



# **Resolução e classificação de alertas de centros de operações de segurança**

Relatório de Aquisição de conhecimentos

2024 / 2025

**1211131 Pedro Pereira**

**1200799 Rafael Branco**

**1240613 Ricardo Gonçalves**

**1222708 Ricardo Lemos**

**1240156 Svetlana Zamyatina**

**ISEP** INSTITUTO SUPERIOR  
DE ENGENHARIA DO PORTO



# Índice

<b>1</b>	<b><i>Introdução / Objetivos do Desafio</i></b> .....	<b>1</b>
<b>2</b>	<b><i>Fontes de Conhecimento</i></b> .....	<b>3</b>
2.1	Paulo Valdeira.....	3
2.2	Documentos da empresa .....	3
<b>3</b>	<b><i>Sessões de aquisição de conhecimento</i></b> .....	<b>5</b>
3.1	Sessão 1 – 01/10/2024.....	5
3.2	Sessão 2 – 10/10/2024.....	5
<b>4</b>	<b><i>Representação do conhecimento adquirido</i></b> .....	<b>7</b>
4.1	Múltiplas falhas de Login para uma única conta .....	7
4.2	Múltiplos inícios de sessão um utilizador em dispositivos diferentes .....	8
4.3	Alterações efetuadas na firewall.....	10
4.4	Nova conta de Utilizador .....	12
4.5	Os dados do utilizador foram alterados .....	13
<b>5</b>	<b><i>Implementação</i></b> .....	<b>15</b>
<b>6</b>	<b><i>Conclusão</i></b> .....	<b>17</b>
<b>7</b>	<b><i>Bibliografia utilizada</i></b> .....	<b>18</b>
<b>8</b>	<b><i>Lista de terminologia específica</i></b> .....	<b>19</b>

# Índice de Figuras

Figura 1 - Fluxograma múltiplos logins falhados para o mesmo utilizador .....	7
Figura 2 - Fluxograma múltiplos inícios de sessão um utilizador em dispositivos diferentes. ..	9
Figura 3- Fluxograma alteração de regras firewall.....	11
Figura 4 - Fluxograma nova conta de utilizador.....	12
Figura 5 – Fluxograma de alteração de conta .....	14

# Índice de Tabelas

**Não foi encontrada nenhuma entrada do índice de ilustrações.**



# 1 Introdução / Objetivos do Desafio

Os sistemas periciais (SP) são programas criados para imitar o pensamento de especialistas humanos, baseando-se do seu conhecimento em setores específicos [1]. Por meio de uma combinação entre uma base de conhecimento e um mecanismo de inferência, estes sistemas resolvem problemas complexos e tomam decisões informadas. As áreas de aplicação destes sistemas vão desde medicina à engenharia e finanças. Um sistema pericial é composto pela aquisição do conhecimento de um especialista e sua representação, desenvolvimento de um motor de inferência e implementação de uma interface amigável para o utilizador.

O desafio proposto para as unidades curriculares de Paradigmas de Programação em Inteligência Artificial (PPROGIA) e Engenharia do Conhecimento (ENG CIA) é o desenvolvimento de um SP, no contexto da área de cibersegurança.

Desta forma, tendo em conta o background dos membros do grupo optou-se pelo desenvolvimento de um sistema pericial para **resolução e classificação de alertas de centros de operações de segurança (SOC)**. Os SOCs gerem uma grande quantidade de dados e eventos diários, concebendo uma vasta quantidade de alertas provenientes de diferentes ferramentas e sensores [2]. Estes alertas precisam de ser analisados e tratados de acordo com sua criticidade e relevância, para garantir que ameaças reais sejam identificadas e resolvidas a tempo.

O crescente volume de ciberataques e a complexidade das ameaças atuais impõem uma carga significativa sobre os analistas de SOC, que muitas vezes precisam de lidar com grandes quantidades de alertas falsos positivos, além duma ampla gama de cenários de ataques que exigem conhecimento especializado. Isso torna os SP uma solução promissora, pois podem replicar o conhecimento de especialistas em cibersegurança e automatizar parte do processo de triagem e classificação dos alertas [3], [4].

O desenvolvimento deste sistema irá auxiliar os peritos e novatos no processo de diagnóstico melhorando o tempo de resposta a novos alertas. O sistema poderá apontar a causa do problema, sugerindo ações a tomar para a resolução do mesmo.





## 2 Fontes de Conhecimento

A construção de um sistema pericial de sucesso dependerá da quantidade e qualidade do conhecimento fornecido a ele. Nesta seção, vamos explorar as diferentes fontes de conhecimento usadas para alimentar o nosso SP. O grupo selecionou Paulo Valdeira, como perito para o projeto, analista de SOC na empresa *Redshift Global*. Para além disso o grupo teve acesso a certos documentos da empresa que descrevem os processos a tomar no caso da receção de um determinado tipo de alerta.

### 2.1 Paulo Valdeira

Paulo Valdeira é um atual *SOC Manager* da empresa *Redshift Global*. O perito exerceu funções na área de IT (*Information Technology*) há cerca de 21 anos, onde 10 desses anos são representados por atividades na área de SOC. O mesmo esteve cinco anos como analista SOC *tier 1*, três anos nos *tiers 2/3* e os dois últimos anos como *SOC Manager*.

Além da vasta experiência na área deste projeto, o perito apresenta as seguintes formações:

- *ETH Ethical Hacking*
- *CyberOPS*
- *Lead Implementer ISMS – ISSO/IEC 27001:2022*
- *Comptia Security+*

### 2.2 Documentos da empresa

Os documentos da empresa são recursos formais que descrevem procedimentos, políticas e orientações que devem ser seguidos pelos colaboradores no desempenho das suas funções. Esses documentos são fundamentais em várias áreas, pois garantem a consistência na execução de processos, promovem a aplicação de boas práticas e ajudam a mitigar riscos, especialmente em setores críticos como a segurança da informação.

Estes documentos apresentam instruções detalhadas sobre como realizar tarefas específicas. No caso da *Redshift Global*, esses manuais explicam as ações a serem tomadas quando um alerta de segurança é recebido, orientando os analistas de SOC sobre os passos corretos para lidar com incidentes. De modo a ser possível modelar o conhecimento, dividiu-se o mesmo por diferentes casos de uso, onde cada um representa um alerta diferente. Por

sua vez, cada caso de uso tem um diagrama e um conjunto de pontos associados que foram disponibilizados em formato de imagem. Deste modo, o grupo conseguiu guiar-se ao dividir as diferentes imagens pelos elementos, de forma ordenada, onde cada caso de uso desenvolvido foi discutido não só pelos membros do grupo, como com o perito Paulo Valdeira, que deu as suas indicações durante as reuniões semanais.

## 3 Sessões de aquisição de conhecimento

Foram realizadas duas sessões de aquisição de conhecimento com o perito, dia 1 de outubro e dia 10 de outubro de 2024. Segue uma breve descrição do conteúdo da reunião:

### 3.1 Sessão 1 – 01/10/2024

Na primeira sessão com o perito Paulo Valdeira, o grupo realizou uma breve apresentação das ideias iniciais para o projeto, com o objetivo de alinhar as expectativas e direções possíveis. O perito de seguida apresentou-se falando um pouco do seu histórico profissional e do trabalho que estava a desenvolver atualmente como analista de SOC, apresentando uma série de mais de 100 casos de uso que podem ser enfrentados no exercício da função de analista de SOC. Dada a amplitude desse leque de possibilidades, o grupo, em conjunto com o perito, decidiu concentrar-se em cinco casos de uso específicos. O perito forneceu uma breve explicação sobre cada um desses casos, acompanhada da documentação pertinente da empresa.

Posteriormente, cada caso de uso foi atribuído a um elemento do grupo e foi combinado que cada elemento do grupo ia elaborar durante a semana um diagrama *workflow*. O objetivo seria que, na próxima reunião, cada integrante apresentasse o seu caso ao perito para revisão e aperfeiçoamento, promovendo assim o refinamento do conhecimento exposto através da análise desses diagramas.

### 3.2 Sessão 2 – 10/10/2024

Esta sessão iniciou com uma breve apresentação do que iria ser tratado na mesma e uma pequena introdução do que fora feito. Cada um dos elementos havia desenhado um diagrama que representava o conhecimento associado aos diferentes alertas, portanto, os mesmos foram apresentados ao perito Paulo Valdeira, de modo que pudessem ser validados baseado no seu conhecimento.

Após a validação por parte do perito, foi possível realizar uma pequena demonstração do que seria a aplicação desenvolvida no modo pergunta-resposta, visto a integração entre os módulos de *frontend* e *backend-drools* já estar desenvolvida e com um pequeno exemplo apresentável.

Concluiu-se a sessão com os objetivos para a semana seguinte e com as melhorias não só nos diagramas, como no projeto de um modo geral.





caso contrário, procede-se a um conjunto de passos para controlar novamente o acesso à conta.

Caso o analista não conheça o utilizador, procede-se à triagem do alerta, a partir da deteção dos IPs e a sua quantidade, como também a nacionalidade e a recorrência. Tipicamente, estes casos são enviados para o *Helpdesk* onde, neste caso, está representado pelo texto “Abrir caso”. Após a abertura do caso, o *Helpdesk* faz o mesmo processo de reconhecimento da pessoa e a resolução seria a mesma, caso contrário verifica as geopolíticas associadas, procede ao bloqueio do/dos IPs e realiza o processo de recuperação e controlo de conta. Este processo conta com o bloqueio temporário da conta, redefinição da *password*, revisão das permissões e a implementação de mecanismos de autenticação mais fortes.

## **4.2 Múltiplos inícios de sessão um utilizador em dispositivos diferentes**

A Figura 2 é um fluxograma que representa um processo de avaliação de atividade de login simultâneo em várias localizações ou endereços IPs, para identificar se há comportamento suspeito ou malicioso em contas de utilizadores.

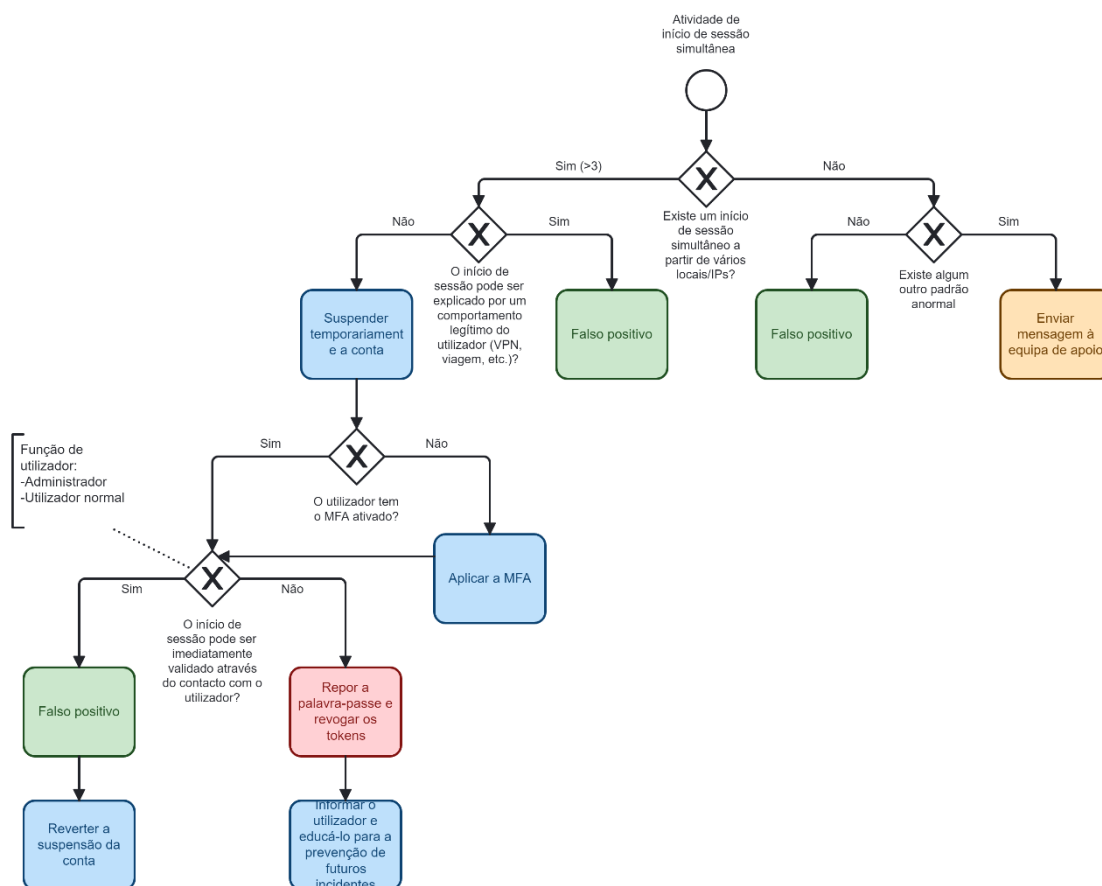


Figura 2 - Fluxograma múltiplos inícios de sessão um utilizador em dispositivos diferentes.

O fluxo começa com a identificação de atividades de login simultâneo por parte de um utilizador. Se houver mais de 3 logins simultâneos (em diferentes localizações ou IPs), o sistema considera que pode haver uma tentativa de acesso suspeita. O número >3 refere-se à quantidade de logins simultâneos que estão a acontecer a partir de diferentes locais ou endereços IPs. Caso não haja mais de 3 logins, segue-se para verificar outros padrões anormais de comportamento. Se houver um padrão anormal no comportamento do login, uma mensagem é enviada à equipa de suporte para investigar mais a fundo, caso contrário o caso é fechado como falso positivo.

Se houver mais de 3 logins simultâneos, de seguida verifica-se se estes podem ser explicados por comportamento legítimo (como VPN, viagens ou outro motivo válido), o resultado é falso positivo se o comportamento for verificado. Se não puder ser explicado, o próximo passo é suspender temporariamente a conta para evitar possíveis riscos e garantir que o utilizador tenha autenticação multifator ativada.

Por fim verifica-se se início de sessão pode ser validado através do contacto com o utilizador. Se o login puder ser validado ao entrar em contacto com o utilizador, é considerado

um falso positivo e a suspensão da conta é revertida. Se o login não puder ser validado, a palavra-passe do utilizador é reposta e os tokens de sessão são revogados. Além disso, o utilizador é informado e educado sobre como prevenir futuros incidentes de segurança.

### **4.3 Alterações efetuadas na firewall**

No fluxograma seguinte (Figura 3) encontra-se representado o processo para verificar as alterações efetuadas numa firewall e se as mesmas podem ou não representar um perigo para o negócio. Com esta representação é possível saber quais os passos a seguir em determinadas situações e qual a melhor forma de intervir e de resolver o problema encontrado.

Assim que um novo alerta é lançado cabe ao analista SOC fazer a análise do mesmo, com o objetivo de encontrar algo que indique atividade suspeita. Se forem detetadas alterações na firewall é necessário perceber se estas foram feitas por uma fonte confiável e segura.

Para isso pode ser necessário proceder a análise de informação que possa tornar possível perceber se alteração foi efetuada de uma forma legítima ou com um objetivo malicioso.

Após a avaliação das alterações e do objetivo das mesmas é necessário proceder a ações de mitigação daquelas que podem ser as vulnerabilidades ou configurações incorretas que terão sido exploradas, de forma a restabelecer o normal funcionamento do sistema.



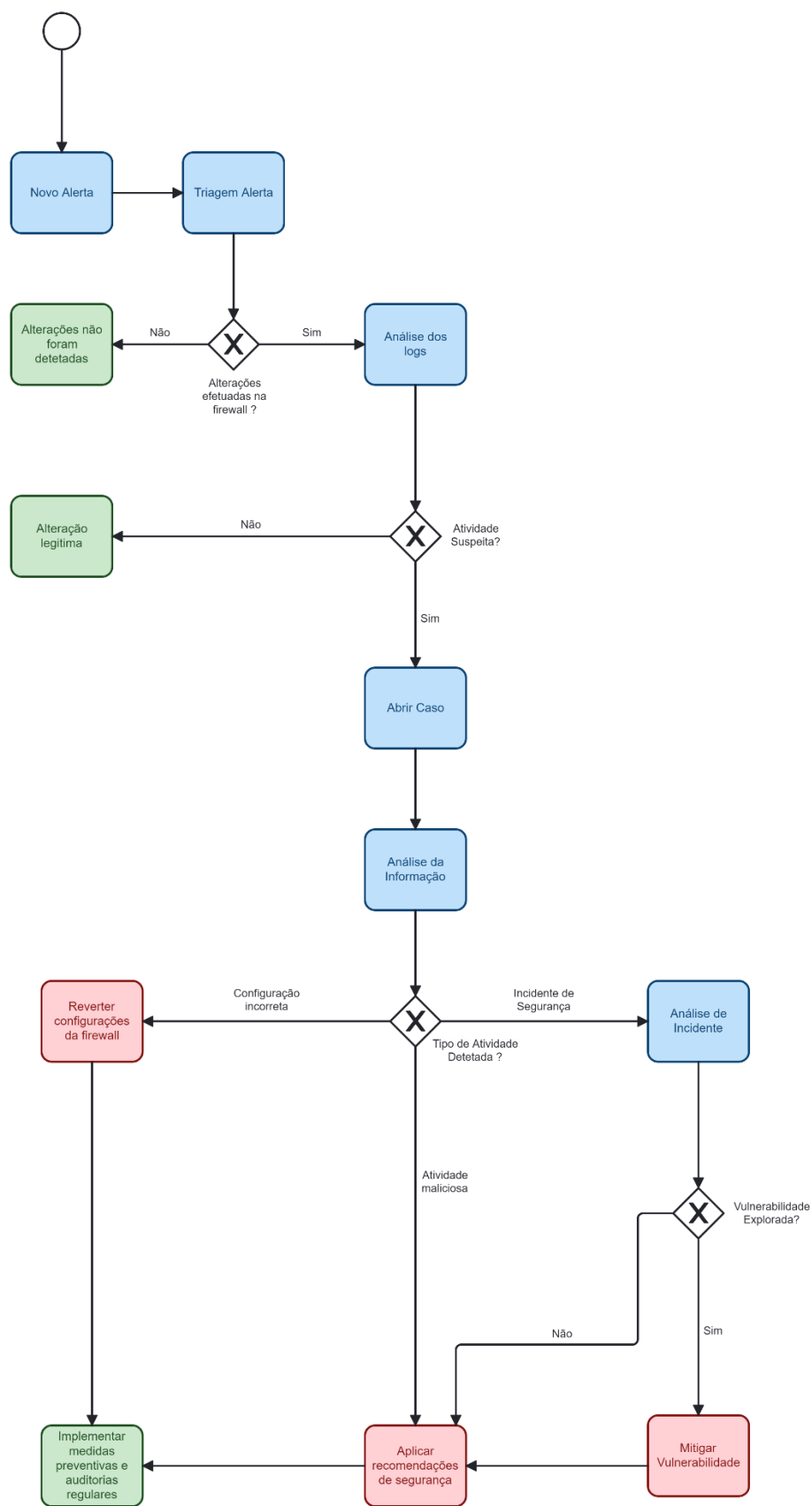


Figura 3- Fluxograma alteração de regras firewall

## 4.4 Nova conta de Utilizador

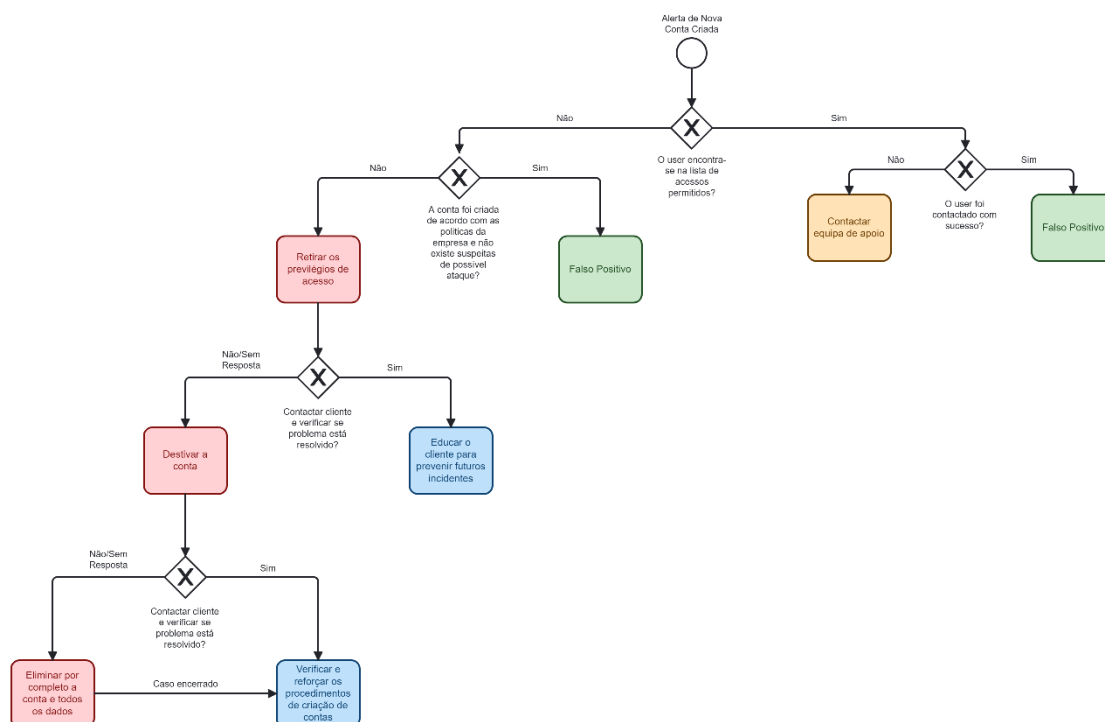


Figura 4 - Fluxograma nova conta de utilizador

Neste tipo de alerta (Figura 4) avaliamos o risco e as ações a tomar no caso da criação de uma nova conta de utilizador

Para fazer a deteção do alerta são monitorizados os eventos de criação de contas e utilizadores através de logs e ferramentas, gerando assim os alertas de possíveis ataques.

Após receber o alerta de nova conta criada, verificamos se o utilizador se encontra na lista de utilizadores conhecidos. Caso esteja na lista será notificado para averiguar a veracidade da conta criada e após a sua resposta positiva, o caso será considerado como falso positivo. Caso o utilizador não esteja presente na lista, não exista resposta ao ser notificado, ou indique que não foi ele a criar uma conta nova, será aberto um novo caso.

Após aberto, o caso começa a ser investigado. Inicialmente, se for confirmado o risco, são retirados os privilégios ou desativa-se a conta temporariamente, notificando o cliente sobre as ações. Se após notificar o cliente, não houver resposta ou ainda existir suspeitas de risco, a conta é removida completamente e o cliente é informado.

Em qualquer das etapas de resolução, assim que o caso for considerado resolvido, os processos de criação de contas são revistos, e caso necessário, implementam-se medidas de monitorização contínua para prevenir futuros incidentes.

## **4.5 Os dados do utilizador foram alterados**

O fluxograma seguinte (Figura 5) representa um procedimento que os analistas do SOC seguirão ao executar tarefas de resposta a incidentes relacionados à alteração de conta de um utilizador. Funciona com base na verificação em várias etapas e é implementado como parte de um sistema de segurança.

Ao verificar um utilizador, o analista primeiro verifica se o utilizador é conhecido e se o mesmo fez a alteração à sua conta. Caso se verifique esta questão, considera-se um falso positivo, caso contrário passa-se para o próximo processo que é representado pelo levantamento dos IPs associados ao alerta.

Posteriormente, verifica-se o tipo de alteração e abre-se um caso, de modo que possa haver intervenção por outras partes. Neste tipo de casos é importante bloquear a conta temporariamente para que não haja alterações indesejáveis até que o caso esteja resolvido. O *Helpdesk* tentará reverter a mudança e contactar a vítima para que a mesma seja alertada da mudança e implementar medidas contracetivas com o objetivo de reduzir este tipo de ataques. Caso contrário, ou seja, não haja forma de contactar a vítima, passa-se ao bloqueio da conta, evitando problemas adicionais.

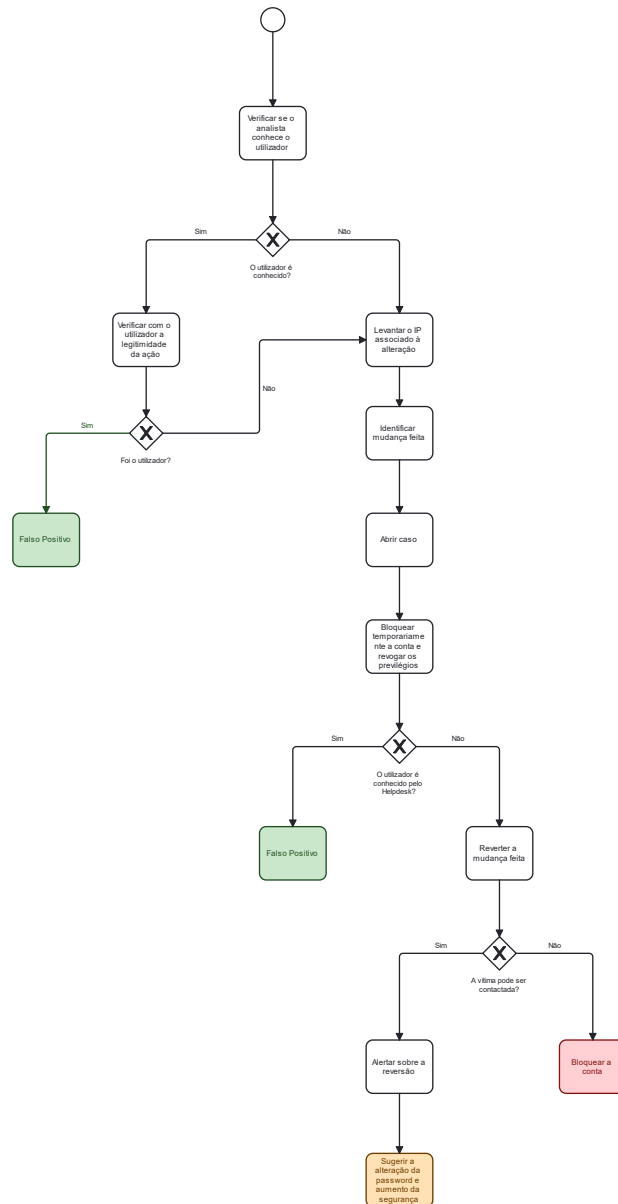


Figura 5 – Fluxograma de alteração de conta

## 5 Implementação



## **6 Conclusão**

## 7 Bibliografia utilizada

- [1] Shu-Hsien Liao, “Expert system methodologies and applications—a decade review from 1995 to 2004,” *Expert Syst Appl*, vol. 28, no. 1, pp. 93–103, 2005, doi: <https://doi.org/10.1016/j.eswa.2004.08.003>.
- [2] M. Vielberth, F. Böhm, I. Fichtinger, and G. Pernul, “Security Operations Center: A Systematic Study and Open Challenges,” *IEEE Access*, vol. 8, pp. 227756–227779, 2020, doi: 10.1109/ACCESS.2020.3045514.
- [3] B. U. Gelman, S. Taoufiq, T. Vörös, and K. Berlin, “That Escalated Quickly: An ML Framework for Alert Prioritization,” *ArXiv*, vol. abs/2302.06648, 2023, doi: 10.48550/arXiv.2302.06648.
- [4] J. Huang, Z. An, S. Meckl, G. Tecuci, and D. Marcu, “Complementary Approaches to Instructable Agents for Advanced Persistent Threats Detection,” *Studies in Informatics and Control*, vol. 29, pp. 269–282, 2020, doi: 10.24846/V29I3Y202001.



## 8 Lista de terminologia específica

<b>ENG CIA</b>	<i>Engenharia do Conhecimento</i>
<b>IP</b>	<i>Internet Protocol</i>
<b>IT/TI</b>	<i>Information Technology/Tecnologias da Informação</i>
<b>MFA</b>	<i>Multifactor Authentication</i>
<b>PPROGIA</b>	<i>Paradigmas da Programação em Inteligência Artificial</i>
<b>SOC</b>	<i>Security Operations Center (centro de operações de segurança)</i>
<b>SP</b>	<i>Sistemas Periciais</i>
<b>VPN</b>	<i>Virtual Private Network</i>