# Obsolescência não-Programada: Análise do Uso de Software Desatualizado em Ambiente de Produção

**Luan Marko Kujavski**[1], **Ulisses Penteado**[2], **Paulo Lisboa de Almeida**[1], **André Grégio**[1]

[1]Departamento de Informática – Universidade Federal do Paraná (UFPR)
Curitiba – PR – Brasil

[2]Bluepex – Centro de P&D
Limeira – SP – Brasil

{luan.marko,paulo,gregio}@ufpr.br, ulisses@bluepex.com.br

***Abstract.*** *The advance of computing has expanded attack surfaces, creating new targets for criminals to exploit known and unpatched vulnerabilities. It is essential to frequently provide system maintenance and updates, but the lack of good practices exposes users to avoidable risks. Reports indicate that 76% of ransomware attacks in 2022 exploited known vulnerabilities. In this article, we investigate the issue of outdated software in organizations, based on data from over 129 million activity records of 23,000 users in 567 organizations. Our contributions include a regionalized analysis of software obsolescence, lessons for prioritizing preventive policies, and the availability of anonymized data for future studies in the field.*

***Resumo.*** *O avanço da computação ampliou as superfícies de ataque, criando novos alvos para criminosos explorarem vulnerabilidades conhecidas e não corrigidas. A manutenção e atualização constante de sistemas são essenciais, mas a falta de boas práticas expõe usuários a riscos evitáveis. Relatórios indicam que 76% dos ataques de ransomware em 2022 exploraram vulnerabilidades conhecidas. Este artigo investiga o problema do software desatualizado em organizações, com base em dados de mais de 129 milhões de registros de atividades de 23 mil usuários em 567 organizações. As contribuições incluem análise regionalizada da desatualização de programas, lições para priorização de políticas preventivas e disponibilização de dados anonimizados para estudos futuros.*

## 1. Introdução

Avanços na computação e sua inserção em praticamente todas as demais áreas de conhecimento expandiram as superfícies de ataque e criaram novos alvos de oportunidade para criminosos e códigos de exploração automatizados. Tais ataques são possíveis devido a vulnerabilidades conhecidas, geralmente catalogadas na base do CVE (*Common Vulnerabilities and Exposures*) [National Vulnerability Database 2024] e não corrigidas pelos usuários desses programas e sistemas vulneráveis. Por exemplo, entre junho e julho de 2023, a Filial Executiva Civil Federal do Governo Americano (FCEB) sofreu um ataque que explorou uma vulnerabilidade crítica (CVE-2023-26360) [NIST 2023], a qual permitia executar código arbitrário [Adobe Security Bulletin 2023]. O ataque foi possível devido ao uso de programas desatualizados e em fim de ciclo de vida [Jones 2023].

No Brasil, o CERT.br foi notificado sobre centenas de milhares de dispositivos expostos na Internet contendo má-configuração ou vulnerabilidades conhecidas no último ano (maio/2023–abril/2024), sendo 15.610 deles somente em abril deste ano [CERT.br 2024].

Uma das principais premissas para proteção é a aplicação de políticas para manutenção e atualização constante de sistemas e aplicações. Embora existam diversos mecanismos para aumentar a segurança e a privacidade de sistemas e seus usuários, a falta de boas práticas ou impossibilidade de atualização (seja por algum motivo de usabilidade ou por problemas inerentes da interação entre sistemas e aplicações) pode quebrar tal premissa. Dessa forma, as organizações e usuários que fazem uso de software desatualizado ficam expostos à exploração de vulnerabilidades que já foram corrigidas e poderiam ser facilmente evitadas. O problema do software desatualizado é tão grave que um relatório disponibilizado em 2023 sobre gerenciamento de vulnerabilidades e ameaças mostrou que 76% dos ataques por *ransomware* em 2022 foram possíveis devido a vulnerabilidades conhecidas publicamente entre 2010 e 2019, e cujos usuários e organizações vítimas não aplicaram as atualização que as corrigiam [Securin et al. 2023]. No mesmo período, estimou-se que *ransomware* foi a maior causa de ataques no ciberespaço brasileiro (52%) [Fan 2023].

Neste artigo, aborda-se o problema do software desatualizado nas organizações através de um estudo realizado em informações geradas a partir de dados reais compostos por cerca de 129 milhões de registros das atividades de mais de 23 mil usuários empregados em 567 organizações. Com base nesses dados, estabeleceu-se as seguintes Perguntas de Pesquisa:

- **PP1**. *Qual a proporção de softwares atualizados e desatualizados empregada pelos usuários?*
- **PP2**. *O quão desatualizados (e.g., em meses) estão os softwares utilizados pelos usuários?*
- **PP3**. *Existe um subconjunto de softwares em que os esforços de monitoramento devem ser focados?*

As principais contribuições do presente trabalho são: (i) prover informações gerais em um conjunto abrangente e regionalizado (América Latina) de dados reais, analisando o quão desatualizados estão os programas utilizados pelos usuários das organizações monitoradas; (ii) tirar lições para priorização de implantação e reforço de políticas preventivas, analisando a existência de subconjunto de programas para os quais os esforços de proteção e atualização podem causar mais impacto; (iii) criar e disponibilizar um conjunto de dados **anonimizados**, cujas características podem dar margem a trabalhos futuros, bem como permitir a reprodutibilidade dos experimentos mostrados nesse artigo.

O restante do artigo está dividido da seguinte forma: na Seção 2, discute-se os trabalhos relacionados mais próximos a este sob a ótica da metodologia aplicada para coleta de informações (entrevistas, análise de *logs*) e das lições aprendidas; na Seção 3, descreve-se os dados coletados e a base de dados modelada para armazená-los de forma a permitir sua posterir análise; na Seção 4, é feita a descoberta de conhecimento via informações providas nos dados e, a partir delas, estuda-se o caso dos navegadores; na Seção 5, apresenta-se as lições aprendidas advindas da análise dos dados disponíveis; por fim, as considerações finais encontram-se na Seção 6.

## 2. Trabalhos Relacionados

Nesta seção, discute-se literatura que motiva o presente trabalho, bem como artigos relacionados ao tema porém em outros contextos e época. A avaliação da literatura é feita com foco nas lições aprendidas de cada artigo examinado.

[Garcia 2023] destaca os riscos significativos associados ao uso de software desatualizado. À medida que a tecnologia avança rapidamente, novas atualizações e versões de software são lançados frequentemente, mas muitos usuários negligenciam a atualização de seus sistemas, expondo-se a graves ameaças de segurança. Vulnerabilidades em software desatualizado são frequentemente exploradas por cibercriminosos para realizar ataques como infecção por malware, roubo de dados e ataques de ransomware. A falta de atualização impede o acesso a *patches* de segurança importantes, deixando o sistema suscetível a *exploits* conhecidos e já corrigidos.

[Bellissimo et al. 2006] exploram a segurança dos mecanismos de atualização de software e destacam as vulnerabilidades existentes. Muitos sistemas de atualização são vulneráveis a ataques do tipo *man-in-the-middle*[1] devido à falta de medidas básicas de segurança, como a verificação de assinaturas digitais. Tecnologias emergentes, como dispositivos móveis e médicos, apresentam desafios adicionais devido à conectividade esporádica e recursos computacionais limitados. Por fim, enfatizam a necessidade de padrões para atualizações seguras e sugere que a infraestrutura de distribuição deve ser considerada não confiável. As lições aprendidas providas como resultados incluem a importância de se implementar técnicas bem compreendidas de distribuição segura de conteúdo em sistemas de atualização de software para evitar vulnerabilidades. Além disso, a conscientização e o compromisso dos desenvolvedores e usuários são cruciais para melhorar a segurança.

[Wash et al. 2014] discutem os desafios e implicações de atualizações automáticas de software em termos de segurança e usabilidade. Os autores argumentam que, embora as atualizações automáticas possam melhorar a segurança ao garantir que os *patches* sejam instalados prontamente, elas também podem causar consequências indesejadas. Muitos usuários não entendem o que está acontecendo em seus computadores devido à falta de transparência no processo de atualização. Essa falta de compreensão pode levar a uma desconexão entre as intenções dos usuários e o comportamento real de seus sistemas, resultando em computadores que, paradoxalmente, podem ser mais ou menos seguros do que os usuários pretendiam. O estudo utilizou uma abordagem multi-metodológica, incluindo entrevistas, pesquisas e análise de dados de *logs* de computadores, com 37 usuários do Windows 7. Descobriu-se que mais da metade dos participantes tinha uma compreensão incorreta das configurações de atualização de seus computadores e muitos não conseguiam executar suas intenções de gerenciamento de atualizações. Isso sugere que, embora a automação das atualizações de software possa melhorar a segurança, ela também dificulta a capacidade dos usuários de aprender e tomar decisões informadas sobre a segurança de seus sistemas. Assim, os autores concluem que um equilíbrio entre automação e intervenção do usuário é essencial para maximizar tanto a segurança quanto

[1] O ataque de *man-in-the-middle* em questão foi realizado interceptando a comunicação entre o cliente e o servidor de atualização. Ao modificar as respostas do servidor ou redirecionar as solicitações do cliente, os atacantes conseguiram introduzir código malicioso, aproveitando-se da falta de autenticação adequada nas conexões e nas assinaturas dos binários.

a usabilidade.

[Li et al. 2019] abordam a criticidade de se manter os sistemas atualizados para garantir a segurança das organizações. Os administradores de sistemas, responsáveis por gerenciar inúmeros computadores, enfrentam desafios únicos em relação ao processo de atualização de software: o estudo baseou-se em uma pesquisa com 102 administradores e 17 entrevistas detalhadas, e identificou cinco etapas principais no processo de atualização: aprendizado sobre atualizações, decisão de atualizar, preparação para a instalação, implantação das atualizações e resolução de problemas pós-implantação. Essas etapas envolvem considerações e ações significativamente diferentes das praticadas pelos usuários finais, destacando a necessidade de focar especificamente na população de administradores para melhorar a eficácia das atualizações e, consequentemente, a segurança dos sistemas. As lições aprendidas no artigo revelam que os administradores de sistemas enfrentam dificuldades em obter informações significativas sobre atualizações, testar e implantar atualizações de maneira eficaz e lidar com problemas induzidos pelas atualizações, e que influências organizacionais e de gestão podem afetar a capacidade dos administradores de gerenciar atualizações de maneira eficiente. As recomendações incluem a necessidade de sistemas melhores para gerenciar atualizações, melhorias no design das atualizações e mudanças nas políticas organizacionais para apoiar melhor os administradores em suas funções cruciais de manter os sistemas seguros, dado que os impactos da não-atualização de software podem ser severos, como exemplificado pela violação de dados da Equifax em 2017 [Federal Trade Comission 2022], que expôs informações pessoais de mais de 140 milhões de indivíduos.

[Martius and Tiefenau 2020] analisam a importância das informações relacionadas a atualizações de software para administradores de sistemas, enfatizando como a falta de informações necessárias pode dificultar a avaliação do impacto dos *patches* e atrasar sua implementação. Para tanto, os autores consideraram a análise das notas de lançamento de quatro fornecedores de software, bem como realizaram entrevistas e pesquisas com administradores de sistemas para entender quais informações são consideradas essenciais. Os resultados indicam que informações sobre o propósito da atualização, dependências e problemas conhecidos são as mais valorizadas pelos administradores, que tendem a ler mais frequentemente as notas de atualizações manuais em comparação com as automáticas. Um dos estudos de caso de exemplo é o do ransomware WannaCry, que explorou uma vulnerabilidade para a qual a Microsoft já havia lançado um *patch*, mas que muitos sistemas não haviam aplicado devido à falta de destaque na criticidade da atualização [Kerner 2017]. O artigo corrobora o senso comum de que os administradores de sistemas, responsáveis por um grande número de máquinas, desempenham um papel crucial na prevenção de explorações, mas a falta de informações claras nas notas de atualização pode atrapalhar o processo de decisão e implementação, expondo sistemas a riscos muitas vezes desnecessários. A principal recomendação do artigo que fica como lição aprendida é a separação de atualizações de segurança das de funcionalidade, de forma a facilitar a gestão e melhorar a segurança geral dos sistemas computacionais.

[Jenkins et al. 2024] abordam as práticas de gerenciamento de *patches* entre administradores de sistemas e como o contexto de trabalho influencia tais práticas. Para tanto, os autores coletaram dados de 220 administradores de sistemas de diversas organizações, examinando fatores como a disponibilidade de ambientes de teste e o uso de

fontes de informação online. Descobriu-se que, embora a maioria dos administradores tenha acesso limitado a ambientes de teste dedicados, muitos adotam abordagens informais, como o uso de máquinas virtuais ou ambientes pessoais para testar *patches*. Além disso, descobriu-se que os administradores em pequenas e médias empresas (PMEs) frequentemente recorrem a fóruns online para suporte, ao contrário de seus colegas em grandes organizações, que tendem a levantar *tickets* diretamente com os fornecedores das soluções implantadas. As perguntas de pesquisa principais desse estudo foram: "Quais práticas os administradores de sistemas adotam durante os diferentes estágios do processo de *patching*, e quão prevalentes são essas práticas?" e "Como o contexto de trabalho de um administrador de sistemas (por exemplo, tamanho da organização, tipo de sistema suportado) impacta as práticas de *patching*?". Os resultados mostraram que as práticas de *patching* variam significativamente com o tamanho da organização e o tipo de sistema gerenciados e que administradores de grandes organizações geralmente seguem políticas de *patching* mais estruturadas e têm maior acesso a recursos de teste, enquanto aqueles em PMEs dependem mais de abordagens informatis e suporte comunitário online.

É visível que os trabalhos relacionados possuem escopo delimitado em suas regiões (que não o Brasil ou América Latina), além de não apresentarem escala (um foi limitado a 37 usuários, outro a 102 administradores de sistemas, um terceiro a 220 administradores de sistemas). A maioria baseou-se em entrevistas que, embora importantes para se compreender os problemas inerentes ao gerenciamento de software desatualizado em organizações de tamanhos diversos, mostra a dificuldade em se ter massa de dados nessa área para investigações técnicas mais profundas e descoberta de tendências. A data de publicação dos trabalhos relacionados também mostra que o problema tem se mantido atual ao longo das décadas. Esses fatos mostram que o presente trabalho, além de ser atual, com dados coletados neste ano de 2024, possui escopo abrangente, tanto na quantidade de organizações quanto nas dezenas de milhares de usuários cujos *logs* foram analisados, e pode fomentar novos estudos que ajudem a compreender melhor os problemas de gerenciamento de *patches* com foco regional nacional.

## 3. Coleta e Armazenamento dos Dados

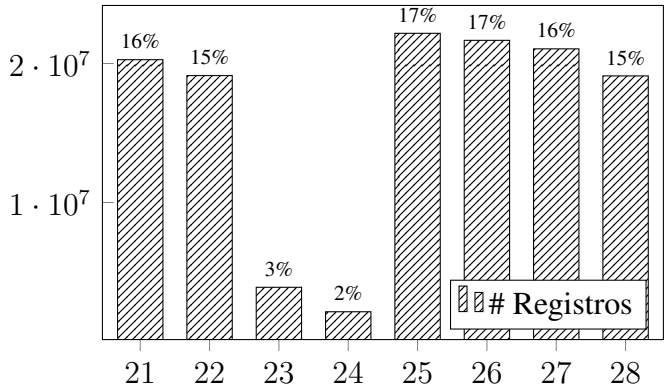
A coleta de dados ocorreu entre os dias 21 e 28 de março de 2024, totalizando oito dias. A base de dados foi gerada a partir do monitoramento das atividades de 23.704 usuários distintos. Para cada usuário, são gerados registros mostrando qual a janela ativa corrente (janela em *foreground*) e por quanto tempo essa janela permaneceu ativa, gerando um total de cerca de 55GB de dados de coleta, representando 129.427.331 registros de atividade.

O histograma da Figura 1 mostra o número de registros coletados para cada um dos dias. Como esperado, a quantidade de registros coletados nos diferentes dias é aproximadamente igual, exceto para os dias 23 e 24 de março, que se tratam de um sábado e domingo, respectivamente.

A coleta se deu por meio de um aplicativo para o monitoramento da segurança desenvolvido por empresa privada, contabilizando uma amostragem de 567 empresas diferentes. Ao todo, há registros de que 9.780[2] softwares diferentes foram usados no período analisado, totalizando 2.011.927 horas de uso ao se considerar todas as aplicações.

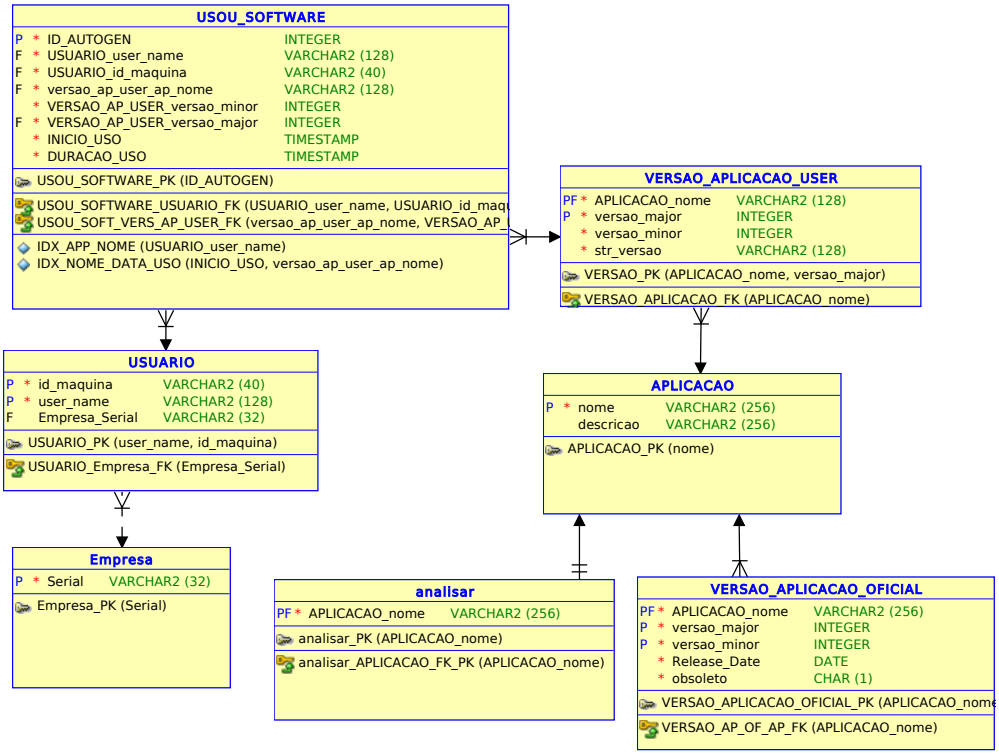
[2]Um fator que influenciou nesse valor expressivo é o grande número de programas executados uma única vez, como instaladores.

**Figura 1. Número de Registros por dia de coleta.**




A fim de facilitar a exploração dos dados coletados, foi modelado um banco de dados relacional utilizando o PostgreSQL 14.11. O diagrama físico do banco de dados modelado está ilustrado no diagrama da Figura 2. O conjunto de dados sanitizados/anonimizados, para preservação da privacidade dos usuários e organizações, está disponibilizado em `https://github.com/secretrdlab/Dataset_users_organizations`.

**Figura 2. Diagrama relacional do banco de dados.**




## 4. Análise dos Dados Coletados

Devido ao grande número de amostras coletadas, começamos nossa análise na Seção 4.1 considerando os 100 softwares mais utilizados pelos usuários. Já na Seção 4.2, realizamos

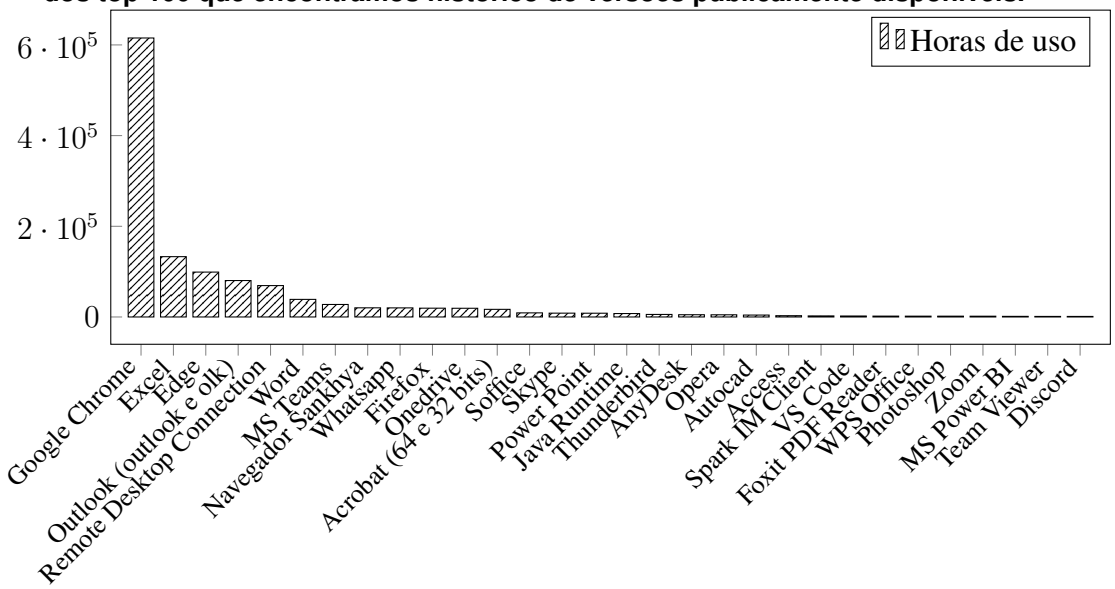
uma análise considerando apenas os navegadores web utilizados pelos usuários, por se tratarem de softwares amplamente utilizados, e por comumente serem porta de entrada para o uso de outros softwares por parte dos usuários.

### 4.1. Análise considerando os top 100 Softwares

Apesar do grande número de softwares distintos utilizados (9.780, como discutido na Seção 3), é possível constatar que os usuários passam 88,0% do tempo usando apenas os top 100 softwares mais usados, representando 1.770.725 horas de uso.

Da lista dos top 100 softwares mais usados removemos softwares nativos do sistema, como o Windows Explorer e a calculadora do Windows, e removemos também os softwares que não possuem histórico de versões disponível publicamente na internet, como softwares criados por encomenda. Com essas remoções, dos top 100 softwares restaram 31, que serão foco de nossa análise. Esses 31 softwares representam 1.230.038 horas de uso (61% do total). O histograma da Figura 3 mostra os nomes desses softwares, juntamente com o número de horas de uso registradas no banco de dados para cada um deles.

**Figura 3. Soma de horas gastas pelos usuários considerando os 31 softwares dos top 100 que encontramos histórico de versões publicamente disponíveis.**




Para cada um dos 31 softwares selecionados, cadastramos em um banco de dados uma lista com um histórico de suas versões e data de lançamento destas, a fim de comparar com as versões utilizadas pelos usuários monitorados. Essa lista de versões foi criada a partir de pesquisas em repositórios disponíveis na internet. Foram registrados um total de 10.405 versões de software no banco de dados. Considerando apenas o navegador Google Chrome, por exemplo, foram cadastradas 318 versões de software.

Com isso, considerando os softwares com versões cadastradas, conseguimos realizar uma análise para 1.140.791 horas de usos de software[3]. A partir desses dados, rea-

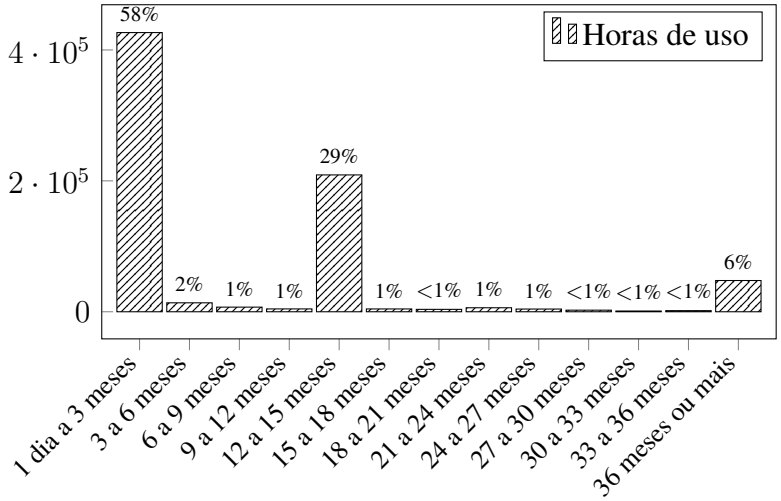
[3]Nossa equipe não foi capaz de encontrar algumas versões de software usadas pelos usuários, portanto

lizamos a descoberta intrigante de que os usuários passaram 65,2% do tempo utilizando softwares desatualizados (744.246 horas).

Para definir se um usuário está usando um software desatualizado, comparamos a versão do software utilizado com a versão disponível na data de uso. Tomamos o cuidado de verificar se a versão do software usada pelo usuário ainda é mantida pela companhia responsável e, caso positivo, verificamos se o usuário está usando a versão mais recente disponível. Por exemplo, se o usuário usou o Microsoft Excel 2019, verificamos se ele usou a versão atualizada do Microsoft Excel 2019 (apesar de existirem versões mais recentes do Excel, como a 2021), pois a Microsoft mantém a Suíte Office 2019 atualizada. Já se, por exemplo, o usuário utilizou o Microsoft Excel 2003, consideramos que ele deveria estar usando a versão mais recente do Excel (2021), pois o a Suíte Office 2003 foi descontinuada.

O histograma da Figura 4 mostra o número de horas gastas em softwares com diferentes quantidades de meses de desatualização. Como pode-se observar, na maioria do tempo (58%) os usuários usam softwares com no máximo 3 meses de desatualização. No entanto, há uma grande quantidade de horas gastas com softwares com cerca de 1 ano de desatualização, e 6% do total de horas de uso com softwares desatualizados são referentes a softwares com 3 anos ou mais de desatualização.

**Figura 4. Horas de uso para softwares com diferentes tempos de obsolescência.**




Nossa pesquisa também mostrou que no período de coleta dos dados, 88,7% dos usuários usaram pelo menos uma vez algum software com desatualização maior ou igual a um ano. Esse valor é alarmante, já que mostra que a grande maioria dos usuários não se preocupa em manter todos seus softwares atualizados.

Na Figura 5 mostramos a quantidade de horas total usada com softwares com um ano ou mais de desatualização[4]. A Figura mostra um ranqueamento diferente do uso de softwares quando comparada com a Figura 3. Podemos observar que os navegadores, que

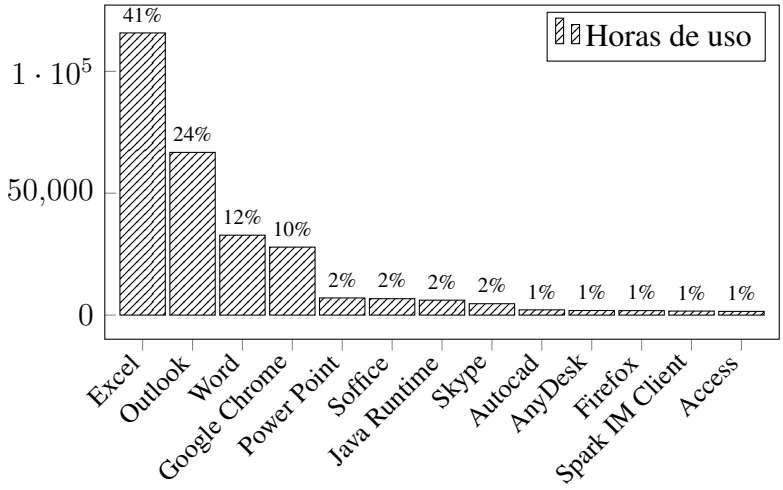
o número é um pouco menor que 1.230.038.

[4]Na Figura mostramos apenas softwares que representam 1% ou mais do uso desatualizado.

apareciam no topo da Figura 3, não aparecem com a mesma frequência quando considerando o uso com um ano ou mais de desatualização.

Nota-se que softwares pagos tendem a aparecer no topo da lista da Figura 5. A suíte do Microsoft Office, por exemplo (Excel, Outlook, Word e Power Point, sem considerar o Access) representa 78,8% dos usos de software com um ano ou mais de desatualização. Outro caso interessante é o do Autocad, que é um software altamente especializado (criação de projetos de engenharia) usado por poucos usuários, representando apenas 0,2% das horas registradas de uso. Apesar disso, quando considerando os usos de softwares com desatualização maior ou igual a um ano, o Autocad salta para 0,8% dos usos. Analisando os dados, detectamos que 51% das horas usos do Autocad eram de versões com um ano ou mais de desatualização (2.140 das 4.211 horas registradas no banco para esse software).

**Figura 5. Horas de uso para softwares com um ano ou mais de desatualização.**




Temos algumas hipóteses para a prevalência de softwares pagos na análise de softwares com um ano ou mais de desatualização:

1. Por questões de custo, os usuários podem continuar usando versões antigas que já não são mais mantidas pelas companhias, em vez de investirem em versões novas. Para corroborar com essa hipótese, constatamos que 28.488 das 257.772 horas (11%) de uso registradas para a suíte do Microsoft Office são referentes a versões anteriores à 16, que já não é mantida pela Microsoft[5].
2. Por questões de compatibilidade ou hábito, os usuários podem optar por continuar usando versões que já não são mantidas de softwares. Por exemplo, usuários podem optar por utilizar versões obsoletas do software Autocad, por terem arquivos (projetos) que foram criados nessas versões, que demandariam algum custo para serem compatibilizados para versões mais novas. Além disso, a atualização dos softwares poderia exigir retreinamento da equipe para se adequar às mudanças introduzidas nas novas versões, acarretando assim, mais uma vez, em custos extras.

[5] `learn.microsoft.com/en-us/deployoffice/endofsupport/resources`

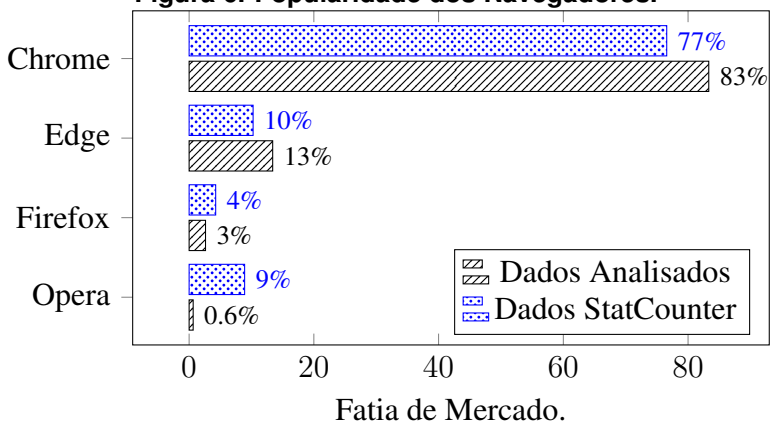
3. Diferente de, por exemplo, navegadores que muitas vezes exigem ou ao menos insistentemente mostram mensagens indicando que precisam ser atualizados, esses softwares são menos invasivos em suas políticas de atualização, mostrando apenas, por exemplo, mensagens esporádicas de que precisam ser atualizados. Essas mensagens podem ser ignoradas ou até desabilitadas pelos usuários.

### 4.2. Análise do Uso de Navegadores

Nessa Seção fazemos uma análise focando apenas no uso de navegadores amplamente disponibilizados ao público em geral, sendo eles o Google Chrome, Microsoft Edge, Mozilla Firefox, e o Opera (Opera Software). A análise dos navegadores merece atenção especial, uma vez que (i) são o tipo de software mais usado pelos usuários, representando 36,7% do total das horas de uso de softwares registradas; (ii) por se tratarem de uma porta de acesso direta à internet e a outras aplicações, são frequentes os registros no banco *Common Vulnerabilities and Exposures* (CVE) referentes a falhas de segurança nessas aplicações; essas falhas comumente são corrigidas em versões atualizadas dos softwares, exigindo assim suas constantes atualizações [Security ScoreCard 2024]; (iii) esse tipo de software é comumente distribuído de forma gratuita, removendo possível viés referente à custos de aquisição.

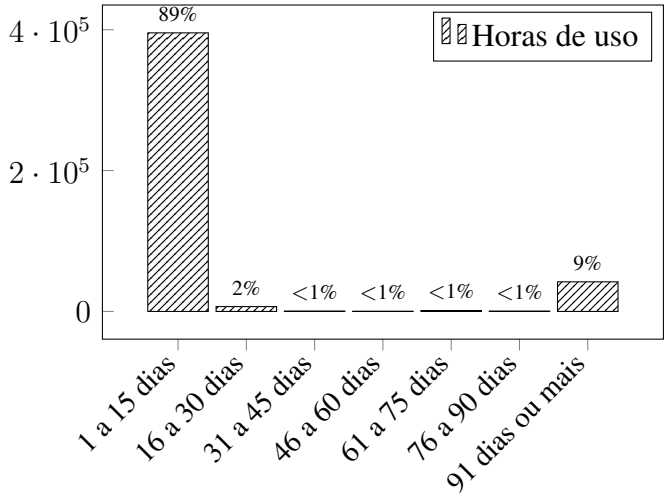
Na Figura 6 começamos mostrando a popularidade dos navegadores nos dados coletados, mostrando a fatia de mercado de cada um. Para fins de comparação, adicionamos também os dados providos pelo serviço StatCounter (`gs.statcounter.com/browser-market-share`) referentes ao mês de março de 2024, considerando os navegadores envolvidos na análise e usuários de sistemas desktop no Brasil. Como pode ser observado, os dados coletados são similares aos disponibilizados pelo StatCounter, exceto para o navegador Opera, que apresenta um uso geral de 9% de acordo com o StatCounter, mas é usado por menos de 1% dos usuários das empresas consideradas neste artigo.

**Figura 6. Popularidade dos Navegadores.**




Um ponto fundamental é descobrir o quão desatualizados os navegadores estão. Na Figura 7 é mostrado que 89% dos navegadores possuem 15 dias ou menos de desatualização. Apesar de ser um número relativamente pequeno de dias, é importante reforçar que, como citado anteriormente, os navegadores são muitas vezes portas de entrada para outros softwares (maliciosos ou não), e é fundamental que eles estejam atualizados.

**Figura 7. Horas de uso de Navegadores com diferentes tempos de obsolescência.**

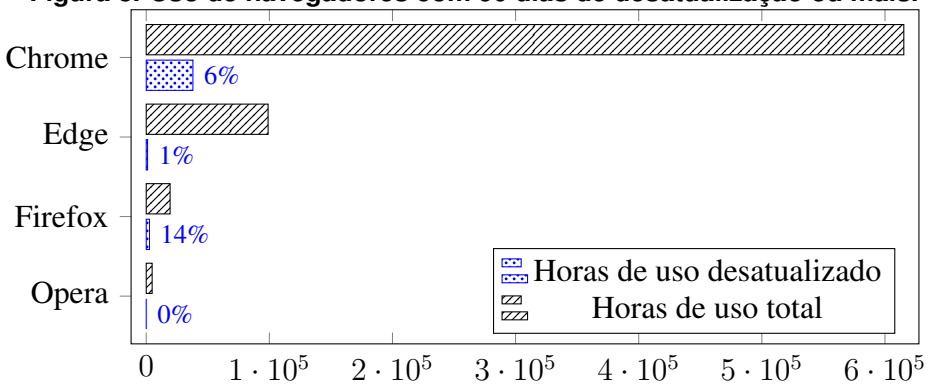



Meses de obsolescência.

Um ponto alarmante da Figura 7 é que 9% das horas de uso de navegadores foram realizadas em navegadores com 91 dias ou mais de desatualização. Uma análise dos dados dispnibilizados pelo CVE mostra que somente neste primeiro semestre de 2024, foram reportadas 96 vulnerabilidades para o Google Chrome (entre 2009 e junho/2024, a quantidade de vulnerabilidades é 3396), 5 para o Microsoft Edge (735 entre 2015 e junho/2024), 76 para o Mozilla Firefox (2604 entre 2003 e junho/2024) e 282 para o Opera entre 2003 e 2018 (não há informações mais recentes deste vendedor no arquivo do CVE) [Security ScoreCard 2024].

Já na Figura 8 são mostrados os navegadores com maior incidência de uso com desatualização de 91 dias ou mais. Como pode-se observar, em números absolutos, o Google Chrome é o navegador mais usado em versões desatualizadas. Já em números relativos, o Mozilla Firefox é o mais usado de forma desatualizada, sendo que 14% das suas horas de uso são referentes a versões com 91 dias ou mais de desatualização (2.666 das suas 19.390 horas de uso registradas em nosso banco de dados).

**Figura 8. Uso de navegadores com 90 dias de desatualização ou mais.**




Horas de Uso.

## 5. Lições aprendidas

A seguir, apresentamos as lições aprendidas com a análise dos dados obtidos nesse artigo, respondendo as perguntas de pesquisa apresentadas na introdução deste trabalho.

**PP1: Qual a proporção de softwares atualizados e desatualizados empregada pelos usuários?** – Considerando as aplicações analisadas, os usuários passaram 65% do tempo usando aplicações desatualizadas, e 89% dos usuários usaram pelo menos uma vez algum software com desatualização maior ou igual a um ano. Essas proporções são alarmantes e mostram a necessidade da implementação de diretivas de atualização de softwares nas companhias, já que esses softwares desatualizados podem ser fontes de falhas de segurança.

**PP2: O quão desatualizados estão os softwares utilizados pelos usuários?** – Nossa pesquisa mostrou que existem softwares em uso com os mais variados períodos de desatualização, variando de alguns dias até vários anos sem nenhuma atualização. Os resultados mostram que os usos de softwares desatualizados se concentram com quantidades de dias de desatualização relativamente pequenos, de até três meses, representando 37% do total dos dados analisados. No entanto, considerando desatualizações severas, de 12 meses ou mais, os dados levantados mostram que os usuários passaram 280.400 horas utilizando softwares desatualizados, representando 24% dos dados analisados. Quando considerando apenas os navegadores, os resultados mostram que 4% das horas gastas com navegadores são referentes a versões com 12 meses ou mais de obsolescência.

**PP3: Existe um subconjunto de softwares em que os esforços de monitoramento devem ser focados?** – Os usuários tendem a concentrar-se em um grupo relativamente pequeno de aplicações. As 100 aplicações mais usadas cobrem 88% de todo o tempo que os usuários gastam durante seus dias de trabalho. Mesmo considerando apenas as 31 aplicações analisadas neste trabalho, há uma cobertura de 61% do tempo de uso dos softwares pelos usuários. Esse resultado mostra que focar o monitoramento nas aplicações mais usadas exigindo que, por exemplo, essas aplicações estejam atualizadas, pode cobrir grande parte dos problemas causados por softwares obsoletos nas companhias, respondendo assim a nossa pergunta de pesquisa 3.

## 6. Conclusão

A utilização de software desatualizado pode levar a problemas de compatibilidade, comprometimento de dispositivos tradicionais e móveis, e riscos associados a dispositivos IoT (Internet das Coisas), muito utilizados em sistemas sensíveis, tais como fechaduras eletrônicas e automação doméstica em geral. Esses dispositivos conectados, se operarem com software desatualizado, podem causar danos extensivos ao serem vinculados a uma rede corporativa.

Além disso, o uso de software obsoleto pode resultar em riscos legais, especialmente para empresas que podem enfrentar ações legais de clientes e parceiros devido a incidentes de segurança cibernética. Para mitigar esses riscos, é crucial manter todos os componentes de software atualizados, implementar processos de gerenciamento de atualizações e educar os usuários sobre a importância de manter o software atualizado.

Neste artigo, analisou-se o uso de software desatualizado entre os usuários, revelando que 65% do tempo foi gasto em aplicações desatualizadas, com 89% dos usuários

utilizando software desatualizado por um ano ou mais. A desatualização variou de alguns dias a vários anos, com 37% do uso concentrado em softwares desatualizados por até três meses e 24% por 12 meses ou mais, incluindo 4% do tempo gasto em navegadores obsoletos.

Isso implica que, ao focar o monitoramento e a atualização das 100 aplicações mais utilizadas, que cobrem 88% do tempo de uso, pode-se resolver grande parte dos problemas causados por softwares desatualizados. Esses achados destacam a necessidade urgente de políticas de atualização de software que sejam realmente implantadas e verificadas nas organizações. Trabalhos futuros incluem a coleta e análise dos dados em mais organizações ao longo de meses, visando estabelecer-se tendências e avaliar mudanças de comportamento dos usuários caso políticas de atualização sejam implantadas.

## Agradecimentos

Este trabalho foi apoiado pelo Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) – Concessão 405511/2022-1 e pela Bluepex CyberSecurity via financiamento de projeto de Inovação da Base Industrial de Defesa – Edital MD/MCTI/FINEP/FNDCT 2022.

## Referências

Adobe Security Bulletin (2023). Security updates available for adobe coldfusion | apsb23-25. `https://helpx.adobe.com/security/products/coldfusion/apsb23-25.html`.

Bellissimo, A., Burgess, J., and Fu, K. (2006). Secure software updates: Disappointments and new challenges. In *First USENIX Workshop on Hot Topics in Security (HotSec 06)*, Vancouver, B.C. Canada. USENIX Association.

CERT.br (2024). Serviços vulneráveis. `https://stats.cert.br/vulns/`.

Fan, R. (2023). Brasil é o país com o maior volume e dados expostos no mundo. `https://www.defesanet.com.br/seguranca/brasil-e-o-pais-com-o-maior-volume-e-dados-expostos-no-mundo/`.

Federal Trade Comission (2022). Equifax data breach settlement. `https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement`. Acessado em Junho de 2024.

Garcia, D. (2023). Ticking time bombs: The danger of outdated software in the cybersecurity landscape. `https://david-garcia.medium.com/ticking-time-bombs-the-danger-of-outdated-software-in-the-cybersecurity-landscape-6498d437ec16`. Accessed: 2024-06-07.

Jenkins, A. D. G., Liu, L., Wolters, M. K., and Vaniea, K. (2024). Not as easy as just update: Survey of system administrators and patching behaviours. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA. Association for Computing Machinery.

Jones, C. (2023). Cisa details twin attacks on federal servers via unpatched coldfusion flaw. `https://www.theregister.com/2023/12/05/cisa_coldfusion_government/`.

Kerner, S. M. (2017). Wannacry ransomware attack hits victims with microsoft smb exploit. https://www.eweek.com/security/wannacry-ransomware-attack-hits-victims-with-microsoft-smb-exploit/. Acessado em Junho de 2024.

Li, F., Rogers, L., Mathur, A., Malkin, N., and Chetty, M. (2019). Keepers of the machines: examining how system administrators manage software updates. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, SOUPS'19, page 273–288, USA. USENIX Association.

Martius, F. and Tiefenau, C. (2020). What does this update do to my systems? – an analysis of the importance of update-related information to system administrators. In *USENIX Symposium on Usable Privacy and Security (SOUPS)*, Virtual Conference. USENIX Association.

National Vulnerability Database (2024). Common vulnerabilities and exposures program. https://www.cve.org.

NIST (2023). Cve-2023-26360 - adobe coldfusion deserialization of untrusted data vulnerability. https://nvd.nist.gov/vuln/detail/CVE-2023-26360.

Securin, CSW, Ivanti, and Cyware (2023). Ransomware report. https://www.securin.io/ransomware-report-2023-download/.

Security ScoreCard (2024). Cvedetails. https://www.cvedetails.com/.

Wash, R., Rader, E., Vaniea, K., and Rizor, M. (2014). Out of the loop: how automated software updates cause unintended security consequences. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, SOUPS '14, page 89–104, USA. USENIX Association.