Mariana Inácia Xavier Borges

Análise da aplicação de RPA para atualização de segurança de senhas

Goiânia

2023

UNIVERSIDADE FEDERAL DE GOIÁS
ESCOLA DE ENGENHARIA ELÉTRICA, MECÂNICA E DE COMPUTAÇÃO

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): Mariana Inácia Xavier Borges

Título do trabalho: Análise da aplicação de RPA para atualização de segurança de senhas

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Marcelo Stehling De Castro**, **Professor do Magistério Superior**, em 17/08/2023, às 19:12, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Mariana Inacia Xavier Borges**, **Discente**, em 17/08/2023, às 19:54, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Mariana Inácia Xavier Borges

Análise da aplicação de RPA para atualização de segurança de senhas

Trabalho de conclusão de curso apresentado na Escola de Engenharia Elétrica, Mecânica e de Computação como requisito para a conclusão do curso de Engenharia de Computação e obtenção do título de Engenheiro de Computação.

Universidade Federal de Goiás – UFG

Escola de Engenharia Elétrica, Mecânica e de Computação (EMC)

Orientador: Prof. Dr. Marcelo Stehling de Castro

Goiânia

2023

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Borges, Mariana Inácia Xavier
Análise da aplicação de RPA para atualização de segurança de senhas [manuscrito] / Mariana Inácia Xavier Borges. - 2023.
15 f.: il.

Orientador: Prof. Dr. Marcelo Stehling de Castro.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Escola de Engenharia Elétrica, Mecânica e de Computação (EMC), Engenharia da Computação, Goiânia, 2023.
Bibliografia.
Inclui siglas, abreviaturas, gráfico, tabelas, algoritmos.

1. Automação robótica de processos. 2. Segurança da informação. 3. Senhas. 4. Autenticação. I. Castro, Marcelo Stehling de, orient. II. Título.

CDU 621.03

UNIVERSIDADE FEDERAL DE GOIÁS
ESCOLA DE ENGENHARIA ELÉTRICA, MECÂNICA E DE COMPUTAÇÃO

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Ao(s) sete dias do mês de agosto do ano de dois mil e vinte e três iniciou-se a sessão pública de defesa do Projeto Final de Curso (PFC) intitulado “Análise da aplicação de RPA para atualização de segurança de senhas”, de autoria de Mariana Inácia Xavier Borges, do curso de Engenharia de Computação, da Escola de Engenharia Elétrica, Mecânica e de Computação da UFG. Os trabalhos foram instalados pelo(a) Prof. Dr. Marcelo Stehling de Castro - EMC/ UFG com a participação dos demais membros da Banca Examinadora: Prof. Dr. Carlos Galvão Pinheiro Júnior - EMC/UFG e Prof. Dr. Leonardo Guerra de Rezende Guedes - EMC/UFG. Após a apresentação, a banca examinadora realizou a arguição do(a) estudante. Posteriormente, de forma reservada, a Banca Examinadora atribuiu a nota final de nove virgula seis pontos , tendo sido o PFC considerado aprovado.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.

Documento assinado eletronicamente por **Carlos Galvão Pinheiro Júnior**, **Vice-Diretor**, em 21/08/2023, às 18:07, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Marcelo Stehling De Castro**, **Professor do Magistério Superior**, em 21/08/2023, às 18:26, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Leonardo Guerra De Rezende Guedes**, **Professor do Magistério Superior**, em 23/08/2023, às 13:28, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3980985** e o código CRC **2CB66B5A**.

Referência: Processo nº 23070.024062/2023-83 SEI nº 3980985

Análise da aplicação de RPA para atualização de segurança de senhas

Mariana Inácia Xavier Borges[1], graduanda em Engenharia da Computação. Marcelo Stehling de Castro[2], Professor Associado. EMC/UFG

Universidade Federal de Goiás (UFG) - Escola de Engenharia Elétrica, Mecânica e de Computação (EMC) - Goiânia, Goiás, Brasil 74601-010, e-mails: mariana_borges@discente.ufg.br[1], mcastro@ufg.br[2].

Resumo — Com o rápido avanço tecnológico, o ambiente virtual se tornou uma extensão da vida do ser humano, a partir disto a segurança da informação faz-se um aspecto importantíssimo para assegurar a privacidade dos indivíduos. A autenticação por meio do uso de senhas é atualmente a maneira mais comum de reafirmar esta privacidade, contudo, o uso imprudente de senhas pode causar consequências pessoais e profissionais, uma vez que a maior parte das violações de dados de empresas relacionadas a cibercrimes estão relacionados com credenciais fracas e reutilizadas de seus colaboradores. Este artigo propõe uma análise na segurança de senhas através do uso de uma ferramenta de *Robotic Process Automation* (RPA) para fazer a verificação e manutenção da segurança de senhas usadas em um ambiente empresarial.

Palavras-chaves — *Robotic Process Automation*, senhas, Segurança da informação, autenticação

Abstract — With the rapid advancement of technology, the virtual environment has become an extension of human life. As a result, information security has become an extremely important aspect in ensuring individuals' privacy. Authentication using passwords is currently the most common way to reaffirm this privacy. However, the careless use of passwords can lead to personal and professional consequences, as most data breaches in companies related to cybercrimes are associated with weak and reused credentials of their employees. This article proposes an analysis of password security using a Robotic Process Automation (RPA) tool to verify and maintain the security of passwords used in a corporate environment.

Keywords — Robotic Process Automation, passwords, Information Security, authentication

I. Introdução

Muito tem-se falado sobre a crescente dependência das pessoas com o ambiente virtual, logo, a segurança da informação, mais do que nunca, tornou-se um aspecto crítico.

A segurança de dados pessoais e confidenciais é indispensável para assegurar a privacidade dos usuários e a integridade de organizações. Portanto, a segurança das senhas representa um aspecto crucial na proteção dos sistemas e dados e na prevenção de acessos não autorizados.

A utilização de senhas é um método comum para autenticação e gerenciamento de acesso a sistemas e informações provadas. Entretanto, a segurança de senhas é constantemente afetada devido a diversos fatores, como senhas fracas, reutilizadas e mal armazenadas por seus usuários. Estes hábitos comuns representam riscos alarmantes para a segurança dos dados sensíveis.

Ainda que as empresas tenham aumentado o investimento em segurança digital, seus colaboradores ainda fazem uma má gestão de suas credenciais aponta o 3º Relatório Anual Global de Segurança de Senhas da LastPass [1].

Nesse relatório, percebe-se que mesmo com 57% das empresas analisadas relatarem que usam soluções de autenticação multifatorial (MFA), seus funcionários ainda possuem senhas fracas em sistemas empresariais de alta importância.

Também foi possível analisar pelo relatório que a reutilização de senhas é muito comum, que acontece quando um usuário cria sempre senhas iguais às suas senhas pessoais, além de usar senhas iguais às de outros funcionários.

Nesse contexto é fundamental reafirmar a importância da atualização e criação de senhas seguras como medida preventiva à ataques. A atualização constante das senhas diminui as chances de ataques bem-sucedidos, uma vez que este hábito diminui consideravelmente o tempo de exposição das senhas a possíveis violações.

Ademais, a adoção de uma boa prática de gerenciamento de senhas, como a utilização de senhas complexas e únicas para cada conta, contribui para aumentar a segurança e dificultar a ação de hackers e invasores.

O uso da tecnologia de *Robotic Process Automation* (RPA) pode ser uma aliada eficaz neste âmbito, para verificar e assegurar a qualidade e segurança das senhas em ambientes empresariais. O RPA oferece a capacidade de automatizar tarefas repetitivas e demoradas, incluindo a verificação de senhas de forma segura e privada, garantindo um serviço eficiente e confiável.

Este artigo propõe uma análise da aplicação da RPA como uma ferramenta para a verificação e atualização de senhas em ambientes empresariais.

Serão explorados os conceitos importantes para esta abordagem, os benefícios dessa abordagem incluem a identificação de senhas fracas ou expiradas, a detecção de padrões suspeitos de uso de senhas e a capacidade de implementar políticas de segurança de senhas de forma consistente.

Além disso, serão discutidas as boas práticas de

implementação da RPA para garantir a confidencialidade e a integridade das senhas, bem como os desafios e considerações relacionados à segurança e privacidade dos dados durante o processo de automação.

Ao compreender a importância da atualização regular de senhas e o papel da RPA na verificação de qualidade e segurança das senhas, é possível promover um ambiente empresarial mais seguro e robusto, protegendo dados sensíveis e mitigando riscos associados a violações de segurança virtual.

A) Motivação

Tendo em vista a que as ameaças virtuais estão evoluindo consonantemente ao desenvolvimento tecnológico, é de suma importância que novas medidas sejam adotadas para evitar vulnerabilidades.

No âmbito da segurança de senhas, é notório que o gerenciamento seguro desempenha um papel crucial na proteção dos sistemas. Entretanto, é fácil encontrar situações em que senhas são escolhidas imprudentemente e ainda reutilizada em diversos cadastros, muitas vezes entre contras pessoais e profissionais, expondo os usuários e suas organizações a riscos significativos.

Ademais, a função de atualizar regularmente as senhas pode se tornar complexa e onerosa, especialmente em ambientes empresariais com grandes quantidades de contas e usuários.

Diante desse cenário, a aplicação de ferramentas como a *Robotic Process Automation* surge como uma promissora solução para a análise e atualização de segurança de senhas.

A Automação Robótica de Processos, baseada em automação de processos por meio de *software*, garante a opção de automatizar tarefas repetitivas e demoradas.

Com o auxílio da RPA, é possível assegurar a conformidade com políticas de segurança, identificar senhas fracas ou expiradas e realizar a manutenção regular das senhas, de forma eficiente e segura.

B) Objetivos

Este trabalho de conclusão de curso em Engenharia de Computação tem como objetivo realizar uma análise detalhada da aplicação da RPA na atualização de segurança de senhas em ambientes empresariais.

Serão explorados os benefícios e desafios dessa abordagem, assim como as melhores práticas de implementação, considerando aspectos como privacidade, confidencialidade, integridade e disponibilidade dos dados.

Objetiva-se fazer uma análise profunda das boas práticas no campo da segurança da informação. Uma revisão abrangente da literatura existente é necessária para compreender as melhores práticas adotadas atualmente no gerenciamento de senhas.

Diretrizes de órgãos reguladores, padrões e normas internacionalmente reconhecidos serão analisados, assim como as recomendações de especialistas especializados na área. Essa análise permitirá identificar as práticas mais eficazes e relevantes para garantir a segurança das senhas.

Para ter uma visão clara dos desafios enfrentados na segurança das senhas e ajudar a desenvolver estratégias eficazes para proteger as informações sensíveis dos usuários, será estudado as principais ameaças à segurança das senhas. Serão investigados diferentes tipos de ataques cibernéticos direcionados às senhas. Serão compreendidas as características desses ataques, seu impacto potencial e as medidas preventivas que podem ser adotadas para prevenir essas ameaças.

C) Relevância

A relevância desse estudo se reflete na contribuição que pode trazer para a área de segurança da informação para organizações e para a proteção dos dados dos usuários. A utilização de boas práticas consonantemente ao uso adequado de ferramentas pode fortalecer exponencialmente a segurança das senhas e, portanto, a proteção das informações confidenciais das empresas e de seus clientes.

A análise das principais ameaças em ambientes virtuais possibilita um entendimento aprofundado dos riscos envolvidos, permitindo a implementação de medidas preventivas e a adoção de estratégias eficientes de defesa contra a ameaça a segurança dos dados sensíveis.

Através dessa pesquisa, espera-se contribuir para o avanço da área de segurança da informação, fornecendo insights valiosos sobre o uso da RPA como uma solução eficiente para a atualização de segurança de senhas.

D) Estrutura do Trabalho

Primeiramente, na construção desta análise faz-se importante a abordagem do referencial teórico, na seção II serão abordados os tópicos de Segurança da Informação e Entropia.

Será apresentada uma revisão abrangente da literatura existente, fornecendo uma base sólida para a compreensão dos conceitos fundamentais relacionados à segurança de senhas.

Abordar-se-á tópicos como a importância da segurança da informação, os princípios básicos da criptografia, técnicas de Hash e a influência da entropia na robustez das senhas.

Adiante, na seção III, será feito um estudo sobre as principais ameaças virtuais, com foco nas principais ameaças à segurança e ameaças específicas direcionadas às senhas.

Serão explorados tipos de ataques comuns, como *phishing* e ataques de força bruta, destacando os riscos associados a senhas fracas, reutilizadas ou facilmente identificáveis.

O estudo específico permitirá abstrair a importância da implementação de medidas de segurança eficazes para proteger as senhas dos usuários.

Na seção IV, será feita uma abordagem das ferramentas utilizadas no âmbito de segurança da informação. Serão analisadas as funcionalidades e recursos dessas ferramentas.

Discutida será a importância de uma abordagem conjunta entre RPA e gerenciamento de senhas para aprimorar a segurança e a eficiência no contexto empresarial.

Por fim, na seção V abordar-se-á o cenário do estudo que foi realizado e adiante a seção VI, consiste na análise de um exemplo prático de utilização do RPA para melhorar a segurança de senhas em um ambiente específico. Uma situação será exemplificada ilustrando como a aplicação de RPA pode contribuir para a detecção de senhas fracas, expiradas ou comprometidas, bem como para a automação da atualização de senhas em conformidade com as boas práticas.

II. Referencial Teórico

É importante considerar o uso de conceitos, técnicas e melhores práticas em processos relacionados à Segurança da Informação (SI) para criar soluções eficientes e adequadas.

O campo de pesquisa de Segurança da Informação é focado em proteger informações contra acesso não autorizado, uso indevido e outras diversas ameaças.

Além disso, é de suma importância considerar a análise da entropia, a qual mede a aleatoriedade e a complexidade das senhas e ajuda a criar senhas fortes e seguras.

Ao abordar segurança de senhas, é essencial também estudar as principais ameaças à integridade de senhas ao utilizar a internet.

Considerar esses tópicos dentro de uma estrutura teórica fornece uma base sólida para entender os desafios e desenvolver uma estratégia eficaz de segurança de senha.

A) Segurança da Informação (SI)

"A segurança das senhas é um elemento crucial na proteção dos sistemas e informações sensíveis, sendo essencial adotar práticas robustas de gerenciamento e armazenamento para minimizar o risco de acesso não autorizado" [2].

A Segurança da Informação (SI) tornou-se indispensável para indivíduos, organizações e sociedade como um todo. A proteção dos dados e informações sensíveis contra ameaças cibernéticas, violações de privacidade e acesso não autorizado tornou-se uma prioridade crucial.

Segundo padrões internacionais, como o ISO/IEC 27001 [3], a Segurança da Informação (SI) é definida como a preservação da confidencialidade, integridade e disponibilidade dos dados através de um processo de gestão de riscos. A confidencialidade presa em assegurar que a informação seja acessível apenas a pessoas autorizadas, a integridade busca manter a precisão e a completude dos dados, já a disponibilidade visa assegurar que a informação esteja acessível e disponível quando necessário.

Adicionalmente, o Instituto Nacional de Padrões e Tecnologia (NIST) retifica que a segurança da informação engloba a proteção contra acesso não autorizado, uso indevido, divulgação inadequada, interrupção, modificação ou destruição dos dados e sistemas de informação. Essa definição ressalta a necessidade de abordar diferentes aspectos da segurança para garantir a proteção abrangente das informações.

1) Confidencialidade

Como o primeiro pilar da Segurança da Informação (SI) a confidencialidade se baseia na proteção dos dados contra acesso não autorizado, assegurando que apenas as entidades ou indivíduos autorizados possam interagir com as informações guardadas.

Esse aspecto da Segurança da Informação (SI) é crucial para preservar a privacidade das organizações.

A fim de assegurar a confidencialidade, diversas medidas de segurança podem ser adotadas. A criptografia se destaca como uma das principais estratégias de segurança, na criptografia os dados são formatados de maneira que fique ilegível. Somente com o uso da chave específica é possível voltar os dados ao seu formato legível.

A criptografia tem sua classificação baseada essencialmente na quantidade de chaves compreendidas no processo criptográfico [4]. A criptografia de chave simétrica compreende os algoritmos que utilizam de uma chave somente tanto para a criptografia quanto para a descriptografia, já a criptografia de chave assimétrica engloba os algoritmos que usam de chaves diferentes para a criptografia e descriptografia, como apresentado na Fig. 1.

2) Integridade

O segundo pilar da Segurança da Informação se atém a garantia da integridade e precisão dos dados ao longo do tempo. A integridade na Segurança da Informação envolve diferentes desafios em sua implementação, uma abordagem efetiva começa com a composição e execução de controles e políticas internas que visam proteger os dados contra modificações não autorizadas ou não intencionais.

As principais medidas que podem ser adotadas incluem o uso de processos de autenticação, para uma gestão eficaz de identidade e a adoção de técnicas de verificação de integridade, como algoritmos de Hash.

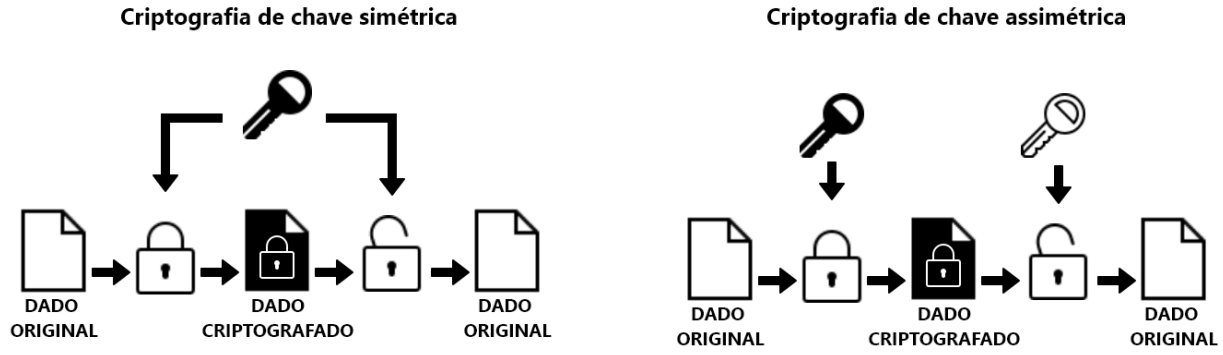

Fig. 1. Classificação de Criptografia. Fonte: elaborado pela autora.

Pode-se definir um algoritmo de Hash como uma função matemática que mapeia dados de tamanhos variados e retorna um valor de tamanho fixo, o qual é denominado de Hash. Conforme é mostrado na Fig. 2, o Hash é uma função unidirecional, ou seja, seu valor não pode ser usado para reconstruir os dados mapeados.

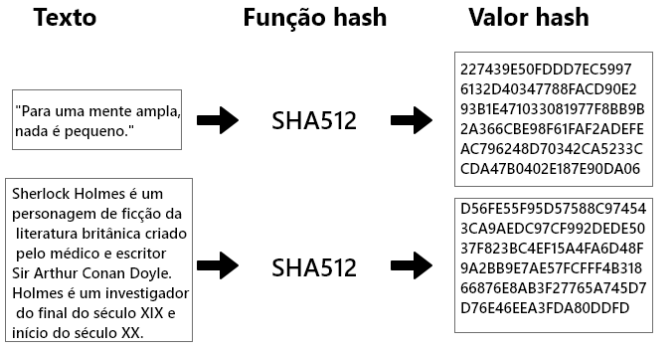

Fig. 2. Função Hash. Fonte: elaborado pela autora.

Na prática, um *software* pode usar um algoritmo de Hash para ter controle da modificação de arquivos armazenados gerando um valor de Hash para cada arquivo.

Quando um arquivo é baixado o site pode comparar o valor de Hash do arquivo baixado com o valor de Hash armazenado anteriormente. Se os dois valores de Hash não corresponderem, significa que o arquivo foi modificado desde que foi enviado para o servidor.

Os algoritmos de Hash também podem ser usados para verificar a autenticidade dos dados. Por exemplo, um desenvolvedor de *software* pode usar um algoritmo de Hash para gerar um valor de Hash para cada cópia de seu *software*.

Quando um usuário baixa o *software*, ele pode comparar o valor de Hash do *software* baixado com o valor de Hash publicado pelo desenvolvedor. Se tais valores não coincidirem, fica evidente que o *software* foi adulterado desde sua publicação.

3) Disponibilidade

O terceiro pilar da Segurança da Informação visa garantir a acessibilidade e usabilidade dos dados sempre que necessário para os usuários autorizados, evitando dessa forma interrupções que possam comprometer o fluxo de processos dentro de uma organização.

Com crescente aumento da dependência de recursos de informação digital, aumentaram também os ataques e falhas nestes mesmos recursos. Isto evidencia que é indispensável um bom controle da disponibilidade da informação, pois as consequências da indisponibilidade de dados podem ser preocupantes.

Em um estudo anual, que analisa o desempenho de *e-commerces* durante a *Black Friday*, a Sofist, teste inteligente para *software*, detectou que problemas de lentidão e instabilidade custaram R$ 48,4 milhões às lojas virtuais em 2022.

Segundo a empresa, durante a *Black Friday* 2022, a cada hora que um e-commerce ficou fora do ar foram perdidos R$ 3.104.398,04 em vendas [5]. Esta avaliação salienta a importância de uma preparação tecnológica eficaz para evitar tamanhas perdas.

Diversos fatores podem afetar diretamente a disponibilidade de arquivos e dados armazenados, para prevenir é importante um breve estudo sobre as mais frequentes causas.

Problemas de hardware e *software* podem deixar o sistema indisponível indefinidamente, mas também ataques *Denial-of-service* (DoS) e de *Malware* são relativamente comuns e podem também danificar o sistema além de afetar a disponibilidade dos dados.

De forma a assegurar a disponibilidade de dados, várias medidas podem ser adotadas:

- Redundância: A redundância se baseia na criação de cópias dos dados importantes do sistema, a fim de que, se algo indisponibilizar uma das cópias disponíveis, ainda é possível utilizar outra cópia. Exemplo: um arquivo pode ficar armazenado em mais de um servidor, cada um em diferentes localizações, se algum deles ficar indisponível, o arquivo ainda poderá ser acessado de outro servidor.
- Balanceamento de carga: Realizar a distribuição do tráfego entre vários servidores para que nenhum servidor fique sobrecarregado e apresente instabilidades. Funciona basicamente do mesmo modo que a medida de Redundância mencionada anteriormente, ao hospedar os dados em diferentes servidores em localizações diferente, se algum apresentar um tráfego alto, a carga pode ser distribuída entre outras regiões.
- *Failover*: Possuir um sistema de backup que pode substituir o sistema principal, caso ele falhe. Exemplo: uma empresa pode possuir uma conexão de internet de backup que pode ser usada caso a conexão principal fique fora do ar.

Aliando todos estes pontos é possível criar um sistema de Alta disponibilidade (HA), exemplificado na Fig. 3, criando um conjunto de tecnologias e processos projetados para garantir que sistemas críticos estejam sempre disponíveis.

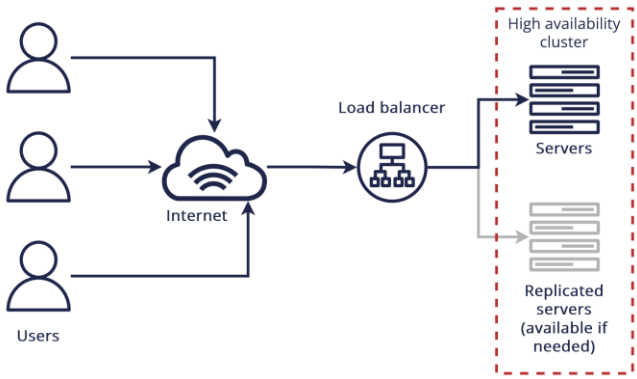

Fig. 3. Exemplo de sistema de alta disponibilidade. Fonte: [6].

É relevante também ter um planejamento de Recuperação de desastres (DR), ou seja, um plano para restaurar sistemas de TI e dados após um incidente. Planos de recuperação de desastres geralmente incluem etapas para identificar riscos, desenvolver estratégias de recuperação e testar o plano regularmente. Por exemplo, uma empresa pode ter um plano de recuperação de

desastres que inclui etapas para restaurar seus dados caso seja vítima de um ciberataque.

B) Entropia

"Criptógrafos utilizam o termo entropia para se referir à aproximação matemática da complexidade de uma senha baseada no método utilizado para criá-la. Uma senha que possui uma entropia mais elevada possui uma chance menor de ser adivinhada por uma pessoa (e mais importante ainda, a senha possui uma chance menor de ser adivinhada por uma máquina). Logo, quando falamos sobre senhas, quanto maior a entropia, melhor" [7].

Em qualquer sistema que envolta a autenticação de usuários a segurança das senhas é fundamental. Neste âmbito, a entropia é um conceito importantíssimo, pois é uma ferramenta extremamente eficaz para avaliar a capacidade e a robustez de uma senha ao enfrentar um ataque de segurança.

Segundo o *National Institute of Standards and Technology* (NIST), a entropia é a quantidade de incerteza existente em um ataque que visa descobrir uma senha, medida em bits.

A entropia exerce uma função importantíssima na determinação da força e segurança de senhas. Senhas com baixa entropia, como sequências simples de números ou uso de palavras do cotidiano estão mais sujeitas a ataques de força bruta e a tentativas de quebra de senha.

Não obstante, senhas com alta entropia, ou seja, mais complexas e imprevisíveis, dificilmente estão suscetíveis a tais vulnerabilidades [8] [9].

TABELA I
TEMPO ESTIMADO PARA DESCOBRIR UMA SENHA EM UM ATAQUE DE FORÇA BRUTA.

Número de Caracteres	Letras maiúsculas e minúsculas	Números, letras maiúsculas e minúsculas	Números, letras maiúsculas, minúsculas e símbolos
4	Instantâneo	Instantâneo	Instantâneo
6	Instantâneo	Instantâneo	Instantâneo
8	28 segundos	2 minutos	5 minutos
10	21 horas	5 dias	14 dias
12	6 anos	53 anos	226 anos
14	17k anos	202k anos	1m anos
16	46m anos	779m anos	5bn anos

Fonte: [10].

A entropia impacta diretamente no espaço e tempo do processo de acertar uma combinação de senha. Ou seja, a medida de entropia é proporcional a dificuldade e tempo de se descobrir uma senha, tornando um possível ataque mais demorado e consequentemente oneroso.

Como mostrado na Tabela , para se calcular a entropia de senhas existem diversas métricas que permitem avaliar sua segurança e aleatoriedade. Os principais são:

- Comprimento da senha: quanto maior o número de caracteres em uma senha, maior é a entropia potencialmente alcançável, portando mais segura a senha.
- Variedade de caracteres: O uso de diferentes tipos de caracteres como letras maiúsculas e minúsculas, números e caracteres especiais aumenta potencialmente a entropia de uma senha.
- Frequência de caracteres: Manter um certo grau de aleatoriedade dentre os caracteres de uma senha também influencia diretamente na entropia desta. É sempre importante evitar padrões e repetições de caracteres.

III. AMEAÇAS VIRTUAIS

As ameaças virtuais são um problema em constante crescimento. Apesar das tecnologias atuais de cyber segurança, diariamente empresas são atingidas com estes ataques.

O antigo CEO da Cisco, uma das maiores empresas de segurança virtual do mundo, John Chambers, afirmou que existem dois tipos de empresas: aquelas que foram invadidas e aquelas que ainda não sabem que foram invadidas.

Existem muitos criminosos intencionados a aproveitarem de brechas de segurança e vulnerabilidades em sistemas coorporativos.

Normalmente, os invasores buscam um resgate: 53% dos ataques virtuais resultaram em danos de US$ 500.000 ou mais. Porém ainda há criminosos com motivações posteriores, que apagam sistemas inteiros como forma de "hacktivismo" [11].

Um estudo de 2022, em mais de 4.000 empresas em todo o mundo, realizado pelo Ponemon Institute e pela Trend Micro descobriu que um terço das empresas globais foram alvo de pelo menos sete ataques de hackers em um período de 12 meses.

Segundo o estudo, o Índice de Risco Cibernético (IRC), que mede o nível de alerta das empresas, apresentou uma deterioração do segundo semestre de 2021 para o primeiro trimestre de 2022. Isso representa um aumento de aproximadamente 84% no número de empresas atacadas por hackers.

Na Fig. 4 é possível verificar as principais causas das ameaças virtuais de 2022. Este gráfico destaca os principais fatores que contribuíram para o aumento das ameaças e ataques cibernéticos durante o ano de 2022.

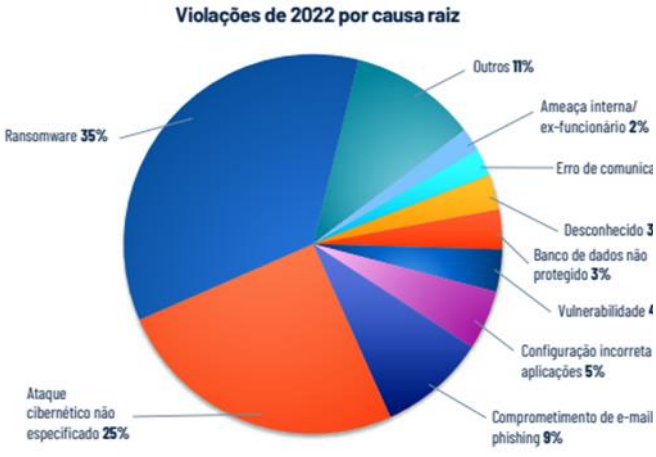

Fig. 4. Causa das violações de dados em 2022. Fonte: [12].

Também constatado nesse estudo, a maior falha de infraestrutura informada é de negligência interna da própria

empresa que tem os dados comprometidos.

Os impactos negativos mais significativos dos ataques cibernéticos incluem danos à infraestrutura crítica, perda de produtividade, custos de consultoria externa, ações e litígios públicos e danos à reputação. Além disso, os ataques de *ransomware* costumam causar caos e perda de produtividade.

A) Ameaças à segurança

Com o crescente desenvolvimento das tecnologias digitais e a fácil conectividade, o ambiente virtual está cada vez mais propício para a evolução de ameaças. Estas ameaças à segurança têm se diversificado ao longo do tempo.

Ataques tradicionais, como *phishing* e malware, estão sendo aprimorados e aprimorados para ultrapassar as defesas de segurança existentes. Novas formas ameaças, como ataques de engenharia social mais elaborados, têm se tornado mais comuns e têm um impacto significativo na segurança dos dados e nas operações das empresas.

A grande disponibilidade de ferramentas e recursos online e crescente desenvolvimento de equipamentos de hardware mais potentes também tem contribuído para o desenvolvimento das ameaças à segurança.

Os *cybers* criminosos têm a sua disposição kits de exploração, malwares personalizados por meio de fóruns clandestinos na *dark web*, ampliando sua efetividade de ataque e tornando-se mais difíceis de serem detectados.

A análise das principais causas destes ataques é fundamental se compreender os pontos fracos e vulnerabilidades que foram explorados pelos cybers criminosos. Isso permite uma melhor compreensão das áreas que requerem atenção e a implementação de medidas de segurança mais eficientes.

1) Malwares

"O malware é um programa que é inserido em um sistema, geralmente de forma oculta, com a intenção de comprometer a confidencialidade, integridade ou disponibilidade dos dados, aplicativos ou sistema operacional da vítima, ou de outra forma causar incômodo ou interrupção ao usuário" [13].

Um ataque de malware normalmente tem início quando algum usuário realiza uma ação que permite a entrada do malware em seu sistema. Isto ocorre quando é feito o download de um arquivo infectado, ao abrir anexos de e-mails suspeitos, ao clicar em um link malicioso, dentre outras maneiras de explorar as vulnerabilidades de segurança.

Após a infecção, o malware pode executar várias atividades maliciosas, dependendo do seu tipo e objetivo. Alguns malwares se replicam e se espalham para outros sistemas, como os *worms*, enquanto outros se disfarçam como programas legítimos para enganar os usuários, como os cavalos de Troia.

De acordo com o relatório sobre tráfego global de Sistema de Nomes de Domínio (DNS) da Akamai Technologies, empresa de cibersegurança em nuvem, 16% das organizações detectaram comunicação com domínios associados a servidores de comando e controle (conhecido como C2). Isso indica que elas sofreram violações de rede, foram alvos de malware, durante o ano de 2022.

Existem vários tipos de malware, entretanto de acordo com a e as pesquisas já abordadas, os mais nocivos e comuns são:

- *Ransomware:* tipo de ataque de segurança cibernética que destrói ou criptografa arquivos e pastas, tornando os dados inacessíveis ao proprietário do dispositivo afetado. Os cibercriminosos podem extorquir dinheiro de proprietários de empresas em troca de chaves para desbloquear dados criptografados. Mas mesmo que sejam pagos, os cibercriminosos podem não liberar as chaves para recuperar o acesso aos proprietários de empresas [14]. A Fig. 5 mostra como esse malware focado em extorsão está crescendo em impacto e probabilidade.
- *Phishing:* Um ataque de *phishing* é o cyber crime mais comum, é uma comunicação maliciosa que parece vir de uma fonte verdadeira, mas pode afetar qualquer tipo de fonte de dados. Esses ataques podem facilitar o acesso a contas online e informações pessoais, permitir que o criminoso tenha permissão para modificar e comprometer sistemas conectados, como terminais de ponto de venda e sistemas de processamento de pedidos e, em alguns casos, assumir o controle de redes inteiras de computadores até que um resgate seja pago. assumir. Os hackers podem se contentar em obter dados pessoais e informações de cartão de crédito para obter ganhos financeiros. E-mails de *phishing* também podem ser enviados para coletar credenciais de funcionários e outros dados para uso em ataques mais maliciosos contra indivíduos e empresas específicas. *Phishing* é um tipo de ataque cibernético que todos devem aprender a se proteger e garantir a segurança do e-mail em uma organização [15]. De acordo com um relatório da empresa de segurança *Egress*, 92% das organizações foram vítimas de ataques de *phishing* em 2022. Isso representa um aumento de 29% nos incidentes de *phishing* em relação a 2021, quando foi detectado e bloqueado um total de mais de 21 milhões de ataques.

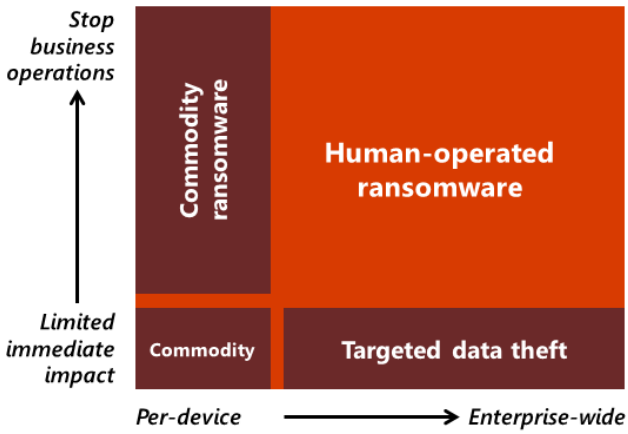

Fig. 5. Impacto do *ransomwar*e. Fonte: [14].

Como apresentado na Fig. 5, o impacto de malwares tem um grande potencial negativo. Para se proteger contra estes faz-se necessário adotar medidas preventivas. É importante manter o *software* atualizado, utilizar de soluções de segurança confiáveis, sempre prestar atenção na procedência de e-mails e

links antes de abrir e verificar a autenticidade de sites. Essas medidas ajudam a reduzir o risco de infecção por malwares e a proteger dispositivos, dados e privacidade.

2) Ataque man-in-the-middle

Man-in-the-Middle (MITM), também conhecido como MIM, MiM, MitM ou MITMA na literatura, é um tipo de ataque no qual uma terceira parte, de forma oculta, assume o controle do canal de comunicação entre duas ou mais partes.

No ataque MITM, o invasor pode interceptar, modificar, alterar ou substituir o tráfego de comunicação do alvo. As vítimas não têm consciência da presença do "*man-in-the-middle*", logo, confiam que o canal de comunicação está protegido [16].

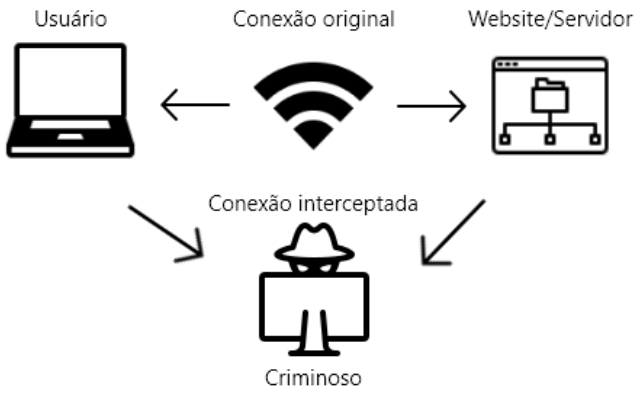

Fig. 6. Exemplo man-in-the-middle. Fonte: elaborado pela autora.

O ataque MITM é um dos ataques mais populares na área de hacking. Especificadamente, como mostrado na Fig. 6, é um ataque em que o invasor intercepta secretamente a conexão entre duas partes que estão se comunicando e, assim, intercepta e retransmite ou até mesmo modifica os dados que estão sendo transferidos entre as duas partes.

Esse tipo de ataque é mais adequado para ambientes de Rede Local (LAN). O MITM só pode ser efetivamente realizado quando o cyber criminoso consegue se fazer passar como uma parte legítima em ambos os extremos da conexão.

Supondo que um invasor se infiltre entre um cliente e um servidor. Agora, o cliente considera o invasor como sendo o servidor, e o servidor considera o invasor como sendo o cliente. Isso resulta em um ataque MITM bem-sucedido [17].

Uma solução eficaz para combater esse problema do ataque MITM é a utilização de um Certificado Digital Secure Socket Layer (SSL). Ao implementar um Certificado SSL, a API é protegida através do protocolo HTTPS, garantindo que o tráfego de comunicação seja criptografado e seguro.

O Certificado SSL atualmente é considerado um requisito básico de segurança nos dias de hoje. No entanto, ainda existem diversos sites que não o adotam, tornando-os altamente vulneráveis a ataques.

3) Inserção de SQL

Muitos bancos de dados de aplicativos da Web são vulneráveis a ataques de injeção de SQL, os quais permitem que os clientes insiram dados confidenciais diretamente.

Eles executam operações inserindo o código de consulta de injeção de SQL malicioso no lado do cliente da API da Web, o que dá acesso para que eles recuperem todos os dados confidenciais do banco de dados.

Logo, a injeção de SQL é uma técnica na qual um criminoso assume acesso total a um login de administrador de um banco de dados da Web e envia solicitações maliciosas de consulta de SQL para modificar dados de entrada ou excluir informações de usuário existentes.

O objetivo dessa técnica é alterar a estrutura e o comportamento das consultas propostas pelos programadores de computador. A análise de injeções de SQL direcionadas a *front-ends* de aplicativos da Web para obter acesso a bancos de dados de *back-end* explora o impacto, a taxonomia e as técnicas desses ataques [18].

A maioria dos casos de injeção de SQL podem ser frustrados usando consultas parametrizadas, em vez de concatenar *strings* nas consultas. As consultas parametrizadas podem ser aplicadas a qualquer situação com entradas não confiáveis.

4) Exploração de dia zero

Um ataque de exploração de dia zero é um ataque de computador que explora uma vulnerabilidade exposta de um sistema. Pode ser visto usado como vulnerabilidade um bug de *software* ou uma falha na política de segurança que permite que um invasor obtenha acesso a um sistema antes que este problema se torne de conhecimento público.

Sua finalidade é acessar ilegalmente ou chantagear um sistema em execução [19]. Os ataques de dia zero são muito difíceis de defender, uma vez que só são detectados depois que um sistema foi comprometido, porém, essa vulnerabilidade não tem assinatura conhecida e nenhum mecanismo para prevenir ou detectar ataques de dia zero [19] [20].

Depois que uma vulnerabilidade é divulgada, os administradores de sistema podem corrigir o bug e as empresas de antivírus podem adicioná-la às suas atualizações de assinatura.

B) Ameaças às senhas

As senhas majoritariamente são a única barreira que segura a privacidade das pessoas e empresas em seus diferentes perfis e contas. Entretanto, o cenário digital expôs um terreno fértil para cyber criminosos, que aproveitaram ao máximo as oportunidades oferecidas pelo aumento das identidades digitais.

O crescente número de fraudes e ataques cibernéticos coloca em risco a segurança das senhas e consequentemente de seus usuários, exigindo medidas mais eficazes e conscientização por parte dos usuários.

Depois da rápida transição de empresas para o regime de trabalho remoto que aconteceu em 2020, em virtude da pandemia de COVID-19, as equipes de TI e segurança da informação enfrentaram um grande desafio para conseguir manter um ambiente seguro nas empresas.

No relatório “The SpyCloud 2022 Identity Exposure Report” foi apresentado que apenas 43% dos profissionais de segurança entrevistados em abril de 2021 estão confiantes de que sua organização está preparada para uma violação de dados por trabalhadores remotos, 50% destes sentiram maior estresse relacionado ao suporte a trabalhadores remotos.

Maus hábitos de segurança comuns de funcionários não

facilitam a vida de uma equipe de segurança já sobrecarregada em virtude do ambiente de trabalho remoto [21].

Existem diversas ameaças que podem comprometer a segurança das senhas, no entanto, algumas são mais comuns e representam riscos significativos. Entre as ameaças mais frequentes estão:

1) Anotação desprotegida

Outrora era um costume pessoas anotarem suas senhas em papel ou em notas adesivas e alocarem estas ao lado do computador e/ou notebook. Este hábito visava tornar o acesso à senha o mais rápido e descomplicado possível, evitando, portanto, o risco de esquecê-la. Porém, essa prática estava longe de ser segura.

Ao armazenar as senhas em um papel, elas se tornam vulneráveis a qualquer pessoa com acesso ao computador. Se uma pessoa mal-intencionada encontrar essas notas, ele terá acesso instantâneo as contas e informações confidenciais do dano delas. Era como se as senhas não existissem porque qualquer um poderia usá-las indiscriminadamente.

À medida que a tecnologia avançou e o uso de dispositivos eletrônicos se popularizou, também aumentaram as maneiras como as senhas são armazenadas.

Atualmente, é muito comum encontrar muitas pessoas optam por anotar suas senhas e informações de login em aplicativos de bloco de notas ou arquivos eletrônicos. Essa atitude parece uma via conveniente, uma vez que as senhas são facilmente acessíveis de qualquer dispositivo conectado.

No entanto, esse método traz inda mais riscos do que o método antigo de fazer anotações em papeis. A maioria dos aplicativos de bloco de notas e arquivos eletrônicos não foram projetados para armazenar informações confidenciais com segurança. Eles não possuem os mecanismos de criptografia e proteção necessários para garantir a confidencialidade da senha.

O armazenamento de senhas em aplicativos não seguros expõe os usuários a possíveis violações de segurança de seus dados pessoais e informações de conta. Cyber criminosos estão sempre procurando maneiras de acessar esses dados confidenciais. Se sua senha for comprometida, todas as contas associadas a ela serão comprometidas.

Um exemplo preocupante desse problema ocorreu em 2016 quando o Portal Brasil, conta na rede social “Twitter” ligada à Secretaria de Comunicação Social da Presidência da República, cometeu um erro grave. Por engano, eles postaram um link que continha todas as suas senhas, desde contas do Instagram até Facebook e Gmail.

Essa falha expôs de forma imprudente informações confidenciais e representou uma séria violação de segurança. Esse incidente serve como um lembrete impactante de como o descuido na proteção das senhas pode resultar em consequências graves e colocar em risco a privacidade e a segurança dos usuários.

É essencial que as organizações e os indivíduos estejam conscientes dos riscos envolvidos e adotem medidas adequadas para proteger suas senhas [22].

2) Keystroke Logging

Um *keylogger* ou *keystroke logger* é um tipo de malware ou hardware que rastreia e registra as teclas digitadas enquanto elas são digitadas no dispositivo alvo.

Ele captura informações e as envia aos cybers criminosos por meio de servidores de comando e controle (C&C). Os criminosos analisam as teclas digitadas para descobrir nomes de usuário e senhas e usá-los para invadir sistemas seguros [23]. A melhor maneira de proteger dispositivos contra *keylogging* é utilizando um antivírus ou firewall de alta qualidade. Estas ferramentas de segurança são projetadas para detectar e bloquear a presença de malware, incluindo *keyloggers*, em dispositivos, monitorando constantemente as atividades do sistema em busca de comportamentos suspeitos e ataques em potencial, logo, impedindo quase sempre que *keyloggers* capturem teclas digitadas.

3) Sniffing

O *sniffing* de senhas permite que invasores monitorem sua rede e coletem dados como senhas dela. Um invasor pode ser capaz informações como [24]:

- Senhas em geral
- ConFig. ção do roteador
- Tráfego DNS
- Tráfego de e-mail
- Tráfego da Web
- Sessões de bate-papo

Os computadores podem ser conectados através de um hub ou um switch. Quando uma rede é conectada por meio de um hub, ela é chamada de Ethernet compartilhada. Quando a conexão passa por um switch, ela é chamada de Ethernet comutada.

Em um ambiente Ethernet compartilhado, os pacotes de transmissão são transmitidos para todos os computadores. Somente o computador de destino acessa os pacotes. Outras máquinas ignoram o pacote.

Essa regra é ignorada pelos criminosos. Na Ethernet comutada, o switch mantém uma tabela contendo os endereços MAC de todos os computadores da rede. Portanto, as mensagens são enviadas apenas para o computador de destino. Apesar da Ethernet comutada ser mais segura, ainda podem acontecer ataques de *sniffing* [24].

Outra maneira de se defender contra o *sniffing* de senhas principalmente no ambiente corporativo é criptografar o tráfego da rede. Isso pode ser feito implementando uma solução de VPN (Rede Privada Virtual) ou utilizando protocolos avançados de criptografia, como SSL/TLS, para proteger as comunicações [25].

4) Engenharia Social

A engenharia social é uma tática amplamente utilizada por cybers criminosos que se aproveita das relações humanas para realizar ataques virtuais.

Um aspecto particularmente interessante desse tipo de ataque é que ele depende da colaboração dos usuários e o seu sucesso está diretamente relacionado com a possibilidade da vítima em identificar a ameaça.

Logo, pode-se chegar à conclusão de que quanto mais conscientes as pessoas estiverem em relação à segurança da informação, mais difícil será para um criminoso explorar as vulnerabilidades humanas para realizar seus crimes [26].

No ambiente empresarial, o fator humano é frequentemente apontado como a parte mais vulnerável no contexto de Segurança da Informação. Porém, é fácil notar que a segurança dos sistemas ainda se concentra majoritariamente nos aspectos técnicos.

É fundamental que as organizações dediquem atenção e recursos para conscientizar colaboradores sobre os riscos e práticas seguras, promovendo treinamentos e políticas de segurança adequadas [26].

Uma das formas mais comuns de engenharia social é o *phishing*, o qual já foi abordado anteriormente, além dele, existem outros métodos de engenharia social que os cibercriminosos utilizam para ter acesso às senhas e informações pessoais:

- *Vishing*: Nesse método, os criminosos entram em contato com as vítimas por telefone e utilizam técnicas de manipulação e persuasão verbal para obter informações pessoais. Eles podem se passar por representantes de instituições financeiras, empresas de serviços públicos ou até mesmo autoridades. Ao estimular a confiança das vítimas e criar um senso de urgência, os atacantes podem obter informações como senhas, números de cartão de crédito ou dados de identificação pessoal.
    - Contas falsas em redes sociais: Com o crescimento das mídias sociais, os criminosos têm explorado essas plataformas para obter informações pessoais sobre os usuários. Eles podem realizar pesquisas detalhadas sobre os perfis das vítimas e usar essas informações para criar mensagens personalizadas e convincentes, podendo se fazer passar por amigos, colegas ou até mesmo pessoas de confiança, com o objetivo de obter acesso a informações pessoais ou enganar os usuários para que cliquem em links maliciosos.

5) Força Bruta

Das maiores e mais populares ameaças às senhas atualmente, são considerados os ataques de força bruta, um ataque em que um invasor tenta adivinhar a senha de login ou de acesso de um determinado sistema ou rede de serviços por meio de tentativa e erro [27].

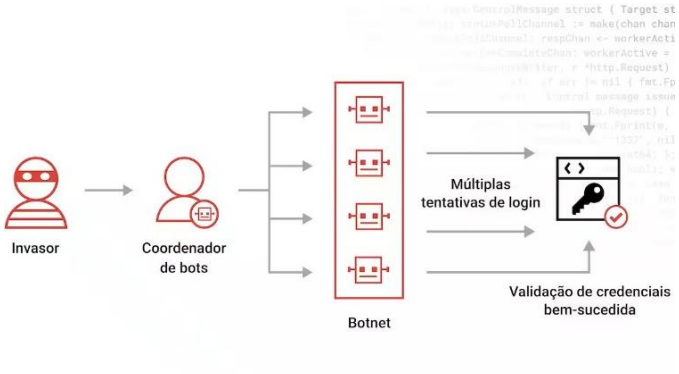

Fig. 7. Como funciona um ataque de força bruta. Fonte: [28].

Como apresentado na Fig. 7, no ataque de força bruta, os cybers criminosos usam várias combinações de nome de usuário e senha para obter acesso a contas pessoais ou ambientes de TI. Praticamente todos os ataques de senha de força bruta são executados por *botnets*. Uma *botnet* é uma rede de *bots* (que podem executar tarefas específicas repetidamente por conta própria sem intervenção humana) que consiste em centenas ou milhares de computadores infectados por malware sob o controle de uma pessoa [28].

Existem diversos tipos de ataques de força bruta, no entanto alguns são mais comuns e são constantemente utilizados por criminosos em seus ataques:

- Ataques simples de força bruta: Este ataque utiliza apenas senhas padrões e informações pessoais, estes ataques somente têm sucesso pois muitos usuários não executam um gerenciamento efetivo de suas senhas, definindo senhas fracas e reutilizando-as em vários sites.
- Ataques reversos: Este ataque ao contrário do anterior visa testar um conjunto de senhas simples em uma lista de possíveis nomes de usuário.
- Ataques de dicionário: Esta técnica visa adivinhar uma senha a partir de tentativas usando cada palavra ou combinação de palavras em um dicionário. Esse tipo de ataque geralmente é mais eficiente do que um ataque de força bruta simples pois muitos usuários tendem a usar palavras ou combinações de palavras específicas de seu idioma como senhas.

Como apresentado na Tabela para prevenir ataques de força bruta é essencial a utilização de senhas fortes, não comuns e evitar a utilização da mesma senha em diferentes cadastros.

Além dessas medidas gerais, este artigo propõe uma solução adicional para fortalecer a segurança das senhas em um ambiente corporativo.

Desenvolveu-se um bot, com uso de ferramentas de RPA, que verifica as senhas armazenadas no banco de dados em busca de vulnerabilidades a ataques de força bruta.

Caso uma senha seja identificada como vulnerável, ela é expirada e o colaborador obrigado a criar uma senha nova, tornando os dados coorporativos menos suscetíveis a esses ataques.

IV. Ferramentas

A utilização de ferramentas especializadas desempenha um papel fundamental na proteção e fortalecimento da segurança virtual.Essas ferramentas são projetadas para identificar, prevenir e combater ameaças virtuais, como malwares, *phishing*, ataques de força bruta e violações. Elas são desenvolvidas com algoritmos sofisticados e atualizadas regularmente para acompanhar as mais recentes técnicas e táticas empregadas pelos cybers criminosos.

Ao adotar ferramentas de segurança, pode-se aumentar significativamente a proteção dos nossos dispositivos, redes e dados pessoais. O uso de antivírus confiáveis e firewalls robustos ajuda a bloquear e eliminar *software*s maliciosos, enquanto as VPNs garantem a privacidade e a criptografia das comunicações online.

Além disso, os gerenciadores de senhas permitem a criação de senhas fortes e únicas, evitando o reuso e o uso de senhas fracas.

Adicionalmente, é pode-se adotar o uso de RPA como um aliado na segurança de senhas no ambiente coorporativo, utilizando de maneira a verificar vulnerabilidades nas credenciais dos colaboradores preservando a privacidade.

A) Antivírus e plataformas de proteção de endpoint

Os antivírus detectam, colocam em quarentena e removem códigos maliciosos para evitar que estes danifiquem o dispositivo onde estão alocados. Os antivírus atuais são atualizados automaticamente para fornecer proteção contra os vírus mais recentes e outros tipos de malware [29].

As plataformas de proteção de *endpoints* (EPPs) fornecem a capacidade de implantar agentes ou sensores para proteger *endpoints* gerenciados, incluindo desktops, laptops, servidores e dispositivos móveis. As EPPs são projetadas para prevenir uma variedade de ataques maliciosos conhecidos e desconhecidos [30].

Enquanto um antivírus apenas bloqueia as ameaças, um EPP também é capaz de encontrar ameaças nos dispositivos e neutralizá-las, tendo em vista que criminosos são capazes de se infiltrar em qualquer perímetro digital com tempo e recursos suficientes, as EPPs são extremamente mais recomendadas para ambientes coorporativos.

Uma pesquisa realizada pela PSafe entre 27 de agosto e 2 de setembro de 2020 analisou o cenário da segurança da informação de trabalhadores que utilizam dispositivos como computador, celular, notebook e tablet fornecidos pela empresa para trabalhar [31].

Fig. 8. Gartner® Magic QuadrantTM for Endpoint Protection Platforms. Fonte: [30].

O estudo mostra que 40% dos entrevistados já introduziram vírus em seu computador ou notebook de trabalho. Estas ameaças, colocam em perigo, especialmente, os dados confidenciais de empresas [31].A Fig. 8, mostra as principais ferramentas atualmente no mercado de plataformas de proteção de *endpoints* e como estas soluções estão posicionados para atender uma empresa a longo prazo.

B) Firewall

O Firewall funciona analisando o tráfego da rede, por meio de filtros, de maneira a impedir que fontes indesejadas obtenham acesso à rede. Essa filtragem é feita através de instruções predefinidas, para que o firewall se comporte atendendo às necessidades do administrador da rede.

Por meio do Firewall apenas usuários autorizados tem permissão para utilizar determinadas funcionalidades na máquina. Logo, esta ferramenta controla a transferência de dados da máquina através da internet, como forma de prevenindo envio de arquivos sigilosos à rede.

O Firewall consegue identificar as tentativas de ataques e a invasão à rede. Logo, ao acontecer um ataque cibernético, o firewall aciona o bloqueio, protegendo automaticamente as informações da empresa.

C) Virtual Private Network (VPN)

Uma Virtual Private Network estabelece uma conexão segura e criptografada entre dois dispositivos ou redes através de uma rede pública, como a Internet.

Ao utilizar uma VPN, os dados são transmitidos de forma protegida e encapsulada, garantindo privacidade e segurança. Ela cria um "túnel" virtual que protege as informações transmitidas, impedindo que terceiros interceptem ou acessem os dados de forma não autorizada.

Nas empresas, as VPNs permitem que os funcionários acessem a rede interna de forma segura de qualquer local, facilitando o trabalho remoto e a conexão com escritórios em diferentes localidades, conforme mostrado na Fig. 9.

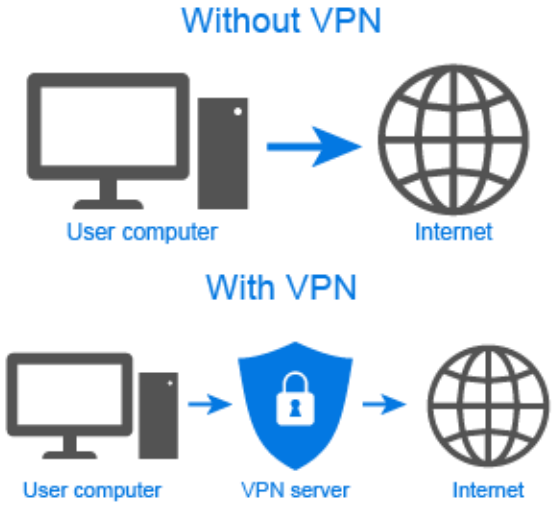

Fig. 9. Funcionamento VPN. Fonte: [32].

D) Automação Robótica de Processos

A Automação Robótica de Processos é uma tecnologia que utiliza um *software* para automatizar tarefas repetitivas e de baixo valor agregado realizadas por seres humanos em processos de negócios.

Esses *bots* de *software* podem executar ações em interfaces

de usuário, emular a interação humana com sistemas e manipular dados para realizar diversas atividades.

A RPA oferece às empresas a oportunidade de reduzir custos de mão de obra e erros humanos. A partir do momento em que o *bot* é criado com o uso de uma ferramenta RPA, este tem a capacidade de capturar e interpretar os processos específicos dos *software*s que os funcionários já operam, ele pode manipular dados, desencadear respostas, iniciar novas ações e comunicar-se com outros sistemas de forma autônoma [33].

Neste artigo uma plataforma RPA será usada no processo de atualização de segurança de senhas em um ambiente empresarial, se maneira a aumentar a segurança de senhas sem interferir na privacidade dos colaboradores.

1) Tipos de RPA

Na automação robótica de processos (RPA), existem duas abordagens principais: RPA assistido e RPA não assistido. O RPA assistido envolve a colaboração entre os *bots* e usuários, enquanto o RPA não assistido se refere à automação completa de tarefas sem a necessidade de intervenção humana. Essas duas modalidades oferecem benefícios e aplicações distintas, dependendo dos requisitos e características do processo a ser automatizado.

- RPA assistido: Os *bots* de RPA assistido funcionam como assistentes virtuais, auxiliando um funcionário individual em suas tarefas para aumentar a produtividade. A automação assistida legada está confinada ao desktop de um único funcionário [34].

- RPA não assistido: Os *bots* de RPA não assistida executam uma automação que funciona de maneira independente de usuários. O objetivo de muitos processos de negócios é a automação de ponta a ponta, onde os *bots* são habilitados para executar processos inteiros de forma automática [34].

2) Plataformas de RPA

As plataformas de RPA desempenham um papel crucial na implementação da automação robótica de processos. Com diferentes categorias disponíveis, as empresas têm a flexibilidade de escolher a plataforma de RPA que melhor atenda às suas necessidades específicas, impulsionando a eficiência operacional, reduzindo erros e capacitando a força de trabalho para se concentrar em atividades estratégicas e de maior valor. a automação robótica de processos.

Com diferentes opções disponíveis, as empresas têm a flexibilidade de escolher a plataforma de RPA que melhor atenda às suas necessidades individuais.

A Fig. 10 mostra a variedade de soluções de RPA, neste artigo, será utilizada a plataforma da IBM como exemplo para ilustrar a aplicação para verificação e atualização de senhas.

Entretanto, é importante ressaltar que o processo e os princípios discutidos podem ser reproduzidos em outras plataformas de RPA, dependendo das necessidades e requisitos específicos de cada empresa.

A escolha da plataforma de RPA adequada deve levar em consideração fatores como funcionalidades, integração com sistemas existentes, suporte técnico e requisitos de segurança.

Fig. 10. Gartner® Magic QuadrantTM for Robotic Process Automation. Fonte: [35]

V. Cenário da Pesquisa

O cenário proposto neste estudo é um ambiente corporativo onde a segurança da informação é prioridade. O *software* corporativo é um ativo crítico para uma organização e o acesso a esse *software* é controlado pelas credenciais do usuário.

As credenciais são armazenadas em um banco de dados protegido para garantir um nível adequado de segurança.

O banco de dados pode usar técnicas de criptografia ou Hash para armazenar senhas de uma forma segura que não pode ser facilmente identificada ou descriptografada, que serão exploradas neste artigo.

Escolher entre criptografia e Hash depende da política de segurança da sua empresa, mas ambas as abordagens fornecem uma camada adicional de proteção por senha. O uso de Hash ou criptografia garante a confidencialidade da senha em caso de violação de segurança ou comprometimento do banco de dados.

Nesse ambiente, é essencial garantir que boas práticas de segurança sejam seguidas no gerenciamento das credenciais. Uma das principais medidas é a atualização regular das senhas pelos usuários.

Entretanto, erra rotina de atualização e senhas raramente é seguida como mostrado na pesquisa apresentada na Fig. 11, onde foram entrevistados em sua maioria profissionais de TI de acordo com as políticas de segurança definidas pela empresa.

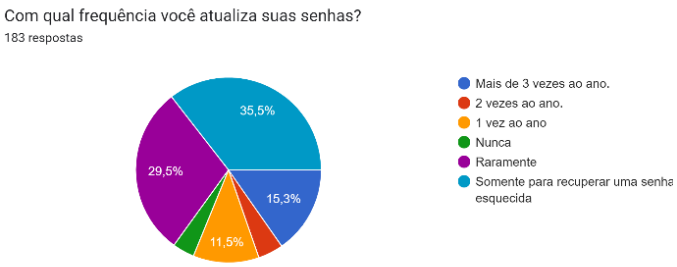

Fig. 11. Pesquisa sobre a frequência de alteração de senhas. Fonte: elaborado pela autora.

O RPA pode ser configurado para interagir com *software* corporativo e acessar bancos de dados. Os robôs de *software* podem reforçar aos usuários a importância de atualizar suas senhas regularmente, de forma a garantir que estejam seguindo as práticas recomendadas de segurança.

Além disso, o RPA pode verificar a complexidade das novas senhas fornecidas pelo usuário para garantir que atendam aos requisitos mínimos de segurança acordados com a empresa.

VI. Análise dos Resultados

A fim de aumentar a eficácia e segurança do gerenciamento de senhas em um ambiente corporativo, foi implementado uma solução de *Robotic Process Automation* (RPA), com os processos exemplificados na Fig. 12.

Utilizou-se a plataforma de RPA da IBM, que oferece uma série de recursos e ferramentas para automatizar tarefas repetitivas e baseadas em regras, como a atualização e verificação de senhas.

Esta análise começou com a criação de um banco de dados que continha informações de 40 usuários de uma empresa, incluindo seus nomes, e-mails, senhas atuais (criptografadas e na versão de Hash) e datas de última atualização.

Para complementar, também foi criado uma tabela com senhas fracas e comuns frequentemente utilizadas no Brasil e no mundo, com o intuito de identificar quais usuários possuíam senhas vulneráveis.

- Dados para teste de funcionalidade: Foram criados 40 registros para representar um banco de dados empresarial, cada registro incluindo um Id único, o primeiro nome, o sobrenome, o e-mail, o nome de usuário, o status da senha (se está expirada ou não), a senha em formato de Hash, a senha em formato criptografado e data da última atualização da senha.
- Biblioteca de senhas vulneráveis: A criação de uma biblioteca de senhas vulneráveis, a partir do relatório da empresa de segurança Nordpass [36], representa uma etapa crucial no processo de conscientização e aprimoramento da segurança de senhas. Essa biblioteca consiste em uma lista de combinações frequentemente utilizadas, como senhas baseadas em nomes, sobrenomes, e outras informações pessoais facilmente acessíveis.

Estas senhas vulneráveis são extremamente arriscadas, pois são amplamente conhecidas e podem ser facilmente adivinhadas ou descobertas por hackers e invasores.

Ao usar essa biblioteca como parte da análise de segurança de senhas, é possível identificar usuários que possuem senhas que estão diretamente expostas a ameaças virtuais, como ataques de força bruta ou ataques de dicionário.

A aplicação dessa biblioteca no processo de análise de senhas, juntamente com o uso de técnicas de automação por meio de RPA, permitiu identificar e notificar rapidamente os usuários que utilizavam senhas fracas.

Após uma senha ser considerada fraca por esse processo, esta é expirada, e os usuários incentivados a alterá-las para senhas mais seguras e complexas, minimizando os riscos de comprometimento da segurança de suas contas e, por consequência, da empresa como um todo.

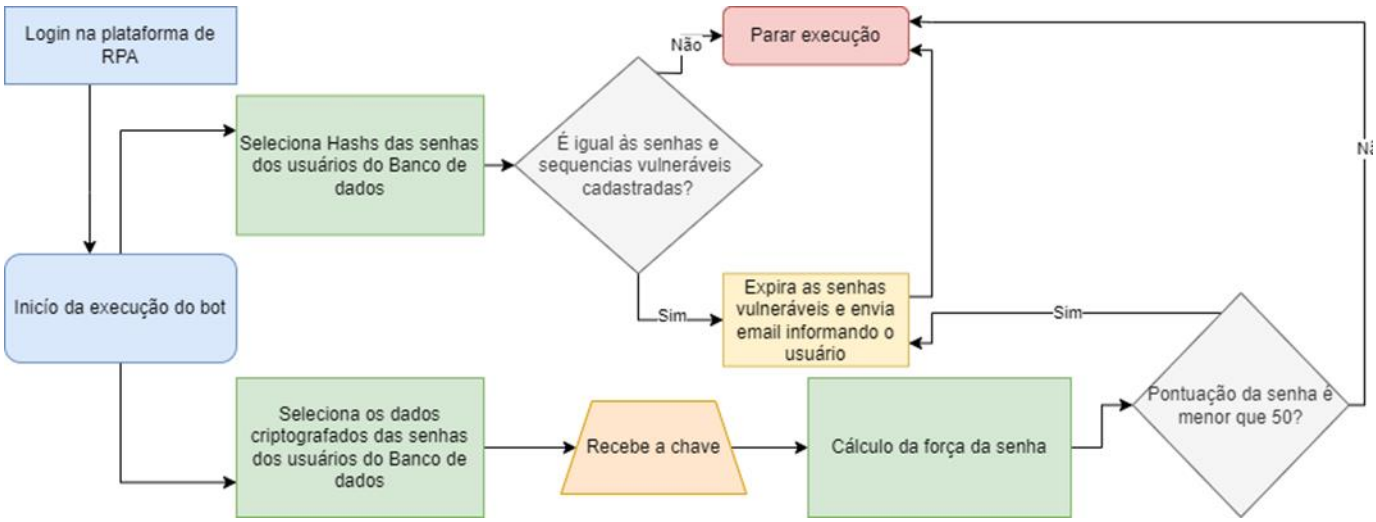

Fig. 12. Fluxograma RPA. Fonte: elaborado pela autora.

1) Verifica segurança de senhas padrão Hash

Conforme apresentado na Fig. 12, a aplicação do RPA no processo de segurança de senhas envolve a verificação dos Hashs cadastrados no banco de dados.

Os Hashs são resultados de funções de Hash aplicadas às senhas, tornando-as irreversíveis e dificultando a obtenção do formato original. Por essa razão, não é possível realizar um cálculo direto da força das senhas com base nos Hashs.

No entanto, mesmo sem calcular a força das senhas, o RPA possui outras funcionalidades importantes para reforçar a segurança das credenciais. Durante a verificação de senhas frágeis o RPA compara os Hashs cadastrados com a biblioteca de senhas vulneráveis, cadastradas previamente. Se identificada uma coincidência o RPA identifica imediatamente a necessidade de atualização da senha.

O RPA pode considerar a data de atualização das senhas para expirar aquelas que não foram modificadas há muito tempo. Senhas que não são atualizadas regularmente representam um risco. Com base nas políticas de segurança da empresa, o RPA pode expirar automaticamente as senhas que ultrapassaram o prazo definido de atualização, incentivando os usuários a criarem senhas mais seguras.

2) Verifica segurança de senhas padrão Criptografia

Foi implementado também um procedimento de criptografia para proteger a chave utilizada no processo de descriptografia. Esse procedimento visa evitar que a chave de criptografia fique armazenada no robô de forma permanente, minimizando os riscos de exposição.

No momento da execução do RPA, o administrador responsável é solicitado a inserir a chave de criptografia, que será usada apenas durante a execução do algoritmo de descriptografia das senhas. Nesta etapa se o usuário for o proprietário do banco também é possível receber esta informação diretamente do banco de dados, diminuindo ainda mais as chances de uma brecha na segurança.

Essa abordagem garante que a chave não seja armazenada em nenhum local e seja utilizada somente no momento necessário para descriptografar as senhas e calcular sua complexidade.

Uma vez descriptografadas, as senhas são submetidas a um algoritmo desenvolvido em linguagem R, que realiza uma análise detalhada para calcular a complexidade de cada senha. Esse cálculo leva em consideração vários fatores, incluindo:

- **Quantidade de Caracteres**: O algoritmo verifica o número de caracteres presentes na senha, classificando-a em diferentes tipos de acordo com essa quantidade.
- **Tipos de Caracteres Usados**: São verificados os tipos de caracteres presentes na senha, como letras maiúsculas, minúsculas, números e caracteres especiais.
- **Uso de Dados Pessoais**: O algoritmo também identifica se a senha contém informações pessoais do usuário, como nome, sobrenome, data de nascimento, entre outros, a fim de incentivar a adoção de senhas mais seguras e menos previsíveis.
- **Quantidade de Dias sem Atualização**: A data de última atualização da senha é considerada para avaliar a periodicidade com que os usuários modificam suas senhas.

Com base na análise desses fatores, o algoritmo atribui uma pontuação de 0 a 100 de segurança para cada senha, indicando o nível de complexidade e força de cada uma. Senhas com pontuação inferior a 50 são consideradas menos seguras e são automaticamente identificadas pelo RPA.

O RPA notifica todos os usuários cujas senhas obtiveram uma pontuação inferior a 50, incentivando-os a atualizarem suas senhas para opções mais seguras. Essas notificações são enviadas diretamente aos usuários, garantindo que eles estejam cientes da necessidade de aprimorar suas senhas para proteger suas contas e os dados da empresa.

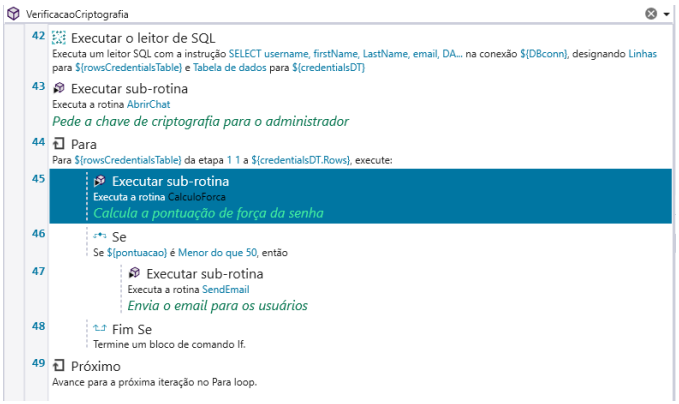

Fig. 13. Tela da verificação de segurança de senhas criptografadas. Fonte: Elaborado pela autora.

Adicionalmente, um relatório detalhado é enviado ao administrador do sistema, contendo a pontuação de segurança de todas as senhas dos funcionários. Esse relatório permite que o administrador tenha um controle pessoal sobre a força das senhas no ambiente corporativo e tome medidas adequadas para garantir a segurança das credenciais de acesso. A Fig. 13 mostra o trecho do Studio de RPA com estes comandos

3) Resultados

Ao executar o robô foi possível identificar o seguinte resultado para o primeiro funcionário cadastrado no banco de dados apresentado na Fig. 14.

Carlos	Braga	carlos.braga@testcompany.com	carlos.braga
Lucas	Souza	lucas.souza@testcompany.com	lucas.souza
Isabela	Oliveira	isabela.oliveira@testcompany.com	isabela.oliveira
Gabriel	Santos	gabriel.santos@testcompany.com	gabriel.santos
Matheus	Costa	matheus.costa@testcompany.com	matheus.costa
Maria	Almeida	maria.almeida@testcompany.com	maria.almeida
João	Pereira	joao.pereira@testcompany.com	joao.pereira
Ana	Rodrigues	ana.rodrigues@testcompany.com	ana.rodrigues
Pedro	Ferreira	pedro.ferreira@testcompany.com	pedro.ferreira

Fig. 14. Banco de dados dos usuários. Fonte: elaborado pela autora.

Na configuração feita para o usuário “Carlos Braga”, foi atribuída a senha “123456”. Esta senha foi identificada como muito fraca tanto na verificação de senhas por Hash quanto na verificação por criptografia, uma vez que é muito usada e facilmente identificável.

Após esta identificação, como sua pontuação de segurança ficou “5” e foi classificada como muito fraca foi enviado um e-mail informando ao usuário que ele deverá alterar sua senha.

Observando agora o usuário “Gabriel Santos” que possuía a senha “87623hsadH%D”, esta senha não foi identificada como fraca nem na verificação por criptografia nem na verificação por Hash, entretanto como havia mais de 120 dias que a senha não havia sido alterada sua pontuação de segurança ficou em “30”, como ainda está abaixo de 50, que é a margem configurada de segurança, este usuário também recebeu um e-mail alertando-o de sua necessidade de alterar a senha.

VII. CONCLUSÕES, TRABALHOS FUTUROS E LIMITAÇÕES

Diante do que foi evidenciado, fica claro que a criação de uma estratégia abrangente de segurança empresarial é de extrema importância.

É necessário que esta política de segurança envolva o uso de ferramentas técnicas avançadas, como VPN, *firewalls* e antivírus, mas é preciso também incluir o treinamento e conscientização dos funcionários sobre boas práticas de segurança virtual.

A implementação do RPA no gerenciamento de senhas pode ser uma solução eficiente para fortalecer a segurança das informações confidenciais, desde que o acesso ao programa seja restrito somente a administradores e que haja uma política rigorosa de gerenciamento de acesso e permissões.

É crucial promover uma cultura de conscientização de senhas dentro da empresa, incentivando a criação de senhas fortes e únicas e a troca regular das mesmas. Somente com uma abordagem completa, envolvendo tecnologia, treinamento e conscientização, é possível alcançar um nível satisfatório de segurança empresarial e proteger efetivamente os dados e ativos da organização contra as ameaças crescentes do mundo virtual.

Adicionalmente, podemos observar que a utilização de senhas salvas em formato de Hash torna mais difícil detectar suas fragilidades, tornando-se uma opção interessante para algumas empresas que buscam maior segurança.

Por outro lado, o uso de criptografia com chaves oferece um controle mais abrangente e granular sobre as senhas dos usuários, permitindo que a empresa tenha um acompanhamento detalhado e emita relatórios de segurança para monitorar a eficácia das políticas de senha.

É importante afirmar que a escolha entre utilizar Hash ou criptografia com chaves dependerá das necessidades e objetivos específicos de cada empresa.

Algumas organizações podem optar por adicionar uma camada adicional de segurança utilizando Hash para proteger as senhas armazenadas, enquanto outras podem preferir um controle mais preciso sobre o uso das senhas, utilizando criptografia.

Independentemente da abordagem escolhida, a implementação de um RPA no gerenciamento de senhas é uma medida eficiente para reforçar a segurança corporativa.

Através do uso inteligente de tecnologia e políticas de segurança, as empresas podem se proteger de ameaças virtuais e garantir uma maior proteção dos dados sensíveis. É fundamental ressaltar que, ao realizar a avaliação de senhas, é necessário estar em conformidade com a Lei Geral de Proteção de Dados (LGPD) e demais regulamentações de privacidade vigentes.

O exemplo de solução apresentado, utilizando o RPA para verificação e manutenção da segurança de senhas, pode ser adaptado e implementado em diversas outras situações, como um gerenciador de senhas empresarial, a proteção dos usuários de bancos de dados empresariais e até mesmo para garantir a segurança dos usuários dos sites da própria empresa.

Com uma abordagem abrangente e alinhada com as normas de proteção de dados, as empresas podem reforçar sua postura de segurança virtual e diminuir os riscos associados ao gerenciamento de senhas.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] LastPass, “Relatório Global sobre Segurança de Senhas,” 2019. [Online]. Available: https://www.lastpass.com/pt/state-of-the-password/global-password-security-report-2019. [Acesso em 17 Julho 2023].

[2] M. E. &. M. H. J. Whitman, Principles of Information Security, Cengage Learning, 2017.

[3] International Organization for Standardization, “ISO/IEC 27001:2022,” 2022. [Online]. Available: https://www.iso.org/. [Acesso em 22 Março 2022].

[4] W. S. a. L. Brown, Computer Security Principles and Practice, Pearson, 2017.

[5] P. Maranhão, “Startupi.com.br,” 12 04 2022. [Online]. Available: https://startupi.com.br/black-friday-instabilidade/. [Acesso em 02 07 2023].

[6] A. Novotný, “AWS High Availability Architecture,” StormIT, [Online]. Available: https://www.stormit.cloud/blog/aws-high-availability-architecture/. [Acesso em 02 Julho 2023].

[7] J. Kissell, Aprendendo a Proteger Suas Senhas, Novatec Editora, 2017.

[8] C. E. Shannon, “A mathematical theory of communication,” *The Bell System Technical Journal*, pp. 379 - 423, Julho 1948.

[9] M. Taha, T. Alhaj, A. Moktar, A. Salim e S. Abdullah, “On Password Strength Measurements: Password Entropy and Password Quality,” em *2013 INTERNATIONAL CONFERENCE ON COMPUTING, ELECTRICAL AND ELECTRONIC ENGINEERING (ICCEEE)*, Khartoum, 2013.

[10] Hive Systems, “Hive Systems,” Hive Systems, 18 Abril 2023. [Online]. Available: https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=header. [Acesso em 02 Julho 2023].

[11] Cisco, “Quais são os ataques virtuais mais comuns?,” [Online]. Available: https://www.cisco.com/c/pt_br/products/security/common-cyberattacks.html. [Acesso em 07 09 2023].

[12] Tenable, “RELATÓRIO DO CENÁRIO DE AMEAÇAS DE 2022 DA TENABLE,” 2023.

[13] NIST, “Computer Security Resource Center,” [Online]. Available: https://csrc.nist.gov/glossary/term/malware. [Acesso em 10 Julho 2023].

[14] Microsoft, “O que é o ransomware?,” 24 Abril 2023. [Online]. Available: https://learn.microsoft.com/pt-br/security/ransomware/human-operated-ransomware. [Acesso em 10 Julho 2023].

[15] Cisco, “What is Phishing,” [Online]. Available: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html. [Acesso em 10 Julho 2023].

[16] M. Conti e N. Dragoni, “A Survey of Man In The Middle Attacks,” *IEEE Communications Surveys & Tutorials*, pp. 2027-2051, 2016.

[17] P. Patni, K. Iyer, R. Sarode, A. Mali e A. Nimkar, “Man-in-the-middle attack in HTTP/2,” em *2017 International Conference on Intelligent Computing and Control (I2C2)*, Coimbatore, 2017.

[18] M. Al-Shareeda, S. Manickam e S. A. Sari, “A Survey of SQL Injection Attacks, Their Methods, and Prevention Techniques,” em *2022 International Conference on Data Science and Intelligent Computing (ICDSIC)*, Karbala, 2022.

[19] Open network foundation, “SDN architecture,” 2014.

[20] H. Al-Rushdan, M. Shurman, S. Alnabelsi e Q. Althebyan, “Zero-Day Attack Detection and Prevention in *Software*-Defined Networks,” em *2019 International Arab Conference on Information Technology (ACIT)*, Al Ain, 2019.

[21] SpyCloud, “2022 SpyCloud Annual Identity Exposure Report,” Austin, 2022.

[22] P. Carvalho, “Conta do governo posta no Twitter todas as senhas do Planalto,” Veja, 10 Janeiro 2017. [Online]. Available: https://veja.abril.com.br/coluna/radar/portal-brasil-posta-senhas-de-todas-as-contas-da-secom-no-twitter. [Acesso em 15 Junho 2023].

[23] Fortinet, “What is a Keylogger? Definition and Types,” [Online]. Available: https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers. [Acesso em 15 Junho 2023].

[24] P. Anu e S. Vimala, “A survey on sniffing attacks on computer networks,” em *2017 International Conference on Intelligent Computing and Control (I2C2)*, Coimbatore, 2017.

[25] R. Clancy, “Password Sniffing in Ethical Hacking and Its Types Explained,” EC-Council, [Online]. Available: https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/ethical-hacking-password-sniffing/#:~:text=Password%20sniffing%20is%20a%20type,passwords%20from%20the%20intercepted%20data.. [Acesso em 15 Junho 2023].

[26] J. E. H. M. Gaspar, “Análise comportamental sobre ataques de engenharia,” 2015.

[27] R. F. Diorio, E. Serafim, K. R. Alves e M. C. Meira, “Ataques de Força Bruta: Um Estudo Prático,” em *2019 Brazilian Technology Symposium*, Capivari, 2019.

[28] Akamai, “O que é um ataque de força bruta?,” [Online]. Available: https://www.akamai.com/pt/glossary/what-is-brute-force-attack. [Acesso em 16 Junho 2023].

[29] Nacional Cyber Security Center, “What is an antivirus product? Do I need one?,” [Online]. Available: https://www.ncsc.gov.uk/guidance/what-is-an-antivirus-product#:~:text=Antivirus%20products%20work%20by%20detecting,and%20other%20types%20of%20malware.. [Acesso em 16 Junho 2023].

[30] Gartner, “Endpoint Protection Plataforms Reviews and Ratings,” 2022. [Online]. Available: https://www.gartner.com/reviews/market/endpoint-protection-platforms. [Acesso em 16 Junho 2023].

[31] Psafe, “PESQUISA SOBRE USO DE DISPOSITIVOS PARA TRABALHO NO BRASIL,” [Online]. Available: https://www.psafe.com/blog/wp-content/uploads/2020/09/Pesquisa-Ciberseguran%C3%A7a-no-Trabalho.pdf.

[32] Computer Hope, “VPN,” [Online]. Available: https://www.computerhope.com/jargon/v/vpn.htm. [Acesso em 07 Julho 2023].

[33] “O Que é Automação Robótica de Processos (RPA)?,” 12 Agosto 2021. [Online]. Available: https://blog.dsacademy.com.br/o-que-e-automacao-robotica-de-processos-rpa/. [Acesso em 16 Julho 2023].

[34] Automation Anywhere, “Descubra as diferenças entre automação assistida e não assistida e qual delas melhor atende as necessidades do seu negócio,” [Online]. Available: https://www.automationanywhere.com/br/rpa/attended-vs-unattended-rpa. [Acesso em 17 Junho 2023].

[35] Gartner, “Gartner Magic Quadrant for Robotic Process Automation,” 2022. [Online]. Available: https://www.gartner.com/en/documents/4016876. [Acesso em Julho 2023].

[36] Nordpass, “Top 200 most common passwords list,” 2022. [Online]. Available: https://nordpass.com/most-common-passwords-list/. [Acesso em 15 Julho 2023].

Marcelo S. de Castro graduou-se em Engenharia Elétrica pela Universidade Federal de Juiz de Fora (1992), com mestrado em Engenharia Elétrica pela Universidade Estadual de Campinas (1995) e doutorado em Engenharia Elétrica pela UnB (2010). Docente Associado da Universidade Federal de Goiás, tendo ingressado em 1996. Possui experiência na área de engenharia de redes, computação paralela e distribuída, comunicações óticas e tecnologias alternativas de última milha (BPL, ZigBee, Wi-Fi). Desenvolve pesquisas em temas que incluem redes de comunicação (5G, Gigabit Wi-Fi), *Smart Grids*, *Smart Cities*, *Smart Campus*, tecnologia da informação e comunicação e gestão aplicadas a projetos de redes de telecomunicações, projetos de automação usando Plataforma Arduino e educação em engenharia.

Mariana Inácia Xavier Borges é graduanda em Engenharia de Computação na Universidade Federal de Goiás. Atualmente é analista de negócios na Ciatécnica em São Paulo-SP. Tendo experiência no desenvolvimento de soluções tecnológicas em RPA que buscam melhorar e otimizar processos.