RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

Doze Anos Viraram Cinco: Obsolescência Induzida Por Software Em PCs A Partir Do Fim De Suporte Do Windows 10 E Dos Requisitos Do Windows 11

Twelve Years Turned Into Five: Software-Induced Obsolescence In PCs Following The End Of Windows 10 Support And The Requirements Of Windows 11

Márcio Mendes Cerqueira, cerqueira.marcio@ufma.br

Rhaynon Carvalho Soares, rhaynon.carvalho@discente.ufma.br

Luís Eduardo Baima do Lago Melônio Junior, leblm.junior@discente.ufma.br

Resumo
A durabilidade prática de computadores pessoais (PCs) tem sido progressivamente reduzida não apenas por falhas físicas, mas por um fenômeno cada vez mais relevante: a obsolescência induzida por *software*. Este artigo investiga, com foco delimitado, como o fim do suporte do Windows 10, em 14 de outubro de 2025 e a exigência de uma linha de base de segurança no Windows 11 (por exemplo, TPM 2.0 e *Secure Boot*) operam como gatilhos de obsolescência funcional, encurtando o horizonte de uso de equipamentos ainda capazes do ponto de vista físico. A metodologia combina análise documental (políticas de suporte, requisitos mínimos e programas de atualização estendida), estruturação de cenários e uma matriz de decisão para usuários domésticos e organizações. Discute-se o impacto sobre risco cibernético, custo total de propriedade e externalidades ambientais à luz da Política Nacional de Resíduos Sólidos (PNRS) e da logística reversa de eletroeletrônicos no Brasil. Por fim, o estudo dialoga com movimentos regulatórios recentes na União Europeia voltados à promoção do reparo e ao ecodesign, propondo recomendações práticas para extensão de vida útil, governança de ciclo de vida e compras mais sustentáveis.
Palavras-chave: obsolescência; fim de suporte; ciclo de vida; lixo-eletrônico; economia circular.

Abstract
The practical lifespan of personal computers has been reduced not only by physical failure but increasingly by software-induced obsolescence. This paper provides a tightly scoped investigation of how Windows 10 end of support on October 14, 2025 and Windows 11 security baseline requirements (e.g., TPM 2.0 and Secure Boot) can trigger functional obsolescence, shortening the usable life of still-capable hardware. The method combines document analysis (support policies, minimum requirements and extended security updates), scenario-building and a decision matrix for home users and organizations. We discuss cybersecurity risk, total cost of ownership and environmental externalities under Brazil's National Solid Waste Policy and e-waste reverse logistics, while connecting findings to recent EU policy moves promoting repair and ecodesign. Finally, we propose actionable recommendations for lifetime extension, lifecycle governance and more sustainable procurement.
Keywords: obsolescence; end of support; lifecycle; e-waste; circular economy.

1 INTRODUÇÃO

A expressão "obsolescência" costuma ser associada ao desgaste físico inevitável de equipamentos. Entretanto, no contexto atual de plataformas digitais, a vida útil prática de um PC depende de um conjunto de camadas sociotécnicas: sistema operacional, aplicativos, padrões de segurança, compatibilidade com *drivers*, requisitos mínimos e a própria política de suporte dos fornecedores. Nesse cenário, computadores que permanecem funcionais do ponto de vista de

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

hardware podem se tornar progressivamente "inadequados" para uso seguro e produtivo por motivos predominantemente de *software*, caracterizando "obsolescência" induzida por *software* (Poppe et al., 2021). Este artigo conclui o escopo em um evento tecnicamente bem definido e com consequências amplas: o fim do suporte do Windows 10, em 14 de outubro de 2025 (Microsoft, 2025), combinado aos requisitos de segurança e compatibilidade do Windows 11 (Microsoft, 2025).

A transição entre versões do Windows é recorrente na história da computação pessoal, mas a dinâmica recente introduz um elemento adicional: a consolidação de uma linha de base de segurança (TPM 2.0, *Secure Boot* e UEFI) que pode excluir parte do sistema instalado, especialmente equipamentos anteriores a determinados ciclos de CPU/*firmware* (Microsoft, 2025). Mesmo onde existam *workarounds*(soluções alternativas temporárias), a discussão relevante para durabilidade é se essas alternativas preservam segurança, desempenho, conformidade e suporte em horizonte realista.

A relevância do tema ultrapassa a tecnologia. O uso de *software* sem suporte é frequentemente apontado por órgãos de cibersegurança como prática de risco elevado, por aumentar a exposição a vulnerabilidades e reduzir a capacidade de resposta a incidentes (Cybersecurity and Infrastructure Security Agency, 2025a, 2025b). Em paralelo, a pressão por atualização pode acelerar a geração de resíduos eletroeletrônicos, cuja tendência global permanece ascendente, com lacunas entre geração e reciclagem documentadas (International Telecommunication Union; UNITAR, 2024). No Brasil, a PNRS e normas específicas de logística reversa de eletroeletrônicos estabelecem deveres e instrumentos para reduzir impactos, mas o desafio operacional permanece significativo (Brasil, 2010; 2020; 2022).

Diante desse quadro, este estudo toma o caso Windows 10/Windows 11 como um recorte empírico para examinar como decisões de suporte e parâmetros técnicos de atualização reconfiguram, na prática, a durabilidade de PCs que ainda se mantêm operacionais do ponto de vista físico. A investigação parte da distinção conceitual entre obsolescência induzida por *software* e obsolescência material do *hardware*, buscando delimitar com clareza o que, nesse processo, decorre do envelhecimento natural dos componentes e o que resulta de alterações nas camadas de *software*, nos requisitos mínimos e nas políticas do fornecedor. Em seguida, descreve-se o marco do encerramento do suporte do Windows 10 e as alternativas que se colocam a usuários e organizações, incluindo opções como programas de atualizações estendidas e estratégias de continuidade que, na prática, costumam ser mobilizadas para reduzir riscos.

Na sequência, mapeiam-se os requisitos do Windows 11 com ênfase nos critérios relacionados à segurança e à compatibilidade — especialmente aqueles que condicionam a atualização a determinadas bases de *firmware* e proteção (como TPM, Secure Boot e UEFI) — para compreender em que medida tais exigências funcionam como barreiras técnicas e institucionais à manutenção do uso de equipamentos mais antigos. A partir dessa análise, no trabalho propõe-se a

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

construção de cenários comparáveis e de uma matriz de decisão capaz de orientar escolhas conforme perfis distintos (usuários domésticos, pequenas organizações e ambientes corporativos), ponderando risco de segurança, custo total de propriedade, desempenho esperado, conformidade e horizonte realista de suporte. Por fim, discute-se como a aceleração das substituições pode repercutir na geração de resíduos eletroeletrônicos e na pressão sobre cadeias de descarte e reaproveitamento, articulando o tema aos instrumentos normativos aplicáveis no Brasil, com destaque para a logística reversa e para os mecanismos previstos na política de resíduos que buscam mitigar impactos e ampliar a destinação ambientalmente adequada.

2 METODOLOGIA

Este estudo adota uma abordagem qualitativa, complementada por um componente estruturado de apoio à decisão, a fim de interpretar como políticas de suporte e requisitos de compatibilidade atuam como mecanismos de obsolescência induzida por *software* no caso Windows 10/Windows 11. A metodologia foi organizada em três frentes principais. Em primeiro lugar, realizou-se uma análise documental de fontes oficiais e técnicas relacionadas ao fim de suporte do Windows 10, aos requisitos e especificações do Windows 11 e à possibilidade de adoção de atualizações de segurança estendidas (ESU) como alternativa para continuidade temporária. Também foram incluídas diretrizes públicas que tratam do risco associado ao uso de *software* sem suporte, especialmente aquelas provenientes de organismos de cibersegurança que orientam práticas de mitigação e gestão de vulnerabilidades. Para sustentar a discussão ambiental e regulatória, foram considerados o arcabouço brasileiro da Política Nacional de Resíduos Sólidos (PNRS) e seus decretos correlatos, além de normas europeias recentes que tratam de durabilidade, reparabilidade e circularidade em produtos eletrônicos.

Em seguida, com base nas evidências documentais e nos condicionantes técnicos mais recorrentes, foram construídos quatro cenários típicos de decisão, combinando perfis de usuário e restrições de compatibilidade. Esses cenários contemplam desde o usuário doméstico com equipamento compatível com o Windows 11 até situações em que o PC não atende aos requisitos de segurança, CPU ou *firmware*; incluem ainda organizações com parque computacional heterogêneo e obrigações formais de segurança e conformidade; e, por fim, organizações que adotam estratégias de economia circular, priorizando reuso, recondicionamento, logística reversa e compras sustentáveis como diretrizes institucionais. A finalidade dos cenários é representar condições plausíveis e comparáveis, permitindo observar como as alternativas de atualização, migração, suporte estendido ou renovação do parque produzem resultados distintos conforme o contexto.

A partir desses cenários, elaborou-se uma matriz de decisão baseada em critérios que refletem os principais *trade-offs* (são escolhas que envolvem ganhos e perdas) do problema:

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

segurança, custo total de propriedade (TCO), continuidade operacional, impacto ambiental, complexidade de implementação e aderência ao suporte. A matriz não busca estabelecer uma resposta única e universal, mas tornar explícitas as escolhas possíveis e suas consequências, fornecendo um instrumento para que a decisão seja tecnicamente justificada e coerente com as necessidades de cada perfil. Por fim, reconhecem-se limitações importantes: o estudo não realiza medições empíricas de desempenho em modelos específicos de PCs, nem estima quantitativamente emissões ou impactos ambientais por unidade. O foco recai sobre os mecanismos de suporte e requisitos e sobre suas implicações decisórias, de modo que, especialmente em ambientes organizacionais, recomenda-se complementar a análise com inventário do conjunto de equipamentos instalados, caracterização do perfil de uso e uma avaliação de risco própria.

3 REFERENCIAL TEÓRICO

A literatura sobre obsolescência descreve que a perda de utilidade de um bem pode ocorrer por mecanismos distintos. Há, por exemplo, a obsolescência material, relacionada a falhas e desgaste físico, e formas de obsolescência funcional e psicológica, associadas, respectivamente, ao momento em que o produto deixa de atender necessidades práticas ou ao desejo por novidade e substituição (Sierra-Fontalvo et al., 2023). No contexto contemporâneo de plataformas digitais, entretanto, a dimensão funcional tende a ganhar centralidade: a vida útil "real" de um PC depende de camadas sociotécnicas como sistema operacional, drivers, compatibilidade de aplicativos, padrões mínimos de segurança e, sobretudo, da política de suporte do fornecedor. Isso significa que um equipamento pode manter-se fisicamente operacional e, ainda assim, tornar-se progressivamente inadequado para uso seguro e produtivo por motivos predominantemente ligados ao software.

Essa constatação se conecta diretamente ao conceito de obsolescência induzida por software. Poppe et al. discutem *software* obsolescence como um processo em que a utilidade se degrada não por defeito físico, mas por transformações no ciclo de vida do *software* e nas dependências que o cercam, distinguindo inclusive efeitos diretos e indiretos (Poppe et al., 2021). Na prática, isso produz uma compressão do período em que o equipamento permanece "adequado" para tarefas reais: mesmo que o *hardware* continue capaz de executar atividades comuns, a experiência de uso e o nível aceitável de segurança podem piorar por falta de correções, incompatibilidades, mudanças no ecossistema ou elevação de requisitos mínimos. Essa compressão é particularmente sensível quando "segurança" deixa de ser uma melhoria desejável e passa a ser uma condição mínima para acesso a serviços, autenticação e operação em rede.

Um elemento teórico importante nessa transição é a consolidação de linhas de base de

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

segurança como critério de compatibilidade. No caso do Windows 11, a exigência de TPM 2.0 e firmware UEFI com capacidade de Secure Boot explicita uma orientação: elevar o patamar mínimo de integridade de inicialização e proteção de credenciais para viabilizar recursos de segurança (Microsoft, 2025). Esse movimento, embora tenha justificativa do ponto de vista técnico, também produz um efeito estruturante sobre a durabilidade prática: a continuidade do uso suportado passa a depender de características de plataforma que não podem ser adicionadas ou habilitadas em parte do parque existente, mesmo quando os equipamentos executam tarefas cotidianas. Assim, a obsolescência induzida por software emerge não apenas do "fim de suporte", mas da interação entre política de suporte, requisitos de segurança e dependência do ecossistema.

Além do plano técnico e conceitual, a discussão se articula a uma dimensão ambiental e normativa. A aceleração de substituições por motivos de *software* tende a pressionar a geração de resíduos eletroeletrônicos. O Global *E-waste* Monitor 2024 (ITU/UNITAR) registra volumes globais recordes de *e-waste* (equipamentos eletroeletrônicos descartados ou obsoletos) e destaca que a reciclagem formal documentada não acompanha o ritmo de crescimento, com projeções de agravamento até 2030 (International Telecommunication Union; UNITAR, 2024). No Brasil, esse debate encontra base na Política Nacional de Resíduos Sólidos, que institui responsabilidade compartilhada pelo ciclo de vida dos produtos (Brasil, 2010), além de diplomas que operacionalizam instrumentos de logística reversa para eletroeletrônicos e regulamentam a PNRS (Brasil, 2020; 2022).

No plano europeu, normas recentes reforçam a agenda de extensão de vida útil: a Diretiva (UE) 2024/1799 promove regras comuns para estimular o reparo, e o Regulamento (UE) 2024/1781 cria um quadro para requisitos de ecodesign voltados à sustentabilidade e circularidade (European Union, 2024a; 2024b). Embora os regimes jurídicos não sejam diretamente equivalentes, essas referências ajudam a contextualizar uma tendência regulatória: reduzir o descarte prematuro exige alinhar incentivos, desenho de mercado e instrumentos de circularidade, e não apenas transferir ao usuário a responsabilidade por decisões individuais de troca.

3.1 Ciclo de suporte, vulnerabilidades e risco cibernético

A relação entre ciclo de suporte e risco cibernético é decisiva para explicar por que a obsolescência induzida por software pode encurtar a vida útil prática de um PC. Quando um sistema operacional entra em fim de suporte, ele deixa de receber correções regulares e atualizações de segurança, alterando o balanço de risco: vulnerabilidades descobertas após esse marco tendem a permanecer sem correção oficial, aumentando a probabilidade de exploração bem-sucedida em ambientes conectados (Microsoft, 2025; Government of the United Kingdom (GOV.UK), [s. d.]). A própria Microsoft caracteriza o fim do suporte do Windows 10 como a cessação de atualizações de segurança, atualizações de software e suporte técnico, ainda que o sistema continue funcionando

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026
(Microsoft, 2025).

As Diretrizes públicas de cibersegurança reforçam esse raciocínio no plano operacional: a CISA recomenda manter software atualizado e substituir hardware ou software em fim de vida, justamente porque produtos sem suporte reduzem a capacidade de prevenção e resposta e ampliam a exposição a atacantes (Cybersecurity & Infrastructure Security Agency (CISA), 2026). Essa orientação ganha peso em contextos organizacionais, onde o risco não é apenas técnico, mas também operacional e de governança: sistemas desatualizados tendem a demandar controles compensatórios, segmentação, restrições de acesso e esforço adicional de gestão de risco — custos que nem sempre aparecem no preço visível do equipamento, mas impactam diretamente o custo total de propriedade e a decisão de migração (Joint Task Force; National Institute of Standards and Technology (NIST), 2020; Government of the United Kingdom (GOV.UK), [s. d.]).

Em síntese, o ciclo de suporte opera como um gatilho que reclassifica um computador de "operante" para "operante com risco crescente". A durabilidade prática, portanto, não se encerra apenas quando o *hardware* falha, mas quando o ambiente de uso exige um patamar mínimo de segurança e compatibilidade que um sistema sem suporte não consegue mais garantir. Essa perspectiva dá base para interpretar a transição Windows 10/Windows 11 não apenas como troca de versão, mas como um caso observável em que suporte, requisitos de segurança e dependência do ecossistema influenciam diretamente o tempo de uso aceitável de PCs.

4. Resultados e discussões: "Do suporte ao descarte: como políticas de atualização e segurança encurtam a durabilidade de PCs"

A análise do caso Windows 10/Windows 11 permite explicar, de modo bastante concreto, por que políticas de atualização e segurança encurtam a durabilidade de PCs. O ponto de partida é reconhecer que a vida útil real de um computador não depende apenas de o *hardware* permanecer fisicamente operacional, mas de ele continuar adequado para uso em um ambiente conectado, com risco administrável (National Cyber Security Centre (NCSC), [s. d.]; Government of the United Kingdom (GOV.UK), [s. d.]). Nesse sentido, o fim do suporte do Windows 10 em 14 de outubro de 2025 constitui um marco decisivo (Microsoft, 2025): a partir dele, o sistema pode continuar iniciando e executando programas, porém deixa de receber correções regulares de segurança e perde o suporte técnico oficial (Microsoft, 2025; Government of the United Kingdom (GOV.UK), [s. d.]). Essa distinção sustenta o argumento central do artigo: "funcionar" não é sinônimo de "permanecer adequado". Para usuários domésticos, a inadequação tende a aparecer primeiro como aumento de exposição a ameaças e, gradualmente, como incompatibilidades e degradações no ecossistema (National Cyber Security Centre (NCSC), [s. d.]; Government of the United Kingdom (GOV.UK),

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

[s. d.]). Para organizações, o problema se agrava porque operar sistemas sem suporte pode conflitar com políticas internas, exigências de auditoria e compromissos de conformidade, elevando custos indiretos de mitigação e gerenciamento de risco (Joint Task Force; National Institute of Standards and Technology (NIST), 2020; Internet Security, Inc. (CIS®), 2024; NHS England, 2023).

A tentativa de "ganhar tempo" por meio de Atualizações de Segurança Estendidas (Extended Security Updates) ilustra bem o caráter sociotécnico desse encurtamento. O ESU pode reduzir risco durante a migração (Microsoft, 2025c; Microsoft, 2025d), mas deve ser lido como ponte, não como solução de durabilidade prolongada: costuma ter horizonte limitado, não necessariamente entrega novas funcionalidades e não substitui o suporte pleno do ecossistema (Microsoft, 2025d; Microsoft, 2025e). Em termos práticos, o ESU tende a postergar a obsolescência induzida por software, sem eliminá-la; e, em certos contextos, desloca parte do custo para o acesso temporário à manutenção de segurança (Microsoft, 2025e). Portanto, mesmo quando há uma estratégia transitória disponível, ela não interrompe o mecanismo de encurtamento — apenas reorganiza o calendário de decisão (Microsoft, 2025d; Governo do Reino Unido (GOV.UK), [s. d.]).

O segundo componente é o papel dos requisitos do Windows 11 na geração de obsolescência por incompatibilidade. A exigência de uma linha de base de segurança, como UEFI com Secure Boot e TPM 2.0 (Microsoft, 2025b), pode ser compreendida por duas lentes que não se excluem: por um lado, elevar o patamar mínimo pode reduzir superfície de ataque e habilitar proteções modernas; por outro, uma parcela dos dispositivos instalados não conseguem atender aos requisitos, o que cria pressão por substituição antecipada. É justamente essa coexistência que torna o fenômeno relevante: a política de segurança, ao mesmo tempo em que fortalece o sistema para quem consegue migrar, pode bloquear a migração de máquinas ainda funcionais. O resultado líquido, então, não é apenas "o Windows 11 é mais seguro", mas que a capacidade de manter o uso seguro e suportado passa a depender da plataforma. Para equipamentos sem TPM 2.0/Secure Boot (ou sem CPUs compatíveis), a alternativa "migrar" pode estar indisponível, e permanecer no Windows 10 após o fim de suporte implica aceitar um risco crescente. (Microsoft, 2025b)

Esse processo se intensifica quando a segurança deixa de ser apenas uma "melhoria" e se torna requisito de uso. À medida que bancos, serviços públicos, navegadores e aplicativos elevam padrões mínimos e exigências de atualização, usuários podem atingir um "ponto de não retorno", em que tarefas simples — autenticação, acesso a serviços e navegação segura — tornam-se mais frágeis ou degradadas em sistemas sem suporte (Government of the United Kingdom (GOV.UK), [s. d.]; National Cyber Security Centre (NCSC), [s. d.]; Internet Security, Inc. (CIS®), 2024).

Por isso, as diretrizes de cibersegurança recomendam explicitamente manter atualizações e substituir software/hardware no fim de vida (Cybersecurity and Infrastructure Security Agency (CISA), 2025; National Cyber Security Center (NCSC), [s. d.]; Internet Security, Inc. (CIS®), 2024).

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

Em ambientes organizacionais, há risco reputacional e possibilidade de incidentes com impacto operacional (Joint Task Force; National Institute of Standards and Technology (NIST), 2020).

Assim, o encurtamento não ocorre por uma única decisão técnica isolada, mas pela interação entre fim de suporte, nova linha de base de segurança e dependência do ecossistema, que empurra indivíduos e instituições para a migração em janelas de tempo mais curtas do que a durabilidade física do equipamento permitiria (Google, [s. d.]; Mozilla, [s. d.]).

A discussão, porém, não se limita à tecnologia: ela revela *trade-offs* econômicos e ambientais. No custo total de propriedade, o usuário doméstico costuma perceber principalmente o preço de um novo computador, mas, para organizações, os custos ocultos podem ser maiores — inventário, testes, re-homologação, treinamento, adaptação de periféricos e gestão de riscos —, e é nesse contexto que soluções como ESU podem ser justificadas como transição para migração escalonada (Microsoft, 2025c). Em paralelo, quando a mudança de *software* induz substituição antecipada, cresce a pressão sobre a geração de resíduos eletroeletrônicos, reconhecida em relatórios internacionais (International Telecommunication Union; UNITAR, 2024). No Brasil, a PNRS estabelece diretrizes e responsabilidade compartilhada (Brasil, 2010), existem normas específicas para logística reversa de eletroeletrônicos de uso doméstico (Brasil, 2020) e o Decreto 10.936/2022 reforça instrumentos de implementação (Brasil, 2022), mas a efetividade depende de infraestrutura e operacionalização; logo, a mitigação ambiental não decorre automaticamente da "decisão tecnológica correta", e sim de políticas e práticas acopladas, como reuso, recondicionamento e destinação adequada.

Finalmente, o debate europeu sobre reparo e *ecodesign* ajuda a enquadrar o tema como algo maior do que escolhas individuais. Instrumentos recentes, como a Diretiva (UE) 2024/1799 (reparo) e o Regulamento (UE) 2024/1781 (*ecodesign*), reforçam que durabilidade pode ser objetivo de política pública e de desenho de mercado (European Union, 2024a, 2024b). Mesmo sem transposição automática ao Brasil, a convergência é clara: se a vida útil prática é encurtada por decisões de suporte, segurança e compatibilidade, então ampliar durabilidade exige também respostas estruturais, de governança, regulação, compras sustentáveis e mecanismos efetivos de circularidade.

4.1 Cenários: decisão prática para usuários e organizações

Após demonstrar, ao longo do referencial teórico e das discussões, que a durabilidade prática de PCs é encurtada pela interação entre fim de suporte, elevação da linha de base de segurança e dependência do ecossistema, torna-se necessário traduzir esse diagnóstico em escolhas concretas. Em outras palavras, se o problema não é apenas "trocar de versão", mas administrar risco, compatibilidade, custos indiretos e impactos ambientais em janelas de tempo cada vez mais curtas,

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026
então a análise precisa avançar do nível explicativo para um nível decisório. Por isso, a seção seguinte organiza o caso Windows 10/Windows 11 em cenários típicos para usuários e organizações, refletindo restrições de compatibilidade e graus distintos de exigência de segurança e conformidade; em seguida, consolida essas alternativas em uma matriz qualitativa de *trade-offs*, tornando explícitas as consequências relativas de cada estratégia em segurança, TCO, impacto ambiental e complexidade de implementação.

C1 — Usuário com PC compatível com Windows 11. A decisão tende a ser migração, com atenção a backup, verificação de drivers e custos de licença (quando aplicável). O ponto crítico é planejar a migração antes da degradação do suporte do ecossistema.

C2 — Usuário com PC não compatível. Há três rotas principais: (a) adquirir novo equipamento; (b) permanecer no Windows 10 com mitigação (idealmente ESU quando aplicável) (Microsoft, 2025); (c) migrar para outro sistema operacional suportado (por exemplo, distribuições Linux), considerando curva de aprendizado e compatibilidade de *software*. A rota (b) é viável apenas como transição e exige prudência; a rota (a) tem custo e impacto ambiental; a rota (c) pode estender vida útil, mas depende do perfil de uso.

C3 — Organização com parque heterogêneo. Aqui, o custo de migração envolve inventário, testes, compatibilidade, suporte interno/terceirizado, e cronograma. A recomendação geral de "atualizar e substituir EOL" é consistente com as diretrizes de segurança (Cybersecurity and Infrastructure Security Agency, 2025), mas uma organização pode adotar estratégias escalonadas, mantendo temporariamente um subconjunto em ESU e redirecionando equipamentos antigos para usos offline, laboratórios controlados ou programas de recondicionamento.

C4 — Organização com estratégia circular. O desafio é conciliar segurança e extensão de vida útil. Estudos sobre TIC circular em organizações indicam barreiras contratuais e de incentivos, além de acesso a peças e equipamentos recondicionados (Mc-Mahon; Mugge; Hultink, 2024). Para superar barreiras, recomenda-se integrar requisitos de circularidade e manutenção nos contratos, evitando que a única "saída" seja renovar parque por indisponibilidade de suporte.

4.2 Matriz de decisão e trade-offs

Na Tabela 1 a seguir apresenta-se uma matriz de decisão qualitativa (escala Baixo/Médio/Alto), útil para comparar estratégias típicas. Os resultados variam conforme contexto, mas a estrutura torna os *trade-offs* explícitos.

Tabela 1: Matriz de decisão para estratégias pós-fim de suporte do Windows 10.

Estratégia	Segurança	TCO	Impacto Ambiental	Complexidade

Migrar para Windows 11 em computador compatível	ALTO	MÉDIO	BAIXO/ MÉDIO	MÉDIO
Comprar novo computador	ALTO	ALTO	ALTO	BAIXO/MÉDIO
Manter Windows 10 com ESU (ponte)	MÉDIO/ALTO	MÉDIO	BAIXO	MÉDIO
Manter Windows 10 sem suporte após 14/10/25	BAIXO	BAIXO (CURTO PRAZO)	BAIXO (CURTO PRAZO)	BAIXO
Migrar para Linux	MÉDIO/ALTO	BAIXO/ MÉDIO	BAIXO	MÉDIO/ ALTO

Fonte: Autoria própria

Do ponto de vista estritamente de segurança, a alternativa "Windows 10 sem suporte" é a mais crítica e, em geral, não recomendada, alinhando-se a alertas sobre risco em *software* EOL (Cybersecurity and Infrastructure Security Agency, 2025). Já do ponto de vista ambiental, a substituição de equipamento tende a ser a pior opção quando ocorre prematuramente, por antecipar descarte e demanda por nova fabricação.

Em ambientes organizacionais, esse tipo de transição raramente ocorre como um "projeto técnico simples". Na prática, é comum que a organização tenha um conjunto de equipamentos heterogêneo, com máquinas em diferentes idades e perfis de uso, além de aplicações legadas e periféricos específicos (impressoras, scanners, módulos de assinatura, sistemas proprietários) cuja compatibilidade nem sempre acompanha o ritmo das atualizações. Frequentemente, a migração é condicionada por janelas operacionais (evitar períodos críticos), por processos de homologação e por dependências contratuais com fornecedores de *software* e suporte. Nesse contexto, a decisão costuma ser fatiada: migram-se primeiro os ativos críticos e compatíveis, mantém-se um subconjunto em regime transitório (com controles compensatórios e, quando aplicável, suporte estendido), e redirecionam-se equipamentos mais antigos para funções de menor exposição ou ambientes controlados, até que seja possível substituição planejada.

5 Conclusão (ou Considerações Finais)

Este artigo sustenta que a durabilidade prática de computadores pode ser reduzida de forma significativa por mecanismos induzidos por *software*, especialmente quando políticas de suporte e requisitos de segurança estabelecem um limiar de compatibilidade que parte do equipamento em uso não consegue ultrapassar. O caso Windows 10/Windows 11 é exemplificativo porque combina um marco temporal bem definido — o fim do suporte do Windows 10 em 14 de outubro de 2025 — com a consolidação de uma linha de base de segurança no Windows 11, baseada em requisitos como TPM

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

2.0, Secure Boot e UEFI, que atuam como filtros de elegibilidade e podem bloquear a atualização em equipamentos ainda funcionais. O resultado é um encurtamento da vida útil prática: computadores que permanecem operacionais do ponto de vista físico passam a conviver com risco crescente ao permanecerem em um sistema sem correções regulares, enquanto a migração para a versão suportada pode ser inviabilizada por limitações de plataforma.

A análise também mostrou que não existe uma solução única aplicável a todos os contextos. Quando o equipamento é compatível, migrar para o Windows 11 tende a ser a alternativa mais consistente do ponto de vista de continuidade e segurança. Quando não há compatibilidade, estratégias de transição tornam-se relevantes, especialmente o uso de Atualizações de Segurança Estendidas (ESU), que pode reduzir risco no curto prazo e permitir migração escalonada, mas deve ser compreendida como ponte, e não como extensão duradoura do ciclo de vida. Em alguns cenários, a migração para sistemas operacionais alternativos suportados pode estender a vida útil prática, desde que compatível com o perfil de uso e com as necessidades de *software*; já a substituição do equipamento, embora resolva o problema de suporte e compatibilidade, tende a ampliar custos e pode intensificar impactos ambientais quando ocorre de forma prematura, antecipando descarte e ampliando a pressão sobre a cadeia de resíduos.

Nesse ponto, a dimensão ambiental e regulatória deixa de ser periférica e passa a integrar a própria racionalidade da decisão. A PNRS estrutura princípios e instrumentos voltados à prevenção, redução, reutilização e tratamento de resíduos, estabelecendo responsabilidade compartilhada, enquanto normas específicas disciplinam a logística reversa obrigatória para eletroeletrônicos de uso doméstico e reforçam instrumentos de implementação. Isso implica que estratégias tecnológicas de migração e renovação do parque precisam ser acopladas a fluxos formais de reuso, recondicionamento e destinação adequada, sob pena de a "solução" de segurança resultar em agravamento de *e-waste*. Em paralelo, iniciativas recentes na União Europeia — voltadas ao reparo e ao ecodesign — reforçam que extensão de vida útil é também uma meta de política pública e de desenho de mercado, e não apenas uma escolha individual do usuário.

Como implicação prática, o estudo sugere que decisões de usuários e organizações tendem a ser melhores quando deixam de ser reativas e passam a ser planejadas. Para usuários domésticos, isso significa verificar compatibilidade com antecedência e evitar a permanência prolongada em sistemas sem suporte; quando a migração não é viável, utilizar alternativas transitórias como ESU quando aplicável ou migrar para sistemas suportados, além de reduzir exposição em usos inevitáveis (por exemplo, evitar tarefas sensíveis em ambiente sem suporte e restringir uso a contextos controlados). Para organizações, a recomendação é tratar *software* em fim de vida como risco material de governança, iniciando por inventário e classificação por criticidade, adotando estratégias híbridas em que ativos críticos migram primeiro e o ESU, quando utilizado, tenha plano claro de saída, além

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

de incorporar cláusulas de circularidade em contratações de TIC (manutenção, reposição de peças, recondicionamento, recompra e destinação adequada), uma vez que barreiras contratuais e de incentivos são relevantes para viabilizar circularidade na prática. Em todos os casos, a destinação ambientalmente adequada deve ser tratada como parte do processo decisório, com aderência a canais formais e auditáveis, alinhados à PNRS e seus regulamentos, e à lógica de gestão de risco recomendada por diretrizes públicas de cibersegurança.

Como contribuição, este estudo propõe um recorte replicável para futuras análises: observar marcos de suporte e requisitos de segurança como variáveis centrais da obsolescência induzida por software, articulando-os a custo total de propriedade e impactos ambientais. Pesquisas futuras podem quantificar emissões evitadas por estratégias de extensão de vida útil, comparar diferentes ecosistemas (Windows, Linux, ChromeOS) e avaliar empiricamente a efetividade de políticas e programas de recondicionamento e logística reversa, com dados de campo e inventários reais de ambientes domésticos e organizacionais.

REFERÊNCIAS

BRASIL. Decreto nº 10.240, de 12 de fevereiro de 2020 (Logística reversa de produtos eletroeletrônicos). 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10240.htm. Acesso em: 03 dez. 2025.

BRASIL. Decreto nº 10.936, de 12 de janeiro de 2022 (Regulamenta a PNRS). 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d10936.htm. Acesso em: 06 dez. 2025.

BRASIL. Lei nº 12.305, de 2 de agosto de 2010 (Política Nacional de Resíduos Sólidos). 2010. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/lei/l12305.htm. Acesso em: 17 nov. 2025.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA). Bad Practices (StopRansomware). 2026. Disponível em: https://www.cisa.gov/stopransomware/bad-practices. Acesso em: 11 dez. 2025.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (CISA). Update Business Software. 2026. Disponível em: https://www.cisa.gov/audiences/small-and-medium-businesses/secure-your-business/update-business-software. Acesso em: 16 dez. 2025.

EUROPEAN UNION. Directive (EU) 2024/1799 on common rules promoting the repair of goods. 2024. Disponível em: https://eur-lex.europa.eu/eli/dir/2024/1799/oj/eng. Acesso em: 20 dez. 2025.

EUROPEAN UNION. Regulation (EU) 2024/1781 establishing a framework for setting ecodesign requirements for sustainable products. 2024. Disponível em: https://eur-lex.europa.eu/eli/reg/2024/1781/oj/eng. Acesso em: 21 dez. 2025.

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

GOOGLE. Chrome browser system requirements. [s. d.]. Disponível em: https://support.google.com/chrome/a/answer/7100626?hl=en. Acesso em: 16 jan. 2026.

GOVERNMENT OF THE UNITED KINGDOM (GOV.UK). Obsolete platforms guidance. 2015. Disponível em: https://assets.publishing.service.gov.uk/media/5a758829e5274a545822c3e7/Obsolete_platforms_guidance.pdf. Acesso em: 16 jan. 2026.

INTERNATIONAL TELECOMMUNICATION UNION (ITU); UNITAR. The Global E-waste Monitor 2024. 2024. Disponível em: https://www.itu.int/en/ITU-D/Environment/Documents/Publications/2025/d-gen-e_waste.01-2024-pdf-e.pdf. Acesso em: 20 dez. 2025.

INTERNET SECURITY, INC. (CIS®). CIS Controls v8.1 Guide (June 2024). 2024. Disponível em: https://etir.unb.br/wp-content/uploads/2024/10/CIS_Controls__v8.1_Guide__2024_06.pdf. Acesso em: 16 jan. 2026.

INTERNET SECURITY, INC. (CIS®). CIS Controls v8.1. [s. d.]. Disponível em: https://www.cisecurity.org/controls/v8-1. Acesso em: 16 jan. 2026.

JOINT TASK FORCE; NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5). 2020. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. Acesso em: 16 jan. 2026.

MCMAHON, K.; MUGGE, R.; HULTINK, E. J. Overcoming barriers to circularity for internal ict management in organizations: A change management approach. Resources, Conservation and Recycling, v. 205, p. 107568, 2024. Disponível em: https://www.sciencedirect.com/science/article/pii/S0921344924001630. Acesso em: 20 dez. 2025.

MICROSOFT. Extended Security Updates (ESU) program for Windows 10. 2025. Disponível em: https://learn.microsoft.com/en-us/windows/whats-new/extended-security-updates. Acesso em: 16 jan. 2026.

MICROSOFT. Product Lifecycle FAQ – Extended Security Updates. [s. d.]. Disponível em: https://learn.microsoft.com/en-us/lifecycle/faq/extended-security-updates. Acesso em: 16 jan. 2026.

MICROSOFT. Stay secure with Windows 11, Copilot+ PCs and Windows 365 before support ends for Windows 10. 2025. Disponível em: https://blogs.windows.com/windowsexperience/2025/06/24/stay-secure-with-windows-11-copilot-pcs-and-windows-365-before-support-ends-for-windows-10/. Acesso em: 16 jan. 2026.

MICROSOFT. Windows 10 Consumer Extended Security Updates (ESU). 2025. Disponível em: https://www.microsoft.com/en-us/windows/extended-security-updates. Acesso em: 21 dez. 2025.

Ano VI, v.1 2026 | submissão: 17/01/2026 | aceito: 19/01/2026 | publicação: 21/01/2026

MICROSOFT. Windows 10 support has ended on October 14, 2025. 2025. Disponível em: https://support.microsoft.com/en-us/windows/windows-10-support-has-ended-on-october-14-2025-2ca8b313-1946-43d3-b55c-2b95b107f281. Acesso em: 21 dez. 2025.

MICROSOFT. Windows 11 Specs and System Requirements. 2025. Disponível em: https://www.microsoft.com/en-us/windows/windows-11-specifications. Acesso em: 21 dez. 2025.

MOZILLA. What Windows 10 end of support means for Firefox users. [s. d.]. Disponível em: https://support.mozilla.org/en-US/kb/firefox-support-windows-10-end-support. Acesso em: 16 jan. 2026.

NATIONAL CYBER SECURITY CENTRE (NCSC). Keeping devices and software up to date. [s. d.]. Disponível em: https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date. Acesso em: 16 jan. 2026.

NATIONAL CYBER SECURITY CENTRE (NCSC). Obsolete products. [s. d.]. Disponível em: https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/obsolete-products. Acesso em: 16 jan. 2026.
NHS ENGLAND. Data Security Standard 8: unsupported systems. 2023. Disponível em: https://www.dsptoolkit.nhs.uk/News/Attachment/765. Acesso em: 16 jan. 2026.

POPPE, E. et al. Is it a bug or a feature? the concept of software obsolescence. In: Proceedings of the 4th PLATE Virtual Conference (Product Lifetimes and the Environment). Limerick, Ireland (virtual): [s. n.], 2021. Disponível em: https://researchrepository.ul.ie/bitstreams/2e091cb3-6520-4e3b-a806-eee74d3f9682/download. Acesso em: 20 dez. 2025.

SIERRA-FONTALVO, L. et al. A deep dive into addressing obsolescence in product design. Heliyon, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S2405844023090643. Acesso em: 20 dez. 2025.