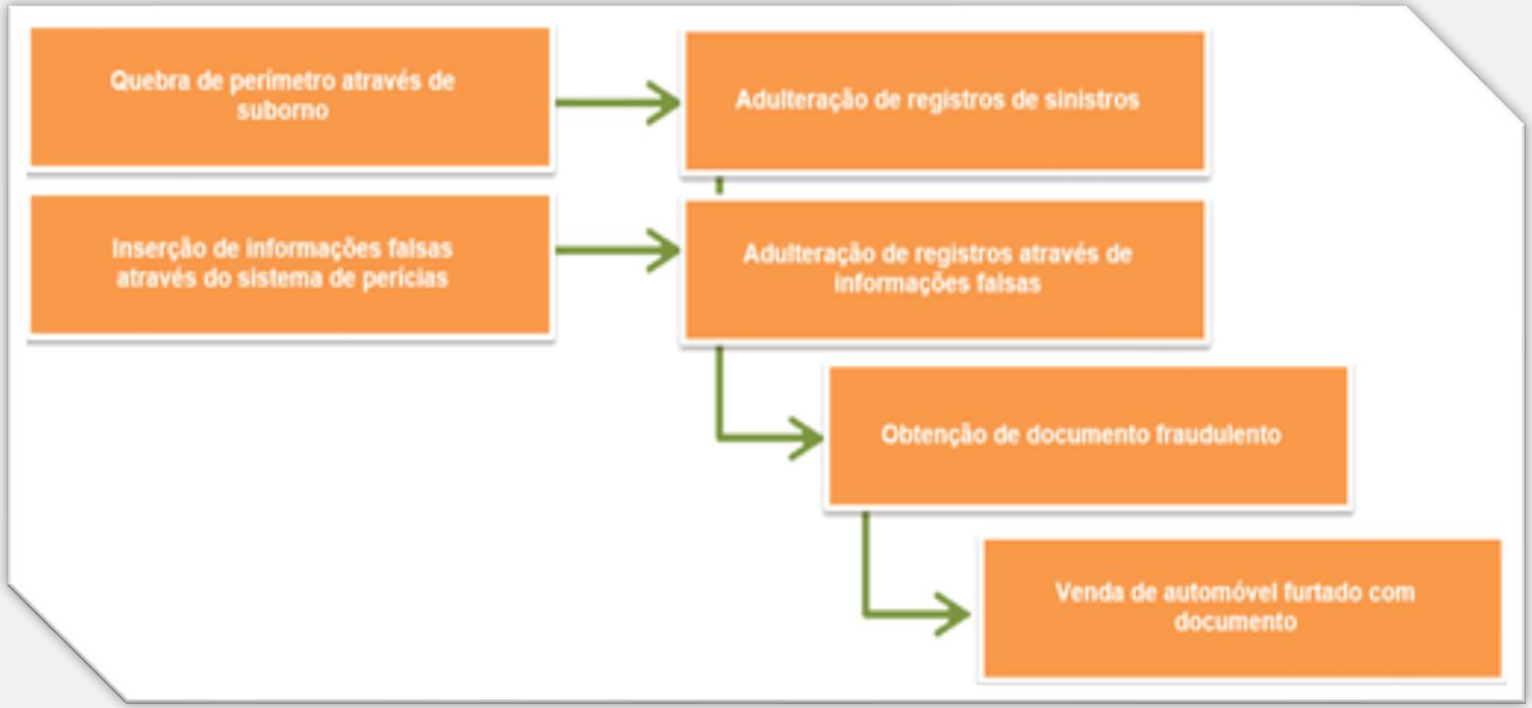
O encadeamento das ameaças é representado no *Grafo de ameaças* através de setas verdes.



Método de registro de ameaças

O grafo também possibilita visualizar que uma ou várias ameaças iniciais podem ser utilizadas pelo *Atacante* para obter o resultado final de um ataque.

Em conjunto com a coloração de risco, a visualização das ameaças em um grafo visa aumentar a eficácia da priorização de medidas de segurança, bem como análise de causa raiz.



Método de registro de ameaças

Alternativamente a construção do grafo com base em elementos simples disponíveis em praticamente qualquer editor de texto, pode-se lançar mão de uma estrutura como a dos mapas mentais para elaboração da apresentação do grafo. Entretanto, vale um alerta. O modelo do mapa mental torna muito mais visível as interconexões entre os passos de um modelo, mas dificulta o foco nas ameaças em si, pois o nome da ameaça tente a ser grande e fica, por vezes, desproporcional, dificultando a leitura. Como os mapas mentais ficamos tentados a "resumir" o nome das ameaças, dificultando a análise do passo a passo de um ataque.